



EUROPESE
COMMISSIE

Brussel, 8.12.2021
COM(2021) 784 final

2021/0410 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende geautomatiseerde gegevensuitwisseling ten behoeve van politieke samenwerking (“Prüm II”) en tot wijziging van de Besluiten 2008/615/JBZ en 2008/616/JBZ van de Raad en de Verordeningen (EU) 2018/1726, (EU) 2019/817 en (EU) 2019/818 van het Europees Parlement en de Raad

{SEC(2021) 421 final} - {SWD(2021) 378 final} - {SWD(2021) 379 final}

TOELICHTING

ACHTERGROND VAN HET VOORSTEL

• **Motivering van het voorstel**

Door criminaliteit wordt in heel Europa de veiligheid en het welzijn van de EU-burgers ondermijnd. De rechtshandhavingsinstanties hebben dan ook solide, goed werkende instrumenten nodig om die criminaliteit doeltreffend te kunnen bestrijden. Samenwerking en informatie-uitwisseling zijn de krachtigste instrumenten om criminaliteit te bestrijden en gerechtigheid na te streven¹. In 2021 was meer dan 70 % van de criminele organisaties in meer dan drie lidstaten aanwezig². Zelfs bij het schijnbaar meest plaatselijke misdrijf kan er een verband bestaan met andere plaatsen in Europa waar dezelfde dader strafbare feiten heeft gepleegd. Ook zijn de banden van veronderstelde plaatselijke criminaliteit met structuren en operaties van georganiseerde misdaad vaak niet duidelijk. Om criminaliteit doeltreffend te bestrijden, moeten de rechtshandhavingsinstanties dan ook tijdig gegevens kunnen uitwisselen. De EU heeft de rechtshandhavingsinstanties al heel wat instrumenten ter beschikking gesteld om uitwisseling van informatie te vergemakkelijken. Die instrumenten zijn cruciaal gebleken om criminele activiteiten en netwerken aan het licht te brengen³, maar er zijn nog steeds informatielacunes die moeten worden aangepakt. Aangezien allerlei gegevens afzonderlijk worden opgeslagen in verschillende nationale IT-systemen en in grootschalige IT-systemen op EU-niveau, moet ervoor worden gezorgd dat die systemen met elkaar kunnen communiceren.

In een ruimte zonder controles aan de binnengrenzen (het “Schengengebied”) bestaan er nog steeds grenzen en obstakels voor de uitwisseling van gegevens tussen rechtshandhavingsinstanties⁴, hetgeen leidt tot blinde vlekken en mazen in de rechtshandhaving voor vele criminelen en terroristen die in meer dan één lidstaat actief zijn. Dit initiatief heeft, samen met het tegelijkertijd aangenomen voorstel voor een richtlijn betreffende informatie-uitwisseling tussen de rechtshandhavingsinstanties van de lidstaten⁵, tot doel de uitwisseling van informatie tussen de lidstaten te versterken en daartoe de rechtshandhavingsinstanties van de EU uit te rusten met betere instrumenten om criminaliteit en terrorisme te bestrijden⁶.

Dankzij het Prüm-kader hebben rechtshandhavingsinstanties in de hele EU al meer dan tien jaar informatie kunnen uitwisselen. De Prüm-besluiten⁷, die in 2008 zijn vastgesteld om de grensoverschrijdende politieke en justitiële samenwerking in strafzaken te ondersteunen, voorzien in geautomatiseerde uitwisseling van specifieke gegevens (DNA-profielen, vingerafdrukken en voertuigregistratiegegevens) tussen instanties die belast zijn met het voorkomen, opsporen en onderzoeken van strafbare feiten. Het Prüm-kader draagt met succes bij tot de bestrijding van criminaliteit en terrorisme in de EU, maar er zijn nog steeds lacunes op het gebied van informatie-uitwisseling en er is dus ruimte voor verdere verbetering.

¹ EU-strategie voor de veiligheidsunie 2020, COM(2020) 605 final van 24.7.2020.

² EU-dreigingsevaluatie van de zware en georganiseerde criminaliteit 2021.

³ EU-strategie voor de aanpak van georganiseerde criminaliteit (2021-2025), COM(2021) 170 final van 14.4.2021.

⁴ Dit betreft bijvoorbeeld de wijze waarop bepaalde categorieën gegevens worden uitgewisseld, het kanaal dat voor de uitwisseling wordt gebruikt, de toepasselijke termijnen enz.
⁵ [Referentie].

⁶ Mededeling “Een strategie voor een volledig functionerend en veerkrachtig Schengengebied”, COM(2021) 277 final van 2.6.2021.

⁷ Besluit 2008/615/JBZ van de Raad inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit en Besluit 2008/616/JBZ van de Raad betreffende de uitvoering van Besluit 2008/615/JBZ. De besluiten van de Raad zijn gebaseerd op het Verdrag van Prüm van 2005.

De conclusies van de Raad over de uitvoering van de Prüm-besluiten, tien jaar na de aanneming ervan, onderstreepten dat de geautomatiseerde bevraging en vergelijking van DNA-profielen, dactyloscopische gegevens en voertuigregistratiegegevens essentieel zijn voor het aanpakken van terrorisme en grensoverschrijdende criminaliteit. De Raad verzocht de Commissie tevens te overwegen de Prüm-besluiten te herzien teneinde de werkingssfeer ervan te verbreden en daartoe de nodige technische en wettelijke voorschriften te actualiseren⁸.

Met Prüm II wordt voortgebouwd op het bestaande Prüm-kader: de verordening versterkt en moderniseert dit kader en maakt interoperabiliteit met andere EU-informatiesystemen mogelijk. Zij zal ervoor zorgen dat alle relevante gegevens die de rechtshandavingsinstanties in een lidstaat ter beschikking staan ook door rechtshandavingsinstanties in andere lidstaten kunnen worden gebruikt. Zij zal er ook voor zorgen dat Europol de lidstaten ondersteuning kan bieden binnen het Prüm-kader. Dit initiatief voorziet in de totstandbrenging van een nieuwe architectuur die eenvoudigere en snellere uitwisseling van gegevens tussen de lidstaten mogelijk maakt en een hoog niveau van bescherming van de grondrechten waarborgt.

- **Doelstellingen van het voorstel**

De algemene doelstelling van dit initiatief hangt samen met het in het Verdrag besloten doel om het beheer van de buitengrenzen van het Schengengebied te verbeteren en tot de interne veiligheid van de Europese Unie bij te dragen. Tot de maatregelen daartoe behoort ook het verzamelen, opslaan, verwerken, analyseren en uitwisselen van relevante informatie⁹. Met dit instrument wordt derhalve gestreefd naar verbetering, stroomlijning en vergemakkelijking van de uitwisseling van informatie tussen de rechtshandavingsinstanties van de lidstaten, maar ook met Europol als EU-centrum voor strafrechtelijke informatie, met het oog op het voorkomen, opsporen en onderzoeken van strafbare feiten en terroristische misdrijven.

Dit voorstel heeft de volgende specifieke beleidsdoelstellingen:

- a) voorzien in een technische oplossing voor efficiënte geautomatiseerde uitwisseling van gegevens tussen rechtshandavingsinstanties, teneinde deze op de hoogte te stellen van relevante gegevens die beschikbaar zijn in de nationale databank van een andere lidstaat;
- b) ervoor zorgen dat een grotere hoeveelheid relevante gegevens (in termen van gegevenscategorieën) in de nationale databanken in andere lidstaten beschikbaar is voor alle bevoegde rechtshandavingsinstanties;
- c) ervoor zorgen dat relevante gegevens (in termen van gegevensbronnen) in de databanken van Europol beschikbaar zijn voor rechtshandavingsinstanties;
- d) rechtshandavingsinstanties efficiënte toegang bieden tot de feitelijke gegevens die overeenkomen met een “hit” in de nationale databank van een andere lidstaat.

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

In de onlangs vastgestelde Schengenstrategie¹⁰ zijn verschillende maatregelen aangekondigd om de politieke samenwerking en informatie-uitwisseling tussen rechtshandavingsinstanties te intensiveren, ter bevordering van de veiligheid in een ruimte zonder binnengrenzen, die gekenmerkt wordt door een inherente onderlinge afhankelijkheid. Samen met het voorstel voor een richtlijn betreffende informatie-

⁸ Conclusies van de Raad over de uitvoering van de Prüm-besluiten, tien jaar na de aanneming ervan (document 11227/18), <https://data.consilium.europa.eu/doc/document/ST-11227-2018-INIT/nl/pdf>.

⁹ Artikel 87, lid 2, punt a), VWEU.

¹⁰ Mededeling van de Commissie aan het Europees Parlement en de Raad “Een strategie voor een volledig functionerend en veerkrachtig Schengengebied”, COM(2021) 277 final van 2.6.2021.

uitwisseling tussen de rechtshandavingsinstanties van de lidstaten draagt dit voorstel bij tot de verwezenlijking van de doelstellingen van deze strategie, door ervoor te zorgen dat de rechtshandavingsinstanties in een lidstaat toegang hebben tot dezelfde informatie als hun collega's in andere lidstaten.

Het voorstel maakt deel uit van de context van de grootschalige EU-informatiesystemen, die sinds de vaststelling van het Prüm-kader aanzienlijk is uitgebreid. Hieronder vallen de drie centrale informatiesystemen van de EU die thans operationeel zijn: het Schengeninformatiesysteem (SIS), het Visuminformatiesysteem (VIS) en het Eurodac-systeem¹¹. Daarnaast zijn momenteel drie systemen in de ontwikkelingsfase: het inreis-uitreis-systeem (EES), het Europees reisinformatie- en -autorisatiesysteem (Etias) en het Europees Strafreregisterinformatiesysteem voor onderdanen van derde landen en staatlozen (Ecris-TCN)¹². Al deze bestaande en toekomstige systemen zijn gekoppeld door middel van het interoperabiliteitskader voor de EU-informatiesystemen¹³ op het gebied van veiligheid, grenzen en migratiebeheer, dat in 2019 is goedgekeurd en dat momenteel wordt ingevoerd. De in dit voorstel vervatte herzieningen zijn bedoeld om het Prüm-kader in overeenstemming te brengen met het interoperabiliteitskader, met name wat betreft de uitwisseling van gegevens en de algemene architectuur waarin dit interoperabiliteitskader voor de EU-informatiesystemen voorziet. Dit moet zorgen voor snelle en gecontroleerde toegang tot de informatie die rechtshandavingsfunctionarissen nodig hebben om hun taken uit te voeren en die voor hen toegankelijk is.

Het SIS bevat al signaleringen van vermiste personen en maakt zoekopdrachten op basis van vingerafdrukken mogelijk. Het SIS is een gecentraliseerd informatiesysteem op hit/no-hitbasis dat tot actie aanleiding kan geven en rechtstreeks toegankelijk is voor een groot aantal eerstelijnsgebruikers. Het bevat signaleringen en geeft onmiddellijk ter plaatse antwoord met vermelding van de maatregelen die moeten worden genomen in verband met de gesignaleerde persoon of het gesignaleerde voorwerp. Het SIS wordt meestal gebruikt bij politie-, grens- en douanecontroles en door visum- en immigratieautoriteiten bij standaardprocedures en -controles.

Het Prüm-kader omvat daarentegen geen centrale componenten of databanken op EU-niveau en wordt alleen gebruikt bij strafrechtelijke onderzoeken. Andere lidstaten krijgen toegang tot geanonimiseerde subgroepen van de nationale strafrechtelijke DNA-databanken en vingerafdruk-databanken van alle verbonden lidstaten. Toegang wordt uitsluitend verleend aan nationale contactpunten. Hoewel de hit/no-hitrespons binnen enkele seconden of minuten wordt verstrekt, kan het weken of zelfs maanden duren om de overeenkomstige persoonsgegevens met betrekking tot de hit te ontvangen.

¹¹ Het SIS helpt de bevoegde instanties in de EU de interne veiligheid te waarborgen nu er geen controles aan de binnengrenzen meer plaatsvinden. Het VIS biedt de Schengenstaten de mogelijkheid om visumgegevens uit te wisselen. Het Eurodac-systeem omvat een EU-vingerafdruk-databank voor asielzaken, waarmee de lidstaten de vingerafdrukken van asielzoekers kunnen vergelijken om na te gaan of betrokkenen eerder asiel hebben aangevraagd of de EU op irreguliere wijze via een andere lidstaat zijn binnengekomen.

¹² Het EES en het Etias hebben tot doel de veiligheidscontroles van niet-visumplichtige reizigers te verscherpen door deze reizigers vooraf te controleren op risico's in verband met irreguliere migratie en veiligheid. Ecris-TCN moet de geconstateerde lacune in de informatie-uitwisseling tussen de lidstaten met betrekking tot veroordeelde onderdanen van derde landen aanpakken.

¹³ Verordening (EU) 2019/817 en Verordening (EU) 2019/818.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• **Rechtsgrondslag**

De rechtsgrondslag van dit voorstel voor een verordening wordt gevormd door artikel 16, lid 2, artikel 87, lid 2, punt a), en artikel 88, lid 2, van het Verdrag betreffende de werking van de Europese Unie (VWEU).

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 87, lid 2, punt a), VWEU beschikt de Unie over de bevoegdheid om voorschriften vast te stellen voor de verzameling, opslag, verwerking, analyse en uitwisseling van relevante informatie met het oog op de politieke samenwerking tussen de bevoegde instanties van de lidstaten, waaronder de politie, de douane en andere gespecialiseerde handhavingsdiensten, met betrekking tot het voorkomen, opsporen en onderzoeken van strafbare feiten. Krachtens artikel 88, lid 2, kunnen het Europees Parlement en de Raad de structuur, de werking, het werkterrein en de taken van Europol vaststellen.

• **Subsidiariteit**

Gezien het grensoverschrijdende karakter van misdaadbestrijding en veiligheidskwesties kan de verbetering van de informatie-uitwisseling tussen politie- en rechtshandavingsinstanties binnen de EU niet voldoende door de lidstaten afzonderlijk worden verwezenlijkt. De lidstaten moeten in dit verband een beroep doen op elkaar.

Via verschillende uitvoeringsprojecten op EU-niveau¹⁴ hebben de lidstaten gepoogd actie te ondernemen om de tekortkomingen van het huidige Prüm-kader aan te pakken¹⁵. Desondanks konden veel van de tekortkomingen die waren beschreven in het verslag van 2012 over de uitvoering van het Prüm-besluit¹⁶, niet worden verholpen. De EU moet derhalve in actie komen, aangezien de maatregelen die door de lidstaten alleen worden uitgevoerd, niet voldoende zijn gebleken om de beperkingen van het huidige Prüm-kader aan te pakken.

Bovendien vergemakkelijken gemeenschappelijke regels, normen en vereisten op EU-niveau de uitwisseling van informatie en zorgen zij voor compatibiliteit tussen de verschillende nationale systemen. Dit maakt weer een zekere mate van automatisering bij de uitwisseling van informatie mogelijk, waardoor rechtshandavingsfunctionarissen allerlei arbeidsintensieve handmatige werkzaamheden uit handen worden genomen.

¹⁴ Bijvoorbeeld het project Mobile Competence Team (MCT) (2011-2014), geïnitieerd door Duitsland en gefinancierd via het programma “Preventie en bestrijding van criminaliteit” (ISEC) van de Commissie. Het MCT was bedoeld om expertise en ondersteuning te bieden aan EU-lidstaten die nog niet operationeel waren wat betreft de uitwisseling van DNA- en vingerafdrukgegevens.

¹⁵ In het kader van een project onder leiding van Finland hebben de lidstaten een analyse verricht van de nationale procedures die na een hit werden toegepast. Naar aanleiding daarvan is een reeks goede, facultatieve werkwijzen aanbevolen om de uitwisseling van informatie na een hit in de hele EU te stroomlijnen (zie document 14310/2/16 REV 2, niet openbaar).

Ook heeft Europol in 2012-2013 steun verleend aan de ontwikkeling van standaardformulieren voor vervolginformatie-uitwisseling, onafhankelijk van het gebruikte communicatiekanaal (zie document 9383/13 voor meer informatie). Het is echter niet bekend in hoeverre de nationale contactpunten van deze formulieren gebruikmaken.

¹⁶ COM(2012) 732 final.

- **Evenredigheid**

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

Het voorstel voorziet in het opzetten van **centrale routers**, de Prüm II-router en Epris, die elk als verbindingspunt tussen de lidstaten fungeren. Het gaat hier om een hybride aanpak die het midden houdt tussen een gedecentraliseerde en een gecentraliseerde oplossing, waarbij geen gegevens op centraal niveau worden opgeslagen. Dit houdt in dat alle nationale databanken in elke lidstaat worden verbonden met de centrale router in plaats van met elkaar. De routers fungeren als “message brokers” die zoektransacties en antwoorden naar de nationale systemen doorsturen, zonder nieuwe dataprocessen te creëren, toegangsrechten uit te breiden of nationale databanken te vervangen. Deze aanpak zorgt ervoor dat de rechtshandavingsinstanties snel en gecontroleerd toegang hebben tot de informatie die zij nodig hebben om hun taken uit te voeren, in overeenstemming met hun toegangsrechten. De router maakt het voor de lidstaten gemakkelijker om via het Prümkader bestaande en toekomstige gegevensuitwisselingen uit te voeren.

Geautomatiseerde uitwisseling van aanvullende gegevenscategorieën, zoals gezichtsopnamen en politiegegevens, is cruciaal voor het uitvoeren van doeltreffend strafrechtelijk onderzoek en voor het identificeren van criminelen. Het in gebruik nemen van deze aanvullende gegevenscategorieën leidt er niet toe dat nieuwe categorieën gegevens worden opgeslagen, aangezien de lidstaten deze reeds op grond van hun nationale wetgeving verzamelen en in nationale databanken opslaan. Het uitwisselen van deze nieuwe gegevenscategorieën vormt een nieuwe verwerking van gegevens. Deze verwerking blijft echter beperkt tot wat nodig is om het beoogde doel te bereiken en maakt slechts in individuele situaties een vergelijking van gegevens mogelijk. Het voorstel voorziet ook in een aantal waarborgen (volledige gegevens worden bijvoorbeeld alleen gedeeld als een zoekopdracht tot een “hit” leidt).

Dit voorstel maakt **Europol** tot een integrerend onderdeel van het Prümkader, allereerst door de lidstaten in staat te stellen om biometrische gegevens uit derde landen waarover Europol beschikt, automatisch te raadplegen. Ten tweede kan Europol ook gegevens uit derde landen vergelijken met die in de nationale databanken van de lidstaten. Deze twee aspecten van de betrokkenheid van Europol bij het nieuwe Prümkader, overeenkomstig de in Verordening (EU) 2016/794 vastgelegde taken van Europol, zorgen ervoor dat er geen lacunes zijn wat betreft de gegevens over zware criminaliteit en terrorisme die van derde landen worden ontvangen. In een open samenleving in een geglobaliseerde wereld zijn door derde landen verstrekte gegevens over criminelen en terroristen van essentieel belang. Dergelijke gegevens maken identificatie mogelijk van criminelen die bekend zijn bij landen buiten de EU, terwijl tegelijkertijd krachtige waarborgen worden geboden voor de bescherming van de privacy, de grondrechten en de fundamentele vrijheden van personen zoals die zijn vastgelegd in de samenwerkingsovereenkomsten die Europol met derde landen heeft gesloten.

Het herziene proces voor **gegevensuitwisseling na een hit** draagt bij tot de binnenlandse veiligheid in de Europese Unie door de uitwisseling van rechtshandavingsinformatie te vereenvoudigen en te stroomlijnen. In vergelijking met de huidige situatie, waarin het uitwisselen van informatie na een hit door het nationale recht wordt geregeld en dus aan verschillende regels en procedures is onderworpen, bieden gemeenschappelijke regels ter harmonisering van deze tweede stap van het Prümproces voorspelbaarheid voor alle gebruikers, aangezien zij allemaal weten welke gegevens zij in deze stap krijgen. Uitwisseling van gegevens wordt vergemakkelijkt door deze gedeeltelijk te automatiseren, wat betekent dat nog menselijke interventie nodig is voordat een uitgebreide vervolguutwisseling van gegevens kan plaatsvinden. De lidstaten blijven eigenaar van hun gegevens en behouden de controle erover.

- **Keuze van het instrument**

Het voorgestelde instrument is een verordening van het Europees Parlement en de Raad. De voorgestelde wetgeving bouwt voort op een bestaand kader van Raadsbesluiten die bijdragen tot de grensoverschrijdende samenwerking tussen EU-lidstaten op het gebied van justitie en binnenlandse zaken¹⁷.

De voorgestelde maatregelen moeten rechtstreeks toepasselijk zijn en uniform in alle lidstaten worden toegepast, en bovendien moet de uitwisseling van informatie worden verbeterd. Een verordening is daarom de juiste keuze voor het rechtsinstrument.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- **Ex-postevaluatie van bestaande wetgeving**

Over het geheel genomen heeft de evaluatie van het Prüm-kader¹⁸ uitgewezen dat het doorzoeken en vergelijken van DNA-gegevens, vingerafdrukgegevens en voertuigregistratiegegevens in databanken van andere lidstaten met het oog op het voorkomen en onderzoeken van strafbare feiten van het allergrootste belang is voor de bescherming van de binnenlandse veiligheid in de EU en de veiligheid van de burgers. Uit de evaluatie is verder gebleken dat de Prüm-besluiten hebben bijgedragen tot de totstandkoming van gemeenschappelijke regels, normen en vereisten op EU-niveau, waardoor de uitwisseling van informatie is vergemakkelijkt en gezorgd is voor compatibiliteit tussen de verschillende nationale systemen.

Sinds het verstrijken van de termijn voor de uitvoering van het Prüm-kader tien jaar geleden heeft de EU echter diverse andere maatregelen genomen om de uitwisseling van informatie tussen rechtshandavingsinstanties te vergemakkelijken¹⁹, waaronder het interoperabiliteitskader²⁰. Bovendien zijn de bepalingen inzake de technische specificaties van zoekopdrachten, beveiligingsmaatregelen en communicatie sinds de vaststelling van de Prüm-besluiten in 2008²¹ niet geactualiseerd. Sommige van deze bepalingen zijn achterhaald door de aanzienlijke ontwikkeling van de afgelopen tien jaar op het gebied van de forensische wetenschap en technologie.

¹⁷ Besluit 2008/615/JBZ van de Raad inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit en Besluit 2008/616/JBZ van de Raad betreffende de uitvoering van Besluit 2008/615/JBZ.

¹⁸ Bijlage 4 bij het begeleidende werkdocument van de diensten van de Commissie [verwijzing naar de Prüm-effectbeoordeling].

¹⁹ Zoals het Europolinformatiesysteem (EIS), de informatiesystemen van Interpol en het Schengeninformatiesysteem (SIS).

²⁰ Verordening (EU) 2019/817 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van grenzen en visa en tot wijziging van Verordeningen (EG) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 en (EU) 2018/1861 van het Europees Parlement en de Raad, Beschikking 2004/512/EG van de Raad en Besluit 2008/633/JBZ van de Raad;

Verordening (EU) 2019/818 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van politieke en justitiële samenwerking, asiel en migratie en tot wijziging van Verordeningen (EU) 2018/1726, (EU) 2018/1862 en (EU) 2019/816.

²¹ Opgenomen in Besluit 2008/616/JBZ van de Raad.

Uit de evaluatie is ook gebleken dat de Prüm-besluiten de afgelopen tien jaar traag ten uitvoer zijn gelegd en dat niet alle lidstaten de nodige stappen hebben ondernomen om de besluiten uit te voeren²². Daardoor is een aantal bilaterale verbindingen niet tot stand gebracht en kunnen er geen zoekopdrachten worden gestart naar gegevens in de databanken van sommige lidstaten. De bevindingen van de evaluatie wijzen ook uit dat de follow-up van hits plaatsvindt op basis van het nationale recht en derhalve buiten de werkingssfeer van de Prüm-besluiten valt. Door verschillen tussen de nationale regels en procedures kan het voor de bevoegde autoriteiten in heel wat gevallen aanzienlijke tijd kosten om informatie te ontvangen na een hit. Deze stand van zaken heeft gevolgen voor de werking van het Prüm-systeem en voor de doeltreffende uitwisseling van informatie tussen de lidstaten, doordat het identificeren van criminelen en het opsporen van grensoverschrijdende verbanden tussen misdrijven wordt bemoeilijkt.

De bevindingen van de evaluatie ondersteunden de opstelling van de effectbeoordeling en van dit voorstel.

- **Raadpleging van belanghebbenden**

Ter voorbereiding van dit voorstel zijn gerichte raadplegingen uitgevoerd van de belanghebbenden, onder wie eindgebruikers van het systeem. Dit zijn de lidstatelijke instanties die gebruikmaken van de geautomatiseerde uitwisseling van gegevens binnen het Prüm-kader, variërend van rechtshandavingsinstanties, gerechtelijke instanties en nationale voertuigregistratie-instanties tot nationale databankbeheerders en forensische laboratoria. Ook Europol en eu-LISA zijn geraadpleegd in het licht van hun respectieve deskundigheid en hun potentiële rol in het nieuwe Prüm-kader.

Het Bureau voor de grondrechten en niet-gouvernementele organisaties zoals EDRi (Europese digitale rechten) en intergouvernementele organisaties (Eucaris – Europees voertuig- en rijbewijisinformatiesysteem) hebben eveneens input geleverd in het licht van hun deskundigheid.

Bij raadplegingsactiviteiten in het kader van de voorbereiding van de effectbeoordeling die aan dit voorstel ten grondslag ligt, is feedback van belanghebbenden verzameld in verschillende fora. Deze activiteiten omvatten met name een aanvangseffectbeoordeling, een openbare raadpleging en een reeks technische workshops. Er is een haalbaarheidsstudie uitgevoerd op basis van documentair onderzoek, gesprekken met deskundigen op het betrokken gebied, vragenlijsten en drie workshops met deskundigen, en er is onderzoek gedaan naar de haalbaarheid van verbetering van de informatie-uitwisseling binnen het kader van de Prüm-besluiten.

Regelmatige besprekingen in de Groep DAPIX/IXIM²³ van de Raad over de uitwisseling van rechtshandavingsinformatie en met name over de Prüm-besluiten hebben ook bijgedragen tot de voorbereiding van dit voorstel.

Op de **aanvangseffectbeoordeling** kon feedback worden gegeven van augustus tot oktober 2020. Er werden in totaal zes bijdragen ontvangen²⁴.

Een publieksgerichte **openbare raadpleging** is gepubliceerd op de website van de Europese Commissie. De antwoorden bevestigden dat het bestaande Prüm-kader relevant is voor de preventie en het onderzoek van strafbare feiten en dat het de uitwisseling van gegevens tussen de rechtshandavingsinstanties van de lidstaten heeft verbeterd. Door te voorkomen dat elke lidstaat

²² Tegen vijf lidstaten heeft de Commissie in 2016 al een inbreukprocedure geopend. In oktober 2021 liepen twee van deze inbreukprocedures nog.

²³ Groep informatie-uitwisseling en gegevensbescherming (DAPIX) van de Raad, en vanaf 1 januari 2020 de Groep informatie-uitwisseling en binnenlandse zaken (IXIM).

²⁴ De aanvangseffectbeoordeling en de bijdragen zijn [hier](#) te vinden.

bilateraal moet worden geraadpleegd, heeft de geautomatiseerde uitwisseling van gegevens binnen het Prüm-kader ook efficiëntiewinst opgeleverd. De antwoorden bevestigden voorts dat het kader in overeenstemming is met de EU-maatregelen en internationale activiteiten op dit gebied, en dat het een toegevoegde waarde heeft ten opzichte van wat de lidstaten zouden kunnen bereiken op het gebied van de uitwisseling van rechtshandavingsinformatie buiten het Prüm-kader. Wat de versterking van het huidige kader betreft, waren de meeste respondenten het erover eens dat het een probleem is dat sommige gegevenscategorieën niet onder het kader vallen en daarom moeten worden uitgewisseld door middel van handmatige zoekopdrachten.

De diensten van de Commissie hebben verder een reeks gerichte informele **technische workshops** georganiseerd met deskundigen uit de lidstaten en de geassocieerde Schengenlanden. De workshops waren bedoeld om eindgebruikers de gelegenheid te geven van gedachten te wisselen over de opties die werden overwogen en beoordeeld om het Prüm-kader uit technisch oogpunt te versterken.

De bijgevoegde effectbeoordeling (bijlage 2) bevat een uitvoerigere beschrijving van de raadpleging van belanghebbenden.

- **Effectbeoordeling**

Dit voorstel wordt ondersteund door een effectbeoordeling, die is opgenomen in het begeleidende werkdocument van de diensten van de Commissie [verwijzing naar effectbeoordeling Prüm]. De Raad voor regelgevingstoetsing heeft de ontwerp-effectbeoordeling op 14 juli 2021 geëvalueerd en op 16 juli 2021 een gunstig advies uitgebracht.

De conclusie van de effectbeoordeling luidde als volgt:

- 1) Ter verwezenlijking van de doelstelling dat een technische oplossing wordt geboden voor efficiënte geautomatiseerde uitwisseling van gegevens, moet een hybride oplossing worden toegepast die het midden houdt tussen een gedecentraliseerde en een gecentraliseerde aanpak, waarbij geen gegevens op centraal niveau worden opgeslagen.
- 2) Ter verwezenlijking van de doelstelling dat meer relevante gegevens (in termen van gegevenscategorieën) beschikbaar zijn voor rechtshandavingsinstanties, moet worden voorzien in uitwisseling van gezichtsopnamen en politiegegevens.
- 3) Ter verwezenlijking van de doelstelling dat relevante gegevens uit de databanken van Europol beschikbaar zijn voor de rechtshandavingsinstanties, moeten de lidstaten binnen het Prüm-kader automatisch biometrische gegevens van derde landen die bij Europol beschikbaar zijn, kunnen controleren. Europol moet ook in staat worden gesteld gegevens uit derde landen te vergelijken met die in de nationale databanken van de lidstaten.
- 4) Ter verwezenlijking van de doelstelling dat efficiënte toegang wordt geboden tot met een “hit” overeenstemmende feitelijke gegevens die beschikbaar zijn in de nationale databank van een andere lidstaat of bij Europol, moet het follow-upproces op EU-niveau worden geregeld in de vorm van semiautomatische uitwisseling van die feitelijke gegevens.

Het belangrijkste positieve effect van dit voorstel zal zijn dat de vastgestelde problemen doeltreffend worden aangepakt en dat het huidige Prüm-kader wordt versterkt met krachtige gerichte aanvullende vermogens voor betere steunverlening aan de lidstaten, en wel door verbetering van de informatie-uitwisseling, met als einddoel dat strafbare feiten en terroristische misdrijven worden voorkomen en onderzocht met volledige inachtneming van de grondrechten.

De uiteindelijke begunstigden van alle voorkeursopties zijn de burgers, die direct en indirect baat zullen hebben bij betere misdaadbestrijding en minder criminaliteit. Wat efficiëntie betreft, zijn de belangrijkste begunstigden de nationale rechtshandavingsinstanties.

De onmiddellijke financiële en economische gevolgen van het voorstel vereisen investeringen op het niveau van zowel de EU als de lidstaten. Er wordt verwacht dat de geraamde investeringskosten zullen worden gecompenseerd door voordelen en besparingen, met name op het niveau van de lidstaten. Ondanks de initiële investeringen zal de invoering van de centrale Prümrouter kosten besparen voor de lidstaten, aangezien de router het overbodig maakt dat elke lidstaat evenveel verbindingen tot stand brengt (en in stand houdt) als er lidstaten en gegevenscategorieën zijn.

- **Grondrechten**

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), en overeenkomstig het discriminatieverbod moet een balans worden gevonden tussen enerzijds de kansen die de aangeboden opties bieden en anderzijds de verplichting om te waarborgen dat iedere inmenging in de grondrechten die daaruit kan voortvloeien, beperkt blijft tot hetgeen strikt noodzakelijk is om daadwerkelijk te beantwoorden aan de nagestreefde doelstellingen van algemeen belang, met inachtneming van het evenredigheidsbeginsel (artikel 52, 1, van het Handvest).

De voorgestelde oplossingen bieden de kans om gerichte preventieve maatregelen vast te stellen ter verbetering van de veiligheid. Zo kunnen zij bijdragen tot het legitieme doel van facilitering van de misdaadbestrijding, dat voor de autoriteiten de positieve verplichting inhoudt om preventieve operationele maatregelen te treffen ter bescherming van een natuurlijke persoon wiens leven in gevaar is, als zij weet hebben of gehad zouden moeten hebben van een directe dreiging²⁵.

- **Bescherming van persoonsgegevens**

Uitwisseling van informatie heeft gevolgen 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 beklemtoond²⁶, heeft het recht op bescherming van persoonsgegevens geen absolute gelding, maar moet het in relatie tot de functie ervan in de maatschappij worden beschouwd. Er is 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.

Wat het Prümkader betreft, is Richtlijn (EU) 2016/680 de toepasselijke gegevensbeschermingswetgeving. Het Prümkader voorziet namelijk in de verwerking van persoonsgegevens in het kader van de uitwisseling van informatie tussen rechtshandhavinginstanties die belast zijn met het voorkomen en onderzoeken van strafbare feiten.

Het vrije verkeer van gegevens in de Unie mag niet worden beperkt om redenen die verband houden met gegevensbescherming. Er moeten echter wel enkele beginselen worden nageleefd. 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:

- 1) de beperkingen moeten bij wet worden gesteld;
- 2) zij moeten de wezenlijke inhoud van de rechten eerbiedigen;

²⁵ Europees Hof voor de Rechten van de Mens, *Osman/Verenigd Koninkrijk*, nr. 87/1997/871/1083 van 28 oktober 1998, punt 116.

²⁶ Arrest van het Hof van Justitie van de EU van 9.11.2010, *Volker und Markus Schecke en Eifert*, C-92/09 en C-93/09, ECLI:EU:C:2010:662.

- 3) zij moeten 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;
- 4) zij moeten noodzakelijk zijn; en
- 5) zij moeten evenredig zijn.

In dit voorstel zijn al deze gegevensbeschermingsregels geïntegreerd, zoals 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 aan entiteiten die er kennis van moeten nemen. De toegang is voorbehouden aan uitsluitend de naar behoren gemachtigde personeelsleden van de lidstatelijke instanties en de EU-organen die bevoegd zijn voor de specifieke doeleinden van het herziene Prüm-kader, en geldt enkel voor de gegevens die vereist zijn voor de uitvoering van hun taken overeenkomstig deze doeleinden.

De Commissie zal bij de publicatie van het verslag over de beoordeling van het gevolg dat aan de [aanbeveling van de Raad inzake operationele politieke samenwerking] is gegeven door de in punt 9, d), van die aanbeveling bedoelde lidstaten, beslissen of er EU-wetgeving inzake grensoverschrijdende operationele politieke samenwerking nodig is. Is dat het geval, dan zal de Commissie een wetgevingsvoorstel betreffende grensoverschrijdende operationele politieke samenwerking indienen, dat er tevens voor zal zorgen dat de bepalingen van Besluit 2008/615/JBZ en Besluit 2008/616/JBZ die niet onder dit voorstel vallen, in overeenstemming worden gebracht met Richtlijn (EU) 2016/680, overeenkomstig de resultaten van de beoordeling uit hoofde van artikel 62, lid 6, van Richtlijn (EU) 2016/680. Mocht EU-wetgeving inzake grensoverschrijdende operationele politieke samenwerking niet nodig zijn, dan zal de Commissie een wetgevingsvoorstel indienen om de bedoelde bepalingen aan te passen, overeenkomstig de resultaten van de beoordeling uit hoofde van artikel 62, lid 6, van Richtlijn 2016/680.

4. GEVOLGEN VOOR DE BEGROTING

Dit wetgevingsinitiatief leidt tot gevolgen voor de begroting en de personeelsbehoeften van eu-LISA en Europol.

Wat eu-LISA betreft, zullen voor de totale MFK-periode naar schatting extra begrotingsmiddelen van ongeveer 16 miljoen EUR en ongeveer 10 extra posten nodig zijn om te waarborgen dat eu-LISA over de nodige middelen beschikt om de in deze voorgestelde verordening aan dat agentschap toegewezen taken te kunnen uitvoeren. Het aan eu-LISA toegewezen budget zal worden verrekend met het instrument voor financiële steun voor grensbeheer en visa.

Wat Europol betreft, zullen voor de totale MFK-periode naar schatting extra begrotingsmiddelen van ongeveer 7 miljoen EUR en ongeveer 5 extra posten nodig zijn om te waarborgen dat Europol over de nodige middelen beschikt om de in deze voorgestelde verordening aan dat agentschap toegewezen taken te kunnen uitvoeren. Het aan Europol toegewezen budget zal worden verrekend met het Fonds voor interne veiligheid.

5. OVERIGE ELEMENTEN

• **Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage**

De Commissie zal ervoor zorgen dat de nodige regelingen zijn getroffen om de werking van de voorgestelde maatregelen te monitoren en aan de belangrijkste beleidsdoelstellingen te toetsen. Twee jaar na de invoering en operationalisering van de nieuwe functies, en vervolgens om de twee jaar, moeten EU-agentschappen aan het Europees Parlement, de Raad en de Commissie een verslag voorleggen over de technische werking van de voorgestelde nieuwe maatregelen. Daarnaast verricht de Commissie drie jaar na de invoering en operationalisering van de nieuwe functies een algemene evaluatie van de maatregelen, waarbij ook wordt stilgestaan bij de eventuele directe en indirecte gevolgen voor de grondrechten. Zij toetst de behaalde resultaten aan de doelstellingen en beoordeelt de onverminderde geldigheid van de uitgangspunten alsook de implicaties voor toekomstige opties. De Commissie legt de evaluatieverslagen aan het Europees Parlement en de Raad voor.

• **Artikelsgewijze toelichting**

Hoofdstuk 1 bevat de algemene bepalingen van deze verordening met betrekking tot onderwerp, doel en toepassingsgebied. Het bevat een lijst van definities en wijst erop dat bij de verwerking van persoonsgegevens voor de toepassing van de verordening het beginsel van non-discriminatie en andere grondrechten in acht moeten worden genomen.

Hoofdstuk 2 bevat bepalingen betreffende de categorieën gegevens die uit hoofde van deze verordening worden uitgewisseld, dat wil zeggen DNA-profielen, dactyloscopische gegevens, voertuigregistratiegegevens, gezichtsopnamen en politiedossiers. De beginselen voor de uitwisseling en de geautomatiseerde opvraging van gegevens, en de regels voor verzoeken en antwoorden worden voor elke categorie gegevens afzonderlijk beschreven. Hoofdstuk 2 bevat tevens gemeenschappelijke bepalingen inzake het uitwisselen van gegevens en het opzetten van nationale contactpunten en uitvoeringsmaatregelen.

Hoofdstuk 3 bevat de details voor de nieuwe (technische) architectuur voor de uitwisseling van gegevens. In afdeling 1 van dit hoofdstuk zijn bepalingen opgenomen over de centrale router, het gebruik van de router en het starten van zoekopdrachten. Er zullen uitvoeringshandelingen moeten worden vastgesteld om de technische procedures voor deze zoekopdrachten te specificeren. Deze afdeling bevat tevens bepalingen over de interoperabiliteit tussen de router en het gemeenschappelijk identiteitsregister met het oog op de toegang voor rechtshandavingsdoeleinden, het bijhouden van logbestanden van alle gegevensverwerkingsactiviteiten in de router, de kwaliteitscontrole en de kennisgevingsprocedures die van toepassing zijn als de router door een technische storing niet kan worden gebruikt. In afdeling 2 staan nadere bepalingen over het gebruik van het Europees Indexsysteem van politiegegevens (Epris) voor het uitwisselen van politiegegevens. In deze afdeling staan ook bepalingen over het bijhouden van logbestanden van alle gegevensverwerkingsactiviteiten in Epris en de kennisgevingsprocedures die van toepassing zijn als Epris door een technische storing niet kan worden gebruikt.

Hoofdstuk 4 beschrijft de processen voor de uitwisseling van gegevens naar aanleiding van een match. Het bevat een bepaling over de geautomatiseerde uitwisseling van kerngegevens, waarbij de gegevens beperkt blijven tot hetgeen nodig is om de betrokken persoon te identificeren, en een bepaling over de uitwisseling van gegevens in niet uitdrukkelijk in de verordening beschreven stadia van het proces uit hoofde van deze verordening.

Hoofdstuk 5 bevat bepalingen over de toegang van de lidstaten tot uit derde landen afkomstige biometrische gegevens die bij Europol zijn opgeslagen en over de toegang van Europol tot gegevens die in de databanken van de lidstaten zijn opgeslagen.

Hoofdstuk 6 over gegevensbescherming bevat bepalingen die waarborgen dat gegevens uit hoofde van deze verordening rechtmatig en op gepaste wijze worden verwerkt, met inachtneming van de bepalingen van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad²⁷. Er wordt in uiteengezet wie bij de verwerking van gegevens uit hoofde van deze verordening de gegevensverwerker is. Voorts wordt uiteengezet welke maatregelen eu-LISA en de lidstatelijke instanties moeten nemen om de beveiliging van de gegevensverwerking, de passende behandeling van beveiligingsincidenten en het toezicht op de naleving van de maatregelen van deze verordening te waarborgen. Ten slotte staan in het hoofdstuk bepalingen over toezicht en audit met betrekking tot gegevensbescherming. Het beginsel dat gegevens die uit hoofde van deze verordening worden verwerkt, niet op geautomatiseerde wijze aan derde landen of internationale organisaties mogen worden doorgegeven of ter beschikking gesteld.

Hoofdstuk 7 beschrijft de taken van de lidstaten, Europol en eu-LISA bij de uitvoering van de maatregelen uit hoofde van deze verordening.

Hoofdstuk 8 betreft wijzigingen van andere reeds bestaande instrumenten, te weten Besluit 2008/615/JBZ, Besluit 2008/616/JBZ, Verordening (EU) 2018/1726, Verordening (EU) 2019/817 en Verordening (EU) 2019/818.

Hoofdstuk 9 bevat slotbepalingen op het gebied van verslagen en statistieken, kosten, kennisgevingen, overgangsbepalingen en afwijkingen. Het beschrijft de vereisten voor het opstarten van de bij deze verordening voorgestelde activiteiten. Het hoofdstuk voorziet ook in de instelling van een comité en de vaststelling van een praktische handleiding ter ondersteuning van de uitvoering en het beheer van deze verordening. Het bevat voorts een bepaling over monitoring en evaluatie en een bepaling over de inwerkingtreding en de toepasselijkheid van deze verordening. Deze verordening vervangt met name de artikelen 2 tot en met 6 en de afdelingen 2 en 3 van hoofdstuk 2 van Besluit 2008/615/JBZ van de Raad alsmede de hoofdstukken 2 tot en met 5 en de artikelen 18, 20 en 21 van Besluit 2008/616/JBZ van de Raad, die bijgevolg vanaf de datum van toepassing van deze verordening uit die besluiten van de Raad zullen worden geschrapt. Als gevolg van deze wijzigingen zullen de vervangen en geschrapte bepalingen niet langer op enige lidstaat van toepassing zijn.

²⁷ In overeenstemming met de bevindingen van de Commissie in haar mededeling van 24 juni 2020 “Volgende stappen om het acquis van de voormalige derde pijler aan de gegevensbeschermingsregels aan te passen”, COM(2020) 262 final.

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende geautomatiseerde gegevensuitwisseling ten behoeve van politieke samenwerking (“Prüm II”) en tot wijziging van de Besluiten 2008/615/JBZ en 2008/616/JBZ van de Raad en de Verordeningen (EU) 2018/1726, (EU) 2019/817 en (EU) 2019/818 van het Europees Parlement en de Raad

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 87, lid 2, punt a), en artikel 88, lid 2,

Gezien het voorstel van de Europese Commissie,

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

Gezien het advies van het Europees Economisch en Sociaal Comité²⁸,

Gezien het advies van het Comité van de Regio's²⁹,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

- (1) De Unie heeft zich ten doel gesteld haar burgers een ruimte van vrijheid, veiligheid en recht te bieden zonder binnengrenzen, waarin het vrije verkeer van personen gewaarborgd is. Deze doelstelling moet onder meer bereikt worden door passende maatregelen ter voorkoming en bestrijding van criminaliteit, waaronder georganiseerde misdaad en terrorisme.
- (2) Deze doelstelling vereist dat rechtshandavingsinstanties tijdig en op efficiënte wijze gegevens uitwisselen om criminaliteit doeltreffend te bestrijden.
- (3) Het doel van deze verordening is derhalve de verbetering, stroomlijning en facilitering van de uitwisseling van strafrechtelijke informatie tussen de rechtshandavingsinstanties van de lidstaten, maar ook met het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol), dat bij Verordening (EU) 2016/794 van het Europees Parlement en de Raad³⁰ is opgericht als het informatiecentrum van de Unie over criminaliteit.
- (4) De Besluiten 2008/615/JBZ³¹ en 2008/616/JBZ³² van de Raad, waarbij voorschriften zijn vastgesteld voor de uitwisseling van informatie tussen met de voorkoming en opsporing van

²⁸ PB C van , blz. .

²⁹ PB C van , blz. .

³⁰ 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).

³¹ Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit (PB L 210 van 6.8.2008, blz. 1).

strafbare feiten belaste instanties door middel van de geautomatiseerde overdracht van DNA-profielen, dactyloscopische gegevens en bepaalde gegevens uit de nationale kentekenregisters, zijn van belang gebleken voor de bestrijding van terrorisme en grensoverschrijdende criminaliteit.

- (5) Bij deze verordening moeten de voorwaarden en procedures worden vastgesteld voor de geautomatiseerde overdracht van DNA-profielen, dactyloscopische gegevens, voertuigregistratiegegevens, gezichtsopnamen en politiegegevens. Daarbij mag geen afbreuk worden gedaan aan de verwerking van deze gegevens in het Schengeninformatiesysteem (SIS) of de uitwisseling van daarmee verband houdende aanvullende informatie via de Sirene-bureaus, noch aan de rechten van personen wier gegevens daarin worden verwerkt.
- (6) De verwerking van persoonsgegevens en de uitwisseling van persoonsgegevens voor de toepassing van deze verordening mogen niet leiden tot discriminatie van personen op welke grond dan ook. Bij de verwerking moeten de menselijke waardigheid en integriteit en andere grondrechten ten volle worden geëerbiedigd, met inbegrip van het recht op eerbiediging van het privéleven en de bescherming van persoonsgegevens, zulks overeenkomstig het Handvest van de grondrechten van de Europese Unie.
- (7) Deze verordening voorziet tevens in de geautomatiseerde bevraging of vergelijking van DNA-profielen, dactyloscopische gegevens, voertuigregistratiegegevens, gezichtsopnamen en politiegegevens, teneinde de opsporing van vermiste personen en niet-geïdentificeerde stoffelijke resten mogelijk te maken. Daarbij moet de opneming van SIS-signalerings van vermiste personen en de uitwisseling van aanvullende informatie over dergelijke signaleringen uit hoofde van Verordening (EU) 2018/1862 van het Europees Parlement en de Raad³³ onverlet worden gelaten.
- (8) Richtlijn (EU) .../... [betreffende informatie-uitwisseling tussen de rechtshandavingsinstanties van de lidstaten] biedt een samenhangend Unierechtskader om te waarborgen dat de rechtshandavingsinstanties gelijkwaardige toegang hebben tot informatie die bij andere lidstaten berust, wanneer zij die nodig hebben in de strijd tegen criminaliteit en terrorisme. Om de uitwisseling van informatie te verbeteren, worden in die richtlijn de procedures voor informatie-uitwisseling tussen de lidstaten geformaliseerd en verduidelijkt, met name voor onderzoeksdoeleinden, met inbegrip van de rol van het centrale contactpunt voor dergelijke uitwisselingen, waarbij ten volle gebruik zal worden gemaakt van Siena, het kanaal voor informatie-uitwisseling van Europol. Elke uitwisseling van informatie die verder gaat dan hetgeen in deze verordening is bepaald, moet worden geregeld bij Richtlijn (EU) .../... [betreffende informatie-uitwisseling tussen de rechtshandavingsinstanties van de lidstaten].
- (9) Voor de geautomatiseerde bevraging van voertuigregistratiegegevens moeten de lidstaten gebruikmaken van het daartoe ontworpen Europees voertuig- en rijbewijsinformatiesysteem (Eucaris), dat is opgezet bij het Verdrag betreffende een Europees voertuig- en rijbewijsinformatiesysteem (Eucaris). Eucaris moet alle deelnemende lidstaten in een netwerk

³² Besluit 2008/616/JBZ van de Raad van 23 juni 2008 betreffende de uitvoering van Besluit 2008/615/JBZ inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit (PB L 210 van 6.8.2008, blz. 12).

³³ Verordening (EU) 2018/1862 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politieke en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie (PB L 312 van 7.12.2018, blz. 56).

verbinden. Er is geen centrale component nodig om de communicatie tot stand te brengen, aangezien elke lidstaat rechtstreeks met de andere verbonden lidstaten communiceert.

- (10) De vaststelling van een strafbaar feit is van essentieel belang voor een succesvol strafrechtelijk onderzoek en succesvolle strafvervolgning. De geautomatiseerde bevraging van gezichtsopnamen van verdachten en veroordeelden moet aanvullende informatie opleveren om criminelen met succes te kunnen identificeren en criminaliteit te kunnen bestrijden.
- (11) De geautomatiseerde bevraging of vergelijking van biometrische gegevens (DNA-profielen, dactyloscopische gegevens en gezichtsopnamen) tussen de instanties die belast zijn met het voorkomen, opsporen en onderzoeken van strafbare feiten uit hoofde van deze verordening, mag alleen betrekking hebben op gegevens in databanken die zijn opgezet voor het voorkomen, opsporen en onderzoeken van strafbare feiten.
- (12) De deelname aan de uitwisseling van politiegegevens moet vrijwillig blijven. Wanneer lidstaten besluiten om er in een geest van wederkerigheid aan deel te nemen, mogen zij de databanken van andere lidstaten niet doorzoeken als zij hun eigen gegevens niet beschikbaar stellen voor zoekopdrachten door andere lidstaten.
- (13) Europol heeft de afgelopen jaren van verschillende derde landen een grote hoeveelheid biometrische gegevens ontvangen van verdachte en veroordeelde terroristen en criminelen. Het opnemen van bij Europol opgeslagen gegevens uit derde landen in het Prüm-kader en het beschikbaar stellen van deze gegevens aan rechtshandavingsinstanties is noodzakelijk om strafbare feiten beter te kunnen voorkomen en onderzoeken. Er wordt daardoor ook bijgedragen aan synergieën tussen verschillende rechtshandavingsinstrumenten.
- (14) Europol moet de databanken van de lidstaten binnen het Prüm-kader kunnen doorzoeken aan de hand van gegevens die van derde landen zijn ontvangen, teneinde grensoverschrijdende verbanden tussen strafzaken vast te stellen. Door gebruik te kunnen maken van Prüm-gegevens, naast de andere databanken waarover Europol beschikt, zou het mogelijk moeten zijn een vollediger en beter onderbouwde analyse van het strafrechtelijk onderzoek te verrichten en Europol in staat te stellen de rechtshandavingsinstanties van de lidstaten beter te ondersteunen. Bij een match tussen de voor de bevraging gebruikte gegevens en de gegevens in de databanken van de lidstaten, kunnen de lidstaten Europol de informatie verstrekken die het agentschap nodig heeft om zijn taken te vervullen.
- (15) De Besluiten 2008/615/JBZ en 2008/616/JBZ voorzien in een netwerk van bilaterale verbindingen tussen de nationale databanken van de lidstaten. Het gevolg van deze technische architectuur is dat elke lidstaat ten minste 26 verbindingen tot stand zou moeten brengen, d.w.z. een verbinding met elke lidstaat voor elke gegevenscategorie. Door de router en het Europees Indexsysteem van politiegegevens (Epris) die bij deze verordening worden ingesteld en als verbindingpunten tussen alle lidstaten fungeren, wordt de technische architectuur van het Prüm-kader vereenvoudigd. De router vereist slechts één verbinding per lidstaat voor biometrische gegevens en Epris vereist slechts één verbinding per lidstaat voor politiegegevens.
- (16) De router moet worden aangesloten op het Europees zoekportaal dat is ingesteld bij artikel 6 van Verordening (EU) 2019/817 van het Europees Parlement en de Raad³⁴ en artikel 6 van

³⁴ Verordening (EU) 2019/817 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van grenzen en visa en tot wijziging van Verordeningen (EG) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 en (EU) 2018/1861 van het Europees Parlement en de Raad, Beschikking 2004/512/EG van de Raad en Besluit 2008/633/JBZ van de Raad (PB L 135 van 22.5.2019, blz. 27).

Verordening (EU) 2019/818 van het Europees Parlement en de Raad³⁵, teneinde de lidstatelijke instanties en Europol in staat te stellen tegelijkertijd zoekopdrachten te starten in zowel de nationale databanken uit hoofde van deze verordening als het gemeenschappelijk identiteitsregister dat is ingesteld bij artikel 17 van Verordening (EU) 2019/817 en artikel 17 van Verordening (EU) 2019/818 voor rechtshandavingsdoeleinden.

- (17) Bij een match tussen de voor de bevraging of vergelijking gebruikte gegevens en de gegevens in de nationale databanken van de aangezochte lidstaat of lidstaten en na bevestiging van deze match door de verzoekende lidstaat, moet door de aangezochte lidstaat of lidstaten binnen 24 uur via de router een beperkte reeks kerngegevens worden teruggezonden. Deze termijn moet zorgen voor een snelle uitwisseling van communicatie tussen de lidstatelijke instanties. De lidstaten moeten de controle behouden over de vrijgave van deze beperkte reeks kerngegevens. Op cruciale punten in het proces moet een zekere mate van menselijke tussenkomst behouden blijven, onder meer wat betreft het besluit om persoonsgegevens te verstrekken aan de verzoekende lidstaat, teneinde te waarborgen dat er geen geautomatiseerde uitwisseling van kerngegevens plaatsvindt.
- (18) Alle niet uitdrukkelijk in deze verordening beschreven uitwisselingen tussen de lidstatelijke instanties of met Europol, in elk stadium van een van de in deze verordening beschreven processen, moeten via Siena plaatsvinden, teneinde te waarborgen dat alle lidstaten gebruikmaken van een gemeenschappelijk, beveiligd en betrouwbaar communicatiekanaal.
- (19) Bij de ontwikkeling van de router en Epris moet gebruik worden gemaakt van de norm inzake het Universal Message Format (UMF). Bij elke geautomatiseerde uitwisseling van gegevens overeenkomstig deze verordening moet gebruik worden gemaakt van de UMF-norm. De lidstatelijke instanties en Europol worden aangemoedigd de UMF-norm ook te gebruiken voor alle verdere uitwisselingen van gegevens tussen hen onderling in de context van het Prüm II-kader. Het UMF moet als norm gelden voor de gestructureerde, grensoverschrijdende informatie-uitwisseling tussen informatiesystemen, instanties en organisaties op het gebied van justitie en binnenlandse zaken.
- (20) Via het Prüm II-kader mag uitsluitend niet-gerubriceerde informatie worden uitgewisseld.
- (21) Bepaalde aspecten van het Prüm II-kader kunnen vanwege hun technische, gedetailleerde en sterk veranderlijke aard niet uitputtend in deze verordening worden geregeld. Deze aspecten omvatten bijvoorbeeld technische regelingen en specificaties voor geautomatiseerde bevragingsprocedures, de normen voor gegevensuitwisseling en de uit te wisselen gegevenselementen. Teneinde eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad³⁶.
- (22) Aangezien deze verordening voorziet in de instelling van het nieuwe Prümkader, moeten de desbetreffende bepalingen van Besluit 2008/615/JBZ en Besluit 2008/616/JBZ worden geschrapt. Die besluiten moeten derhalve dienovereenkomstig worden gewijzigd.

³⁵ Verordening (EU) 2019/818 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van politieke en justitiële samenwerking, asiel en migratie en tot wijziging van Verordeningen (EU) 2018/1726, (EU) 2018/1862 en (EU) 2019/816 (PB L 135 van 22.5.2019, blz. 85).

³⁶ 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).

- (23) Aangezien de router moet worden ontwikkeld en beheerd door het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige informatiesystemen op het gebied van vrijheid, veiligheid en recht, dat is opgericht bij Verordening (EU) 2018/1726 van het Europees Parlement en de Raad³⁷ (eu-LISA), moet Verordening (EU) 2018/1726 worden gewijzigd door de desbetreffende taken aan de taken van eu-LISA toe te voegen. Om ervoor te zorgen dat de router kan worden aangesloten op het Europees zoekportaal, zodat de router en het gemeenschappelijk identiteitsregister gelijktijdig kunnen worden doorzocht, moet Verordening (EU) 2019/817 worden gewijzigd. Teneinde het mogelijk te maken dat de router op het Europees zoekportaal wordt aangesloten, zodat de router en het gemeenschappelijk identiteitsregister gelijktijdig kunnen worden doorzocht en verslagen en statistieken van de router kunnen worden opgeslagen in het centraal register voor rapportage en statistieken, is het noodzakelijk Verordening (EU) 2019/818 te wijzigen. Deze verordeningen moeten derhalve dienovereenkomstig worden gewijzigd.
- (24) Overeenkomstig de artikelen 1 en 2 van Protocol nr. 22 betreffende de positie van Denemarken, dat aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is gehecht, neemt Denemarken niet deel aan de vaststelling van deze verordening en is deze niet bindend voor, noch van toepassing op die lidstaat.
- (25) [Overeenkomstig artikel 3 van 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, heeft Ierland kennisgegeven van zijn wens deel te nemen aan de vaststelling en toepassing van deze verordening.] OF [Overeenkomstig de artikelen 1 en 2 van 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, en onverminderd artikel 4 van dat protocol, neemt Ierland niet deel aan de vaststelling van deze verordening en is deze niet bindend voor, noch van toepassing op die lidstaat.]
- (26) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad³⁸ en heeft op [XX] advies uitgebracht³⁹.

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK 1

ALGEMENE BEPALINGEN

³⁷ Verordening (EU) 2018/1726 van het Europees Parlement en de Raad van 14 november 2018 betreffende het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA), tot wijziging van Verordening (EG) nr. 1987/2006 en Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EU) nr. 1077/2011 (PB L 295 van 21.11.2018, blz. 99).

³⁸ Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

³⁹ [PB C ...].

Artikel 1

Voorwerp

Bij deze verordening wordt een kader vastgesteld voor de uitwisseling van informatie tussen de instanties die belast zijn met het voorkomen, opsporen en onderzoeken van strafbare feiten (Prüm II).

Bij deze verordening worden de voorwaarden en procedures vastgesteld voor de geautomatiseerde bevraging van DNA-profielen, dactyloscopische gegevens, gezichtsopnamen, politiegegevens en bepaalde voertuigregistratiegegevens, alsmede de regels voor de uitwisseling van kerngegevens na een match.

Artikel 2

Doel

Het doel van Prüm II is de intensivering van grensoverschrijdende samenwerking met betrekking tot aangelegenheden die vallen onder deel III, titel V, hoofdstuk 5, van het Verdrag betreffende de werking van de Europese Unie, en met name de uitwisseling van informatie tussen de instanties die belast zijn met het voorkomen, opsporen en onderzoeken van strafbare feiten.

Prüm II heeft ook tot doel de opsporing van vermiste personen en niet-geïdentificeerde stoffelijke resten mogelijk te maken voor de instanties die belast zijn met het voorkomen, opsporen en onderzoeken van strafbare feiten.

Artikel 3

Toepassingsgebied

Deze verordening is van toepassing op de nationale databanken die worden gebruikt voor de geautomatiseerde overdracht van categorieën van DNA-profielen, dactyloscopische gegevens, gezichtsopnamen, politiegegevens en bepaalde voertuigregistratiegegevens.

Artikel 4

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

- 1) “loci”: de specifieke moleculaire structuur op de verschillende DNA-locaties;
- 2) “DNA-profiel”: een letter- of cijfercode die een set identificatiekenmerken van het niet-coderende gedeelte van een geanalyseerd menselijk DNA-monster vertegenwoordigt, dat wil zeggen de specifieke moleculaire structuur op de verschillende DNA-locaties;
- 3) “niet-coderend gedeelte van DNA”: chromosoomgebieden die geen genetische uitdrukking bevatten, d.w.z. waarvan niet bekend is dat zij voorzien in functionele eigenschappen van een organisme;
- 4) “DNA-referentiegegevens”: een DNA-profiel en het in artikel 9 bedoelde referentienummer;
- 5) “DNA-persoonsprofiel”: het DNA-profiel van een geïdentificeerde persoon;
- 6) “niet-geïdentificeerd DNA-profiel”: een DNA-profiel dat is verkregen uit tijdens het opsporingsonderzoek verzamelde sporen en toebehoort aan een nog niet geïdentificeerde persoon;

- 7) “dactyloscopische gegevens”: beelden van vingerafdrukken, van latente vingerafdrukken, van handpalmafdrukken en van latente handpalmafdrukken, alsook de sjablonen (templates) van die beelden (gecodeerde minutiae), die zijn opgeslagen en verwerkt in een geautomatiseerde databank;
- 8) “dactyloscopische referentiegegevens”: dactyloscopische gegevens en het in artikel 14 bedoelde referentienummer;
- 9) “individueel geval”: één onderzoeksdossier;
- 10) “gezichtsopname”: een digitale afbeelding van het gezicht;
- 11) “biometrische gegevens”: DNA-profielen, dactyloscopische gegevens of gezichtsopnamen;
- 12) “match”: het bestaan van een overeenkomst die aan het licht wordt gebracht door een automatische vergelijking tussen persoonsgegevens die in een informatiesysteem of databank zijn of worden geregistreerd;
- 13) “kandidaat”: gegevens waarmee een match heeft plaatsgevonden;
- 14) “verzoekende lidstaat”: de lidstaat die via Prüm II een zoekopdracht uitvoert;
- 15) “aangezochte lidstaat”: de lidstaat in de databanken waarvan de zoekopdracht van de verzoekende lidstaat wordt uitgevoerd via Prüm II;
- 16) “politiegegevens”: elk gegeven dat beschikbaar is in het nationale register of de nationale registers waarin gegevens van bevoegde autoriteiten worden opgeslagen, met het oog op het voorkomen, opsporen en onderzoeken van strafbare feiten;
- 17) “pseudonimisering”: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer tot een specifieke betrokkene te herleiden zijn zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om te waarborgen dat de persoonsgegevens niet naar een geïdentificeerde of identificeerbare natuurlijke persoon te herleiden zijn;
- 18) “Europolgegevens”: persoonsgegevens die door Europol worden verwerkt overeenkomstig Verordening (EU) 2016/794;
- 19) “toezichthoudende autoriteit”: een door een lidstaat op grond van artikel 41 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad⁴⁰ ingestelde onafhankelijke overheidsinstantie;
- 20) “Siena”: de beveiligde netwerkapplicatie voor informatie-uitwisseling, beheerd door Europol, die tot doel heeft de uitwisseling van informatie tussen de lidstaten en Europol te faciliteren;
- 21) “significant incident”: elk incident, tenzij het een beperkte impact heeft en het waarschijnlijk al goed in kaart is gebracht in termen van methode of technologie;
- 22) “significante cyberdreiging”: een cyberdreiging met de bedoeling, de gelegenheid en het vermogen om een significant incident te veroorzaken;

⁴⁰ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

- 23) “significante kwetsbaarheid”: een kwetsbaarheid die bij exploitatie waarschijnlijk tot een significant incident zal leiden;
- 24) “incident”: een incident in de zin van artikel 4, lid 5, van Richtlijn (EU).../... van het Europees Parlement en de Raad⁴¹ [NIS 2-voorstel].

HOOFDSTUK 2

UITWISSELING VAN GEGEVENS

AFDELING 1

DNA-profielen

Artikel 5

Aanmaken van nationale DNA-analysebestanden

1. De lidstaten maken ter opsporing van strafbare feiten nationale DNA-analysebestanden aan en houden deze bij.

De verwerking van de uit hoofde van deze verordening in deze bestanden opgeslagen gegevens geschiedt behoudens de overige bepalingen van deze verordening, met inachtneming van het voor de verwerking geldende nationale recht.

2. De lidstaten dragen er zorg voor dat DNA-referentiegegevens uit hun nationale DNA-analysebestanden als bedoeld in lid 1 beschikbaar zijn.

DNA-referentiegegevens mogen geen gegevens bevatten waarmee de betrokkene rechtstreeks kan worden geïdentificeerd.

DNA-referentiegegevens die niet op een persoon zijn teruggevoerd (ongeïdentificeerde DNA-profielen), worden als zodanig herkenbaar gemaakt.

Artikel 6

Geautomatiseerde bevraging van DNA-profielen

1. De lidstaten verlenen de in artikel 29 bedoelde nationale contactpunten en Europol toegang tot de DNA-referentiegegevens in hun DNA-analysebestanden met het oog op geautomatiseerde bevraging door vergelijking van DNA-profielen ten behoeve van het onderzoek naar strafbare feiten.

De bevraging mag slechts worden uitgevoerd in individuele gevallen en met inachtneming van het nationale recht van de verzoekende lidstaat.

2. Indien bij een geautomatiseerde bevraging wordt vastgesteld dat een verstrekt DNA-profiel een match vertoont met een in het bestand van de aangezochte lidstaat opgeslagen DNA-profiel, dan ontvangt het nationale contactpunt van de verzoekende lidstaat op geautomatiseerde wijze de DNA-referentiegegevens waarmee een match is vastgesteld.

Indien er geen match is, wordt de verzoekende lidstaat daarvan op geautomatiseerde wijze in kennis gesteld.

⁴¹ Richtlijn (EU) .../... van het Europees Parlement en de Raad van ... betreffende ... (PB ...).

3. Het nationale contactpunt van de verzoekende lidstaat bevestigt een match van DNA-profielgegevens met de DNA-referentiegegevens die bij de aangezochte lidstaat berusten, nadat de DNA-referentiegegevens die vereist zijn om een match te bevestigen, automatisch zijn verstrekt.

Artikel 7

Geautomatiseerde vergelijking van niet-geïdentificeerde DNA-profielen

1. Met het oog op het onderzoek van strafbare feiten kunnen de lidstaten via hun nationale contactpunten hun ongeïdentificeerde DNA-profielen vergelijken met alle DNA-profielen die voorkomen in andere nationale DNA-analysebestanden. De profielen worden op geautomatiseerde wijze verstrekt en vergeleken.
2. Indien een aangezochte lidstaat bij de vergelijking als bedoeld in lid 1 vaststelt dat er een match is tussen een verstrekt DNA-profiel en een DNA-profiel in zijn DNA-analysebestand, verstrekt hij onverwijld aan het nationale contactpunt van de andere lidstaat de referentiegegevens waarmee een match is vastgesteld.
3. De bevestiging dat er een match is van een DNA-profiel met DNA-referentiegegevens die bij de aangezochte lidstaat berusten, wordt door het nationale contactpunt van de verzoekende lidstaat gegeven nadat de voor de bevestiging van de match benodigde DNA-referentiegegevens op geautomatiseerde wijze zijn verstrekt.

Artikel 8

Kennisgevingen over DNA-analysebestanden

Elke lidstaat stelt de Commissie en eu-LISA overeenkomstig artikel 73 in kennis van de nationale DNA-analysebestanden waarop de artikelen 5 tot en met 7 van toepassing zijn.

Artikel 9

Referentienummers voor DNA-profielen

De referentienummers voor DNA-profielen zijn een combinatie van:

- a) een referentienummer aan de hand waarvan de lidstaten bij een match nadere gegevens en overige informatie uit hun in artikel 5 bedoelde databanken kunnen opvragen en overeenkomstig de artikelen 47 en 48 aan een of meer andere lidstaten verstrekken;
- b) een code ter aanduiding van de lidstaat waarbij het DNA-profiel berust;
- c) een code ter aanduiding van het soort DNA-profiel (DNA-persoonsprofiel of niet-geïdentificeerd DNA-profiel).

Artikel 10

Beginnelsen voor de uitwisseling van DNA-referentiegegevens

1. De vertrouwelijkheid en de integriteit van naar andere lidstaten gezonden DNA-referentiegegevens worden gegarandeerd door middel van passende maatregelen, waaronder versleuteling.
2. De lidstaten nemen de nodige maatregelen om de integriteit van beschikbaar gestelde of voor vergelijking aan de andere lidstaten toegezonden DNA-profielen te waarborgen en ervoor te zorgen dat de genomen maatregelen voldoen aan de relevante internationale normen voor de uitwisseling van DNA-gegevens.

3. De Commissie stelt uitvoeringshandelingen vast ter bepaling van de relevante internationale normen die de lidstaten moeten gebruiken voor de uitwisseling van DNA-referentiegegevens. Die uitvoeringshandelingen worden vastgesteld volgens de procedure van artikel 76, lid 2.

Artikel 11

Voorschriften voor verzoeken en antwoorden betreffende DNA-profielen

1. In verzoeken om geautomatiseerde bevraging of vergelijking wordt uitsluitend de volgende informatie opgenomen:

- a) de code van de verzoekende lidstaat;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) DNA-profielen en de bijbehorende referentienummers als bedoeld in artikel 9;
- d) het soort DNA-profiel dat wordt overgedragen (niet-geïdentificeerde DNA-profielen of DNA-persoonsprofielen).

2. In antwoorden op verzoeken als bedoeld in lid 1 wordt uitsluitend de volgende informatie opgenomen:

- a) de indicatie of er sprake is van één of meer matches of niet;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) de datum, de tijd en het verwijsnummer van het antwoord;
- d) de codes van de verzoekende en de aangezochte lidstaat;
- e) de referentienummers van de DNA-profielen van de verzoekende en de aangezochte lidstaat;
- f) het soort DNA-profielen die zijn overgedragen (niet-geïdentificeerde DNA-profielen of DNA-persoonsprofielen);
- g) de DNA-profielen die een match vertonen.

3. Er wordt slechts geautomatiseerd melding gemaakt van een match als de geautomatiseerde bevraging of vergelijking een match heeft opgeleverd voor een minimumaantal loci. Ter bepaling van dit minimumaantal loci stelt de Commissie uitvoeringshandelingen vast volgens de procedure van artikel 76, lid 2.

4. Indien een bevraging of vergelijking met niet-geïdentificeerde DNA-profielen tot een match leidt, kan elke aangezochte lidstaat met gegevens die een match vertonen een markering in zijn nationale databank opnemen waaruit blijkt dat er na de bevraging of vergelijking van een andere lidstaat een match is geweest voor dat DNA-profiel.

5. De lidstaten zorgen ervoor dat verzoeken in overeenstemming zijn met de overeenkomstig artikel 8 ingediende kennisgevingen. Deze kennisgevingen worden opgenomen in de handleiding als bedoeld in artikel 78.

AFDELING 2

Dactyloscopische gegevens

Artikel 12

Dactyloscopische referentiegegevens

1. De lidstaten zien erop toe dat dactyloscopische referentiegegevens uit het bestand van de voor het voorkomen, opsporen en onderzoeken van strafbare feiten opgezette nationale geautomatiseerde dactyloscopische identificatiesystemen beschikbaar zijn.
2. Dactyloscopische referentiegegevens mogen geen gegevens bevatten waarmee de betrokkene rechtstreeks kan worden geïdentificeerd.
3. Dactyloscopische referentiegegevens die niet op een persoon zijn teruggevoerd (ongeïdentificeerde dactyloscopische gegevens) worden als zodanig herkenbaar gemaakt.

Artikel 13

Geautomatiseerde bevraging van dactyloscopische gegevens

1. Met het oog op het voorkomen, opsporen en onderzoeken van strafbare feiten verlenen de lidstaten de nationale contactpunten van de andere lidstaten en Europol toegang tot de dactyloscopische referentiegegevens van de geautomatiseerde dactyloscopische identificatiesystemen die zij daartoe hebben opgezet, zulks met het oog op geautomatiseerde bevraging door middel van een vergelijking met dactyloscopische referentiegegevens.

De bevraging mag slechts worden uitgevoerd in individuele gevallen en met inachtneming van het nationale recht van de verzoekende lidstaat.

2. Het nationale contactpunt van de verzoekende lidstaat bevestigt een match van dactyloscopische gegevens met de dactyloscopische referentiegegevens die bij de aangezochte lidstaat berusten, nadat de dactyloscopische referentiegegevens die vereist zijn om een match te bevestigen, automatisch zijn verstrekt.

Artikel 14

Referentienummers voor dactyloscopische gegevens

De referentienummers voor dactyloscopische gegevens zijn een combinatie van:

- a) een referentienummer aan de hand waarvan de lidstaten bij een match nadere gegevens en overige informatie uit hun in artikel 12 bedoelde databanken kunnen opvragen en overeenkomstig de artikelen 47 en 48 aan een of meer andere lidstaten kunnen verstrekken;
- b) een code ter aanduiding van de lidstaat waarbij de dactyloscopische gegevens berusten.

Artikel 15

Beginnelsen voor de uitwisseling van dactyloscopische gegevens

1. Dactyloscopische gegevens worden gedigitaliseerd en aan de andere lidstaten verstrekt conform een uniform gegevensformaat. Ter bepaling van het uniforme gegevensformaat stelt de Commissie uitvoeringshandelingen vast volgens de procedure van artikel 76, lid 2.

2. Elke lidstaat ziet erop toe dat de dactyloscopische gegevens die hij verstrekt van voldoende kwaliteit zijn voor een vergelijking door middel van het geautomatiseerde vingerafdrukidentificatiesysteem.
3. De lidstaten treffen passende maatregelen, waaronder versleuteling, om de vertrouwelijkheid en de integriteit van de verzonden dactyloscopische gegevens te waarborgen.
4. Ter bepaling van de relevante door de lidstaten te gebruiken bestaande normen voor de uitwisseling van dactyloscopische gegevens stelt de Commissie uitvoeringshandelingen vast. Die uitvoeringshandelingen worden vastgesteld volgens de procedure van artikel 76, lid 2.

Artikel 16

Bevragingscapaciteit voor dactyloscopische gegevens

1. Elke lidstaat zorgt ervoor dat zijn bevragsverzoeken de door de aangezochte lidstaat bepaalde bevragscapaciteit niet overtreffen.

De lidstaten doen de Commissie en eu-LISA overeenkomstig artikel 79, leden 8 en 10, mededeling van hun maximale capaciteit per dag voor dactyloscopische gegevens van geïdentificeerde personen en voor dactyloscopische gegevens van nog niet geïdentificeerde personen.

2. Ter bepaling van het maximumaantal te vergelijken kandidaten dat per bevraging wordt geaccepteerd, stelt de Commissie uitvoeringshandelingen vast volgens de procedure van artikel 76, lid 2.

Artikel 17

Voorschriften voor verzoeken en antwoorden in verband met dactyloscopische gegevens

1. In verzoeken om geautomatiseerde bevraging wordt uitsluitend de volgende informatie opgenomen:

- a) de code van de verzoekende lidstaat;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) de dactyloscopische gegevens en de bijbehorende referentienummers als bedoeld in artikel 14.

2. In antwoorden op verzoeken als bedoeld in lid 1 wordt uitsluitend de volgende informatie opgenomen:

- a) de indicatie of er sprake is van één of meer matches of niet;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) de datum, de tijd en het verwijsnummer van het antwoord;
- d) de codes van de verzoekende en de aangezochte lidstaat;
- e) de referentienummers van de dactyloscopische gegevens van de verzoekende en de aangezochte lidstaat;
- f) de dactyloscopische gegevens die een match vertonen.

AFDELING 3

Voertuigregistratiegegevens

Artikel 18

Geautomatiseerde bevraging van voertuigregistratiegegevens

1. Met het oog op het voorkomen, opsporen en onderzoeken van strafbare feiten verlenen de lidstaten de nationale contactpunten van andere lidstaten en Europol toegang tot de volgende nationale voertuigregistratiegegevens om in individuele gevallen geautomatiseerde bevragingen uit te voeren:

- a) gegevens met betrekking tot eigenaars of exploitanten;
- b) gegevens met betrekking tot voertuigen.

2. De bevraging mag uitsluitend met gebruikmaking van een volledig chassisnummer of een volledig registratienummer worden verricht.

3. De bevraging mag slechts worden uitgevoerd met inachtneming van het nationale recht van de verzoekende lidstaat.

Artikel 19

Beginselen inzake geautomatiseerde bevraging van voertuigregistratiegegevens

1. Voor de geautomatiseerde bevraging van voertuigregistratiegegevens maken de lidstaten gebruik van het Europees voertuig- en rijbewijsinformatiesysteem (Eucaris).

2. De via Eucaris uitgewisselde informatie wordt in versleutelde vorm overgedragen.

3. Ter bepaling van de uit te wisselen gegevenselementen van de voertuigregistratiegegevens stelt de Commissie uitvoeringshandelingen vast. Die uitvoeringshandelingen worden vastgesteld volgens de procedure van artikel 76, lid 2.

Artikel 20

Bijhouden van logbestanden

1. Elke lidstaat houdt logbestanden bij van de zoekopdrachten die zijn verricht door de naar behoren tot het uitwisselen van voertuigregistratiegegevens gemachtigde personeelsleden van zijn autoriteiten en houdt tevens logbestanden bij van door andere lidstaten gevraagde zoekopdrachten. Europol houdt logbestanden bij van de zoekopdrachten van zijn naar behoren gemachtigde personeelsleden.

Alle lidstaten en Europol houden logbestanden bij van alle gegevensverwerkingsverrichtingen met betrekking tot voertuigregistratiegegevens. In deze logbestanden worden de volgende gegevens opgenomen:

- a) de lidstaat die of het agentschap van de Unie dat het verzoek tot uitvoering van een zoekopdracht heeft ingediend;
- b) de datum en het tijdstip van het verzoek;
- c) de datum en het tijdstip van het antwoord;
- d) de nationale databanken waarnaar een verzoek tot uitvoering van een zoekopdracht is verzonden;
- e) de nationale databanken die een positief antwoord hebben verstrekt.

2. De in lid 1 bedoelde logbestanden mogen uitsluitend worden gebruikt voor het verzamelen van statistieken en het toezicht op de gegevensbescherming, alsmede het verifiëren van de toelaatbaarheid van een verzoek en de rechtmatigheid van de gegevensverwerking, en voor het waarborgen van de beveiliging en de integriteit van de gegevens.

Deze logbestanden worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanmaken ervan gewist. Indien zij echter nodig zijn voor reeds aangevangen monitoringprocedures, worden zij gewist wanneer de logbestanden niet langer nodig zijn voor de monitoringprocedures.

3. Met het oog op het toezicht op de gegevensbescherming, waaronder het verifiëren van de toelaatbaarheid van een zoekopdracht en de rechtmatigheid van de gegevensverwerking, hebben de verwerkingsverantwoordelijken toegang tot de logbestanden voor interne monitoring als bedoeld in artikel 56.

AFDELING 4

Gezichtsopnamen

Artikel 21

Gezichtsopnamen

1. De lidstaten zien erop toe dat gezichtsopnamen uit hun voor het voorkomen, opsporen en onderzoeken van strafbare feiten opgezette nationale databanken beschikbaar zijn. De relevante gegevens omvatten uitsluitend gezichtsopnamen en het in artikel 23 bedoelde referentienummer, en vermelden of de gezichtsopnamen tot een bepaalde persoon zijn herleid.

De lidstaten stellen in dit verband geen gegevens beschikbaar aan de hand waarvan een persoon rechtstreeks kan worden geïdentificeerd.

2. Gezichtsopnamen die niet op een persoon terug te voeren zijn (ongeïdentificeerde gezichtsopnamen) moeten als zodanig herkenbaar zijn.

Artikel 22

Geautomatiseerde bevraging van gezichtsopnamen

1. Met het oog op het voorkomen, opsporen en onderzoeken van strafbare feiten verlenen de lidstaten de nationale contactpunten van andere lidstaten en Europol toegang tot de in hun nationale databanken opgeslagen gezichtsopnamen om geautomatiseerde bevragingen uit te voeren.

De bevraging mag slechts worden uitgevoerd in individuele gevallen en met inachtneming van het nationale recht van de verzoekende lidstaat.

2. De verzoekende lidstaat ontvangt een lijst met matches voor de vermoedelijke kandidaten. Die lidstaat beoordeelt de lijst om vast te stellen of een match kan worden bevestigd.

3. Er wordt een minimumkwaliteitsnorm vastgesteld voor het bevragen en vergelijken van gezichtsopnamen. Ter bepaling van die minimumkwaliteitsnorm stelt de Commissie uitvoeringshandelingen vast. Die uitvoeringshandelingen worden vastgesteld volgens de procedure van artikel 76, lid 2.

Artikel 23

Referentienummers voor gezichtsopnamen

De referentienummers voor gezichtsopnamen zijn een combinatie van:

- a) een referentienummer aan de hand waarvan de lidstaten bij een match nadere gegevens en overige informatie uit hun in artikel 21 bedoelde databanken kunnen opvragen en overeenkomstig de artikelen 47 en 48 aan een of meer andere lidstaten kunnen verstrekken;
- b) een code ter aanduiding van de lidstaat waarbij de gezichtsopnamen berusten.

Artikel 24

Voorschriften voor verzoeken en antwoorden in verband met gezichtsopnamen

1. In verzoeken om geautomatiseerde bevraging wordt uitsluitend de volgende informatie opgenomen:

- a) de code van de verzoekende lidstaat;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) de gezichtsopnamen en de bijbehorende referentienummers als bedoeld in artikel 23.

2. In antwoorden op verzoeken als bedoeld in lid 1 wordt uitsluitend de volgende informatie opgenomen:

- a) de indicatie of er sprake is van één of meer matches of niet;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) de datum, de tijd en het verwijsnummer van het antwoord;
- d) de codes van de verzoekende en de aangezochte lidstaat;
- e) de referentienummers van de gezichtsopnamen van de verzoekende en de aangezochte lidstaat;
- f) de gezichtsopnamen die een match vertonen.

AFDELING 5

Politiegegevens

Artikel 25

Politiegegevens

1. De lidstaten kunnen beslissen deel te nemen aan de geautomatiseerde uitwisseling van politiegegevens. De lidstaten die deelnemen aan de geautomatiseerde uitwisseling van politiegegevens zorgen voor de beschikbaarheid van de biografische gegevens van verdachten en criminelen die zijn opgenomen in hun voor het onderzoek van strafbare feiten ingestelde politieregisters. Deze gegevensverzameling bevat, indien beschikbaar, de volgende gegevens:

- a) voornaam of voornamen;
- b) familienaam of familienamen;
- c) alias of aliassen;
- d) geboortedatum;

- e) nationaliteit of nationaliteiten;
- f) plaats en land van geboorte;
- g) geslacht.

2. De in lid 1, punten a), b), c), e) en f), bedoelde gegevens worden gepseudonimiseerd.

Artikel 26

Geautomatiseerde bevraging van politiegegevens

1. Ten behoeve van het onderzoek van strafbare feiten verlenen de lidstaten de nationale contactpunten van andere lidstaten en Europol toegang tot de in hun nationale politieregisters opgeslagen gegevens met het oog op geautomatiseerde bevraging.

De bevraging mag slechts worden uitgevoerd in individuele gevallen en met inachtneming van het nationale recht van de verzoekende lidstaat.

2. De verzoekende lidstaat ontvangt de lijst van matches met een indicatie van de kwaliteit ervan.

De verzoekende lidstaat wordt ook meegedeeld in de databank van welke lidstaat de gegevens die tot de match hebben geleid, zijn opgenomen.

Artikel 27

Referentienummers voor politiegegevens

De referentienummers voor politiegegevens zijn een combinatie van:

- a) een referentienummer aan de hand waarvan de lidstaten bij een match persoonsgegevens en overige informatie uit hun in artikel 25 bedoelde registers kunnen opvragen en overeenkomstig de artikelen 47 en 48 aan een of meer andere lidstaten kunnen verstrekken;
- b) een code ter aanduiding van de lidstaat waarbij de politiegegevens berusten.

Artikel 28

Voorschriften voor verzoeken en antwoorden in verband met politiegegevens

1. In verzoeken om geautomatiseerde bevraging wordt uitsluitend de volgende informatie opgenomen:

- a) de code van de verzoekende lidstaat;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) de politiegegevens en de bijbehorende referentienummers als bedoeld in artikel 27.

2. In antwoorden op verzoeken als bedoeld in lid 1 wordt uitsluitend de volgende informatie opgenomen:

- a) de indicatie of er sprake is van één of meer matches of niet;
- b) de datum, de tijd en het verwijsnummer van het verzoek;
- c) de datum, de tijd en het verwijsnummer van het antwoord;
- d) de codes van de verzoekende en de aangezochte lidstaat;
- e) de referentienummers van de politiegegevens van de aangezochte lidstaten;

AFDELING 6

Gemeenschappelijke bepalingen

Artikel 29

Nationale contactpunten

Elke lidstaat wijst een nationaal contactpunt aan.

De nationale contactpunten worden belast met het verstrekken van de in de artikelen 6, 7, 13, 18, 22 en 26 bedoelde gegevens.

Artikel 30

Uitvoeringsmaatregelen

Ter bepaling van de technische regelingen voor de procedures van de artikelen 6, 7, 13, 18, 22 en 26 stelt de Commissie uitvoeringshandelingen vast. Die uitvoeringshandelingen worden vastgesteld volgens de procedure van artikel 76, lid 2.

Artikel 31

Technische specificaties

De lidstaten en Europol nemen gemeenschappelijke technische specificaties in acht voor alle verzoeken en antwoorden met betrekking tot de bevraging en vergelijking van DNA-profielen, dactyloscopische gegevens, voertuigregistratiegegevens, gezichtsopnamen en politiegegevens. Ter bepaling van deze technische specificaties stelt de Commissie uitvoeringshandelingen vast volgens de procedure van artikel 76, lid 2.

Artikel 32

Beschikbaarheid van geautomatiseerde gegevensuitwisseling op nationaal niveau

1. De lidstaten treffen alle nodige maatregelen om ervoor te zorgen dat de geautomatiseerde bevraging of vergelijking van DNA-profielen, dactyloscopische gegevens, voertuigregistratiegegevens, gezichtsopnamen en politiegegevens 24 uur per dag en zeven dagen per week mogelijk is.
2. De nationale contactpunten stellen de andere nationale contactpunten, de Commissie, Europol en eu-LISA er onmiddellijk van in kennis wanneer door een technisch probleem de geautomatiseerde gegevensuitwisseling niet beschikbaar is.

De nationale contactpunten komen overeenkomstig het toepasselijke Unierecht en de nationale wetgeving tijdelijke alternatieve informatie-uitwisselingsregelingen overeen.

3. De nationale contactpunten herstellen de geautomatiseerde gegevensuitwisseling zo snel mogelijk.

Artikel 33

Redenen voor de gegevensverwerking

1. Elke lidstaat registreert de redenen waarom zijn bevoegde autoriteiten zoekopdrachten hebben uitgevoerd.

Europol registreert de redenen waarom het zoekopdrachten heeft uitgevoerd.

2. Bij de registratie van de redenen voor de verwerking worden de volgende gegevens vermeld:
- het doel van de zoekopdracht, onder verwijzing naar de specifieke zaak of het specifieke onderzoek;
 - of de zoekopdracht betrekking heeft op een verdachte of een dader van een strafbaar feit;
 - of de zoekopdracht bedoeld is om een onbekende persoon te identificeren of om meer gegevens over een bekende persoon te verkrijgen.

3. De in lid 2 bedoelde redenen voor de verwerking mogen uitsluitend worden gebruikt voor het toezicht op de gegevensbescherming, waaronder de verificatie van de toelaatbaarheid van een zoekopdracht en de rechtmatigheid van de gegevensverwerking, en voor het waarborgen van de beveiliging en de integriteit van de gegevens.

De redenen voor de gegevensverwerking worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanmaken ervan gewist. Indien zij echter nodig zijn voor reeds aangevangen monitoringprocedures, worden zij gewist wanneer de opgave van redenen voor de gegevensverwerking niet langer nodig is voor de monitoringprocedures.

4. Met het oog op het toezicht op de gegevensbescherming, waaronder de verificatie van de toelaatbaarheid van een zoekopdracht en de rechtmatigheid van de gegevensverwerking, hebben de verwerkingsverantwoordelijken toegang tot de redenen voor de gegevensverwerking voor interne monitoring als bedoeld in artikel 56.

Artikel 34

Gebruik van het Universal Message Format

- Bij de ontwikkeling van de in artikel 35 bedoelde router en Epris wordt gebruikgemaakt van de norm inzake het Universal Message Format (UMF).
- Bij elke geautomatiseerde uitwisseling van gegevens overeenkomstig deze verordening wordt gebruikgemaakt van de UMF-norm.

HOOFDSTUK 3

ARCHITECTUUR

AFDELING 1

Router

Artikel 35

De router

- Er wordt een router opgezet ter facilitering van de totstandbrenging overeenkomstig deze verordening van verbindingen tussen de lidstaten en met Europol met het oog op het doorzoeken met biometrische gegevens, het opvragen van die gegevens en het bepalen van het matchingpercentage van die gegevens.
- De router bestaat uit:

- a) een centrale infrastructuur, met inbegrip van een zoekinstrument waarmee de in de artikelen 5, 12 en 21 bedoelde databanken van de lidstaten en de gegevens van Europol gelijktijdig kunnen worden doorzocht;
- b) een beveiligd communicatiekanaal tussen de centrale infrastructuur, de lidstaten en de agentschappen van de Unie die gebruik mogen maken van de router;
- c) een beveiligde communicatie-infrastructuur tussen de centrale infrastructuur en het Europees zoekportaal voor de toepassing van artikel 39.

Artikel 36

Gebruik van de router

Het gebruik van de router is voorbehouden aan de lidstatelijke instanties die bevoegd zijn voor de uitwisseling van DNA-profielen, dactyloscopische gegevens en gezichtsopnamen en aan Europol, overeenkomstig deze verordening en Verordening (EU) 2016/794.

Artikel 37

Zoekopdrachten

1. De in artikel 36 bedoelde routergebruikers verzoeken om een zoekopdracht door biometrische gegevens door te geven aan de router. De router stuurt het verzoek om een zoekopdracht naar de databanken van de lidstaten en de Europolgegevens, gelijktijdig met de door de gebruiker doorgegeven gegevens en met inachtneming van diens toegangsrechten.
2. Nadat het verzoek om een zoekopdracht is ontvangen van de router, starten elke aangezochte lidstaat en Europol onverwijld en op geautomatiseerde wijze een zoekopdracht in hun databanken.
3. Alle matches die voortvloeien uit de zoekopdracht in de databanken van elke lidstaat en de Europolgegevens worden op geautomatiseerde wijze teruggezonden naar de router.
4. De router rangschikt de antwoorden op basis van een score die aangeeft in hoeverre de voor de bevraging gebruikte biometrische gegevens overeenstemmen met de in de databanken van de lidstaten opgeslagen biometrische gegevens en de Europolgegevens.
5. De lijst van biometrische gegevens die een match vertonen en de scores ervan wordt door de router naar de routergebruiker teruggezonden.
6. De Commissie stelt uitvoeringshandelingen vast tot nadere bepaling van de technische procedure aan de hand waarvan de router de databanken van de lidstaten en de Europolgegevens doorzoekt, het formaat van de antwoorden van de router en de technische voorschriften voor het bepalen van de score die aangeeft in hoeverre de biometrische gegevens overeenstemmen. Die uitvoeringshandelingen worden vastgesteld volgens de procedure van artikel 76, lid 2.

Artikel 38

Kwaliteitscontrole

De aangezochte lidstaat controleert de kwaliteit van de doorgezonden gegevens door middel van een volledig geautomatiseerde procedure.

Mochten de gegevens zich niet lenen voor geautomatiseerde vergelijking, dan stelt de aangezochte lidstaat de verzoekende lidstaat daarvan via de router onverwijld in kennis.

Interoperabiliteit tussen de router en het gemeenschappelijk identiteitsregister met het oog op de toegang voor rechtshandavingsdoeleinden

1. De in artikel 36 bedoelde routergebruikers kunnen tegelijk met een zoekopdracht in de databanken van de lidstaten en de Europolgegevens een zoekopdracht in het gemeenschappelijk identiteitsregister starten indien aan de toepasselijke voorwaarden uit hoofde van het Unierecht is voldaan en in overeenstemming met hun toegangsrechten. Daartoe be vraagt de router het gemeenschappelijk identiteitsregister via het Europees zoekportaal.

2. Zoekopdrachten in het gemeenschappelijk identiteitsregister voor rechtshandavingsdoeleinden worden uitgevoerd overeenkomstig artikel 22 van Verordening (EU) 2019/817 en artikel 22 van Verordening (EU) 2019/818. Het resultaat van de zoekopdrachten wordt doorgezonden via het Europees zoekportaal.

Slechts de aangewezen autoriteiten als bedoeld in artikel 4, punt 20, van Verordening (EU) 2019/817 en artikel 4, punt 20, van Verordening (EU) 2019/818 mogen deze gelijktijdige zoekopdrachten indienen.

Gelijktijdige zoekopdrachten in de databanken van de lidstaten en de Europolgegevens en het gemeenschappelijk identiteitsregister mogen slechts worden gestart indien het waarschijnlijk is dat gegevens over een verdachte, dader of slachtoffer van een terroristisch misdrijf of een ander ernstig strafbaar feit in de zin van respectievelijk artikel 4, punten 21 en 22, van Verordening (EU) 2019/817 en artikel 4, punten 21 en 22, van Verordening (EU) 2019/818 in het gemeenschappelijke identiteitsregister zijn opgeslagen.

Bijhouden van logbestanden

1. eu-LISA houdt logbestanden bij van alle gegevensverwerkingsverrichtingen in de router. In deze logbestanden worden de volgende gegevens opgenomen:

- a) de lidstaat die of het agentschap van de Unie dat het verzoek tot uitvoering van een zoekopdracht heeft ingediend;
- b) de datum en het tijdstip van het verzoek;
- c) de datum en het tijdstip van het antwoord;
- d) de nationale databanken of de Europolgegevens waarnaar een verzoek tot uitvoering van een zoekopdracht is verzonden;
- e) de nationale databanken of Europolgegevens die een antwoord hebben opgeleverd;
- f) indien van toepassing het feit dat er gelijktijdig een zoekopdracht in het gemeenschappelijk identiteitsregister is uitgevoerd.

2. Elke lidstaat houdt logbestanden bij van de zoekopdrachten die zijn verricht door zijn bevoegde instanties en de naar behoren tot het gebruik van de router gemachtigde personeelsleden van die instanties, en houdt tevens logbestanden bij van door andere lidstaten gevraagde zoekopdrachten.

Europol houdt logbestanden bij van de zoekopdrachten van zijn naar behoren gemachtigde personeelsleden.

3. De in de leden 1 en 2 bedoelde logbestanden mogen uitsluitend worden gebruikt voor het verzamelen van statistieken en het toezicht op de gegevensbescherming, alsmede het verifiëren van de

toelaatbaarheid van een verzoek en de rechtmatigheid van de gegevensverwerking, en voor het waarborgen van de beveiliging en de integriteit van de gegevens.

Deze logbestanden worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanmaken ervan gewist. Indien zij echter nodig zijn voor reeds aangevangen toezichtprocedures, worden zij gewist wanneer de logbestanden in het kader van de toezichtprocedures niet langer nodig zijn.

4. Met het oog op het toezicht op de gegevensbescherming, waaronder het verifiëren van de toelaatbaarheid van een zoekopdracht en de rechtmatigheid van de gegevensverwerking, hebben de verwerkingsverantwoordelijken toegang tot de logbestanden voor interne monitoring als bedoeld in artikel 56.

Artikel 41

Kennisgevingsprocedures wanneer de router door een technische storing niet kan worden gebruikt

1. Indien het wegens een storing van de router technisch onmogelijk is de router te gebruiken voor het bevragen van een of meer nationale databanken of Europolgegevens, stelt eu-LISA de routergebruikers daarvan op geautomatiseerde wijze in kennis. eu-LISA treft onverwijld maatregelen om de technische storing die het gebruik van de router verhindert, te verhelpen.
2. Indien het wegens een storing in de nationale infrastructuur van een lidstaat technisch onmogelijk is de router te gebruiken om een of meer nationale databanken of de Europolgegevens te doorzoeken, stelt die lidstaat eu-LISA en de Commissie daarvan op geautomatiseerde wijze in kennis. De lidstaten treffen onverwijld maatregelen om de technische storing die het gebruik van de router verhindert, te verhelpen.
3. Indien het wegens een storing in de infrastructuur van Europol technisch onmogelijk is de router te gebruiken om een of meer nationale databanken of de Europolgegevens te doorzoeken, stelt Europol de lidstaten, eu-LISA en de Commissie daarvan op geautomatiseerde wijze in kennis. Europol treft onverwijld maatregelen om de technische storing die het gebruik van de router verhindert, te verhelpen.

AFDELING 2

Epris

Artikel 42

Epris

1. Voor de in artikel 26 bedoelde geautomatiseerde bevraging van politiegegevens maken de lidstaten en Europol gebruik van het Europees Indexsysteem van politiegegevens (Epris).
2. Epris bestaat uit:
 - a) een centrale infrastructuur, met inbegrip van een zoekinstrument dat de gelijktijdige bevraging van de databanken van de lidstaten mogelijk maakt;
 - b) een beveiligd communicatiekanaal tussen de centrale Epris-infrastructuur, de lidstaten en Europol.

Gebruik van Epris

1. Voor de bevraging van politiegegevens via Epris worden de volgende reeksen gegevens gebruikt:
 - a) voornaam of voornamen;
 - b) familienaam of familienamen;
 - c) geboortedatum.
2. Indien beschikbaar, mogen ook de volgende reeksen gegevens worden gebruikt:
 - a) alias of aliases;
 - b) nationaliteit of nationaliteiten;
 - c) plaats en land van geboorte;
 - d) geslacht.
3. De in lid 1, punten a) en b), en lid 2, punten a), b) en c), bedoelde gegevens die voor bevraging worden gebruikt, worden gepseudonimiseerd.

Zoekopdrachten

1. De lidstaten en Europol verzoeken om een zoekopdracht door de in artikel 43 bedoelde gegevens te versturen.

Epris zendt het verzoek om een zoekopdracht in overeenstemming met deze verordening door naar de databanken van de lidstaten, samen met de door de verzoekende lidstaat toegezonden gegevens.

2. Nadat het verzoek om een zoekopdracht is ontvangen van Epris, start elke aangezochte lidstaat onverwijld en op geautomatiseerde wijze een zoekopdracht in zijn nationale politiegegevens.

3. Alle matches die voortvloeien uit de zoekopdracht in de databank van elke lidstaat worden op geautomatiseerde wijze teruggezonden naar Epris.

4. De lijst van matches wordt door Epris aan de verzoekende lidstaat teruggezonden. In de lijst van matches wordt de kwaliteit van de match aangegeven, alsmede de lidstaat waarvan de databank de gegevens bevat die tot de match hebben geleid.

5. Na ontvangst van de lijst van matches beslist de verzoekende lidstaat voor welke matches een follow-up nodig is en zendt hij de aangezochte lidstaat of lidstaten via Siena een met redenen omkleed follow-upverzoek met eventuele relevante aanvullende informatie.

6. Door de aangezochte lidstaat of lidstaten worden deze verzoeken onverwijld behandeld om te beslissen of zij de in hun databank opgeslagen gegevens delen of niet.

Na bevestiging worden de in artikel 43 bedoelde gegevens, voor zover beschikbaar, door de aangezochte lidstaat of lidstaten gedeeld. Deze informatie-uitwisseling geschiedt via Siena.

7. De Commissie stelt uitvoeringshandelingen vast met specificaties voor de technische procedure die Epris toepast voor het bevragen van de databanken van de lidstaten, en voor het formaat van de antwoorden. Die uitvoeringshandelingen worden vastgesteld volgens de procedure van artikel 76, lid 2.

Bijhouden van logbestanden

1. Europol houdt logbestanden bij van alle gegevensverwerkingsverrichtingen in Epris. In deze logbestanden worden de volgende gegevens opgenomen:

- a) de lidstaat die of het agentschap van de Unie dat het verzoek tot uitvoering van een zoekopdracht heeft ingediend;
- b) de datum en het tijdstip van het verzoek;
- c) de datum en het tijdstip van het antwoord;
- d) de nationale databanken waarnaar een verzoek tot uitvoering van een zoekopdracht is verzonden;
- e) de nationale databanken die een antwoord hebben opgeleverd.

2. Elke lidstaat houdt logbestanden bij van de verzoeken voor zoekopdrachten die zijn gedaan door zijn bevoegde instanties en de personeelsleden van die instanties die naar behoren gemachtigd zijn om Epris te gebruiken. Europol houdt logbestanden bij van de verzoeken om zoekopdrachten die zijn naar behoren gemachtigde personeelsleden hebben gedaan.

3. De in de leden 1 en 2 bedoelde logbestanden worden uitsluitend gebruikt voor het toezicht op de gegevensbescherming, onder meer door de toelaatbaarheid van een zoekopdracht en de rechtmatigheid van de gegevensverwerking te controleren, en voor het verzekeren van de gegevensbeveiliging en -integriteit.

Deze logbestanden worden met passende maatregelen tegen ongeoorloofde toegang beschermd en één jaar na het aanmaken ervan gewist.

Indien zij echter nodig zijn voor reeds aangevangen toezichtprocedures, worden zij gewist wanneer de logbestanden in het kader van de toezichtprocedures niet langer nodig zijn.

4. Met het oog op het toezicht op de gegevensbescherming, waaronder het verifiëren van de toelaatbaarheid van een zoekopdracht en de rechtmatigheid van de gegevensverwerking, hebben de verwerkingsverantwoordelijken toegang tot de logbestanden voor interne monitoring als bedoeld in artikel 56.

Kennisgevingsprocedures wanneer Epris door een technische storing niet kan worden gebruikt

1. Indien Epris wegens een technische storing in de infrastructuur van Europol niet kan worden gebruikt om een of meer nationale databanken te doorzoeken, stelt Europol de lidstaten daarvan op geautomatiseerde wijze in kennis. Europol treft onverwijld maatregelen om de technische storing die het gebruik van Epris verhindert, te verhelpen.

2. Indien Epris wegens een technische storing in de nationale infrastructuur van een lidstaat niet kan worden gebruikt om een of meer nationale databanken te doorzoeken, stelt die lidstaat Europol en de Commissie daarvan op geautomatiseerde wijze in kennis. De lidstaten treffen onverwijld maatregelen om de technische storing die het gebruik van Epris verhindert, te verhelpen.

HOOFDSTUK 4

UITWISSELING VAN GEGEVENS NAAR AANLEIDING VAN EEN MATCH

Artikel 47

Uitwisseling van kerngegevens

Indien de in artikel 6, 7, 13 of 22 bedoelde procedures een match opleveren tussen de voor de bevraging of vergelijking gebruikte gegevens en de gegevens in de databank van de aangezochte lidstaat of lidstaten, en na bevestiging van deze match door de verzoekende lidstaat, zendt de aangezochte lidstaat binnen 24 uur via de router een beperkte reeks kerngegevens terug. Deze reeks kerngegevens bevat, indien beschikbaar, de volgende gegevens:

- a) voornaam of voornamen;
- b) familienaam of familienamen;
- c) geboortedatum;
- d) nationaliteit of nationaliteiten;
- e) plaats en land van geboorte;
- f) geslacht.

Artikel 48

Gebruik van Siena

Elke uitwisseling tussen de bevoegde autoriteiten van de lidstaten of met Europol, in enig stadium van een van de procedures van deze verordening, waarin deze verordening niet uitdrukkelijk voorziet, vindt plaats via Siena.

HOOFDSTUK 5

Europol

Artikel 49

Toegang van lidstaten tot bij Europol opgeslagen uit derde landen afkomstige biometrische gegevens

1. De lidstaten hebben overeenkomstig Verordening (EU) 2016/794 toegang tot biometrische gegevens die door derde landen aan Europol zijn verstrekt voor de toepassing van artikel 18, lid 2, punten a), b) en c), van Verordening (EU) 2016/794, en kunnen deze via de router bevragen.
2. Wanneer deze procedure leidt tot een match tussen de voor de bevraging gebruikte gegevens en de Europolgegevens, vindt de follow-up plaats overeenkomstig Verordening (EU) 2016/794.

Artikel 50

Toegang van Europol tot in de databanken van de lidstaten opgeslagen gegevens

1. Europol heeft overeenkomstig Verordening (EU) 2016/794 toegang tot gegevens die de lidstaten overeenkomstig deze verordening in hun nationale databanken hebben opgeslagen.

2. Zoekopdrachten van Europol met biometrische gegevens als zoekcriterium worden uitgevoerd met behulp van de router.
3. Zoekopdrachten van Europol met voertuigregistratiegegevens als zoekcriterium worden uitgevoerd met behulp van Eucaris.
4. Zoekopdrachten van Europol met politiegegevens als zoekcriterium worden uitgevoerd met behulp van Epris.
5. Europol verricht zoekopdrachten overeenkomstig lid 1 uitsluitend bij de uitvoering van zijn taken als bedoeld in Verordening (EU) 2016/794.
6. Indien de in artikel 6, 7, 13 of 22 bedoelde procedures een match opleveren tussen de voor de bevraging of vergelijking gebruikte gegevens en de gegevens in de nationale databank van de aangezochte lidstaat of lidstaten, en na bevestiging van die match door Europol, beslist de aangezochte lidstaat binnen 24 uur of hij via de router een beperkte reeks kerngegevens terugzendt. Deze reeks kerngegevens bevat, indien beschikbaar, de volgende gegevens:
 - a) voornaam of voornamen;
 - b) familienaam of familienamen;
 - c) geboortedatum;
 - d) nationaliteit of nationaliteiten;
 - e) plaats en land van geboorte;
 - f) geslacht.
7. Het gebruik door Europol van informatie die is verkregen uit een zoekopdracht overeenkomstig lid 1 en de uitwisseling van kerngegevens overeenkomstig lid 6, is onderworpen aan de toestemming van de lidstaat in de databank waarvan de match zich heeft voorgedaan. Indien de lidstaat het gebruik van die informatie toestaat, wordt deze door Europol behandeld overeenkomstig Verordening (EU) 2016/794.

HOOFDSTUK 6

GEGEVENSBESCHERMING

Artikel 51

Doel van de gegevens

1. De verzoekende lidstaat, dan wel Europol, mag persoonsgegevens uitsluitend verwerken voor de doeleinden waarvoor deze door de aangezochte lidstaat uit hoofde van deze verordening zijn verstrekt. Verwerking voor andere doeleinden is slechts toegestaan met voorafgaande toestemming van de aangezochte lidstaat.
2. Verwerking van op grond van artikel 6, 7, 13, 18 of 22 verstrekte gegevens door de bevragende of vergelijkende lidstaat is slechts toegestaan om:
 - a) vast te stellen of de vergeleken DNA-profielen, dactyloscopische gegevens, voertuigregistratiegegevens, gezichtsopnamen en politiegegevens een match vertonen;
 - b) een politieel verzoek om rechtshulp op te stellen en in te dienen wanneer die gegevens een match vertonen;
 - c) logbestanden bij te houden als bedoeld in de artikelen 40 en 45.

3. De verzoekende lidstaat mag de hem overeenkomstig artikel 6, 7, 13 of 22 verstrekte gegevens slechts verwerken voor zover dit voor de doeleinden van deze verordening noodzakelijk is. Na de vergelijking van de gegevens of de geautomatiseerde antwoorden op de zoekopdrachten worden de verstrekte gegevens onverwijld gewist, tenzij verdere verwerking door de verzoekende lidstaat noodzakelijk is voor het voorkomen, opsporen of onderzoeken van een strafbaar feit.

4. De overeenkomstig artikel 18 verstrekte gegevens mogen door de verzoekende lidstaat slechts worden gebruikt voor zover dit voor de doeleinden van deze verordening noodzakelijk is. Na geautomatiseerde beantwoording van zoekopdrachten worden de verstrekte gegevens onverwijld gewist, tenzij verdere verwerking noodzakelijk is voor het bijhouden van logbestanden op grond van artikel 20. De verzoekende lidstaat mag de als antwoord verkregen gegevens uitsluitend gebruiken voor de procedure op grond waarvan de bevraging is geschied.

Artikel 52

Juistheid, relevantie en bewaring van gegevens

1. De lidstaten zien toe op de juistheid en actualiteit van persoonsgegevens. Indien een aangezochte lidstaat bemerkt dat onjuiste gegevens of gegevens die niet hadden mogen worden verstrekt, toch verstrekt zijn, dan wordt dit onverwijld aan de ontvangende lidstaat of lidstaten meegedeeld. Alle betrokken verzoekende lidstaten zijn verplicht de gegevens dienovereenkomstig te corrigeren of te wissen. Voor het overige worden verstrekte persoonsgegevens gecorrigeerd als blijkt dat ze onjuist zijn. Als de verzoekende lidstaat reden heeft om aan te nemen dat de verstrekte gegevens onjuist zijn of gewist moeten worden, dan stelt hij de aangezochte lidstaat daarvan op de hoogte.

2. Wanneer een betrokkene de juistheid van gegevens die in het bezit zijn van een lidstaat betwist, wanneer de juistheid door de betrokken lidstaat niet op betrouwbare wijze kan worden vastgesteld en wanneer de betrokkene daarom verzoekt, worden de gegevens in kwestie voorzien van een markering. Indien er een markering is aangebracht, mag deze door een lidstaat slechts met toestemming van de betrokkene of op basis van een besluit van de bevoegde rechter of een onafhankelijke gegevensbeschermingsautoriteit worden verwijderd.

3. Verstrekte gegevens worden gewist als zij niet verstrekt of ontvangen hadden mogen worden. Rechtmatig verstrekte en ontvangen gegevens worden gewist:

- a) als zij niet of niet meer noodzakelijk zijn voor het doel waarvoor zij zijn verstrekt;
- b) na afloop van een uit hoofde van het nationale recht van de aangezochte lidstaat vastgestelde maximumtermijn voor het bewaren van gegevens, indien de aangezochte lidstaat de verzoekende lidstaat bij de verstrekking van de gegevens op die maximumtermijn heeft gewezen.

Als er reden bestaat om aan te nemen dat door het wissen van de gegevens de belangen van de betrokkene worden geschaad, worden de gegevens afgeschermd in plaats van gewist. Afgeschermd gegevens mogen alleen worden verstrekt of gebruikt voor het doel dat ertoe heeft geleid dat ze niet zijn gewist.

Artikel 53

Verwerker

1. eu-LISA is de verwerker in de zin van artikel 3, punt 12, van Verordening (EU) 2018/1725 met betrekking tot de verwerking van persoonsgegevens via de router.

2. Europol is de verwerker met betrekking tot de verwerking van persoonsgegevens via Epris.

Beveiliging van de verwerking

1. Europol, eu-LISA en de lidstatelijke instanties waarborgen de beveiliging van de verwerking van persoonsgegevens die plaatsvindt uit hoofde van deze verordening. Europol, eu-LISA en de lidstatelijke instanties werken samen op het gebied van beveiligingsgerelateerde taken.
2. Onverminderd artikel 33 van Verordening (EU) 2018/1725 en artikel 32 van Verordening (EU) 2016/794 nemen eu-LISA en Europol de nodige maatregelen ter beveiliging van respectievelijk de router en Epris, alsmede de bijbehorende communicatie-infrastructuren.
3. Met name nemen eu-LISA en Europol passende maatregelen in verband met respectievelijk de router en Epris, waaronder de vaststelling van een veiligheidsplan, een bedrijfscontinuïteitsplan en een uitwijkplan, om:
 - a) de gegevens fysiek te beschermen, onder andere door middel van noodplannen voor de bescherming van kritieke infrastructuur;
 - b) te voorkomen dat onbevoegden toegang krijgen tot gegevensverwerkende apparatuur en installaties;
 - c) te voorkomen dat onbevoegden de gegevensdragers lezen, kopiëren, wijzigen of verwijderen;
 - d) te voorkomen dat gegevens onrechtmatig worden ingevoerd en dat opgeslagen persoonsgegevens onrechtmatig worden ingezien, gewijzigd of verwijderd;
 - e) te voorkomen dat gegevens onrechtmatig worden verwerkt, gekopieerd, gewijzigd of gewist;
 - f) te voorkomen dat onbevoegden de systemen voor geautomatiseerde gegevensverwerking gebruiken met behulp van datatransmissieapparatuur;
 - g) te waarborgen dat personen die toestemming hebben voor toegang tot de router en tot Epris, uitsluitend toegang krijgen tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft, en uitsluitend door middel van persoonlijke gebruikersidentiteiten en vertrouwelijke toegangsprocedures;
 - h) te waarborgen dat kan worden nagegaan en vastgesteld aan welke instanties persoonsgegevens mogen worden doorgegeven door middel van datatransmissieapparatuur;
 - i) te waarborgen dat kan worden nagegaan en vastgesteld welke gegevens wanneer, door wie en met welk doel in de router en in Epris zijn verwerkt;
 - j) te voorkomen, in het bijzonder door middel van passende versleutelingstechnieken, dat bij de doorgifte van persoonsgegevens vanuit en naar de router of Epris, of gedurende het transport van gegevensdragers, de gegevens onrechtmatig worden gelezen, gekopieerd, gewijzigd of gewist;
 - k) ervoor te zorgen dat de normale werking van de geïnstalleerde systemen in geval van storing kan worden hersteld;
 - l) de betrouwbaarheid te verzekeren door ervoor te zorgen dat eventuele functionele storingen in de router en in Epris correct wordenesignaleerd;
 - m) de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen te monitoren, met betrekking tot de interne monitoring de nodige organisatorische maatregelen te nemen om te waarborgen dat deze verordening wordt nageleefd en die beveiligingsmaatregelen te beoordelen in het licht van nieuwe technologische ontwikkelingen.

Beveiligingsincidenten

1. Elke gebeurtenis die gevolgen heeft of kan hebben voor de beveiliging van de router of van Epris, of kan leiden tot beschadiging of verlies van gegevens die daarin 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 gekomen of kan zijn gekomen.
2. Het beheer van beveiligingsincidenten is gericht op een snelle, doeltreffende en passende respons.
3. De lidstaten stellen hun bevoegde toezichthoudende autoriteiten onverwijld in kennis van beveiligingsincidenten.

Onverminderd artikel 34 van Verordening (EU) 2016/794 stelt Europol CERT-EU onverwijld, maar in ieder geval uiterlijk 24 uur nadat Europol ervan kennis heeft genomen, op de hoogte van significante cyberdreigingen, significante kwetsbaarheden en significante incidenten. Aan CERT-EU wordt inzake cyberdreigingen, cyberkwetsbaarheden en cyberincidenten onverwijld melding gemaakt van nuttige en passende technische details die proactieve opsporing, een respons op incidenten of beperkende maatregelen mogelijk maken.

Bij beveiligingsincidenten die verband houden met de centrale infrastructuur van de router stelt eu-LISA CERT-EU onverwijld, maar in ieder geval uiterlijk 24 uur nadat eu-LISA ervan kennis heeft genomen, op de hoogte van significante cyberdreigingen, significante kwetsbaarheden en significante incidenten. Aan CERT-EU wordt inzake cyberdreigingen, cyberkwetsbaarheden en cyberincidenten onverwijld melding gemaakt van nuttige en passende technische details die proactieve opsporing, een respons op incidenten of beperkende maatregelen mogelijk maken.

4. Informatie betreffende beveiligingsincidenten die gevolgen hebben of kunnen hebben voor de werking van de router of voor de beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens, wordt door de betrokken lidstaten en agentschappen van de Unie onverwijld verstrekt aan de lidstaten en Europol en gerapporteerd in overeenstemming met het door eu-LISA te verstrekken incidentenbeheerplan.
5. Informatie betreffende beveiligingsincidenten die gevolgen hebben of kunnen hebben voor de werking van Epris of voor de beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens, wordt door de betrokken lidstaten en agentschappen van de Unie onverwijld verstrekt aan de lidstaten en gerapporteerd in overeenstemming met het door Europol te verstrekken incidentenbeheerplan.

Interne monitoring

1. De lidstaten en de betrokken agentschappen van de Unie zorgen ervoor dat elke instantie met recht op toegang tot Prüm II de nodige maatregelen treft om haar naleving van deze verordening te monitoren en, indien nodig, samenwerkt met de toezichthoudende autoriteit.
2. De verwerkingsverantwoordelijken nemen de nodige maatregelen, waaronder frequente verificatie van de in de artikelen 40 en 45 bedoelde logbestanden, om na te gaan of de gegevens in overeenstemming met deze verordening worden verwerkt, en werken indien nodig samen met de toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming.

Artikel 57

Sancties

De lidstaten zorgen ervoor dat misbruik, verwerking of uitwisseling van gegevens in strijd met deze verordening strafbaar wordt gesteld volgens het nationale recht. De sancties moeten doeltreffend, evenredig en afschrikkend zijn.

Artikel 58

Bewijslast

1. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat personen die zich gediscrimineerd achten als gevolg van de verwerking of uitwisseling van hun persoonsgegevens, niet de bewijslast dragen. Wanneer een persoon van mening is dat die in het kader van een geautomatiseerde vergelijking uit hoofde van deze verordening voor een rechtbank of andere bevoegde rechterlijke instantie is gediscrimineerd, motiveren de lidstatelijke instanties die de gegevens hebben verwerkt, waarom er geen sprake was van discriminatie.
2. Lid 1 is niet van toepassing op strafprocedures.
3. De lidstaten treffen geen specifieke maatregelen in de zin van lid 1 bij procedures waarin het aan de rechter of bevoegde rechterlijke instantie is om de feiten van de zaak te onderzoeken.

Artikel 59

Aansprakelijkheid

Indien schade aan de router of aan Epris ontstaat doordat een lidstaat zijn verplichtingen uit hoofde van deze verordening niet is nagekomen, is deze lidstaat daarvoor aansprakelijk, tenzij en voor zover eu-LISA, Europol of een andere door deze verordening gebonden lidstaat heeft nagelaten redelijke stappen te ondernemen om het optreden van de schade te voorkomen of de omvang ervan zo veel mogelijk te beperken.

Artikel 60

Audits door de Europese Toezichthouder voor gegevensbescherming

1. De Europese Toezichthouder voor gegevensbescherming zorgt ervoor dat voor de doeleinden van deze verordening ten minste om de vier jaar een audit van de verrichtingen van eu-LISA en Europol op het gebied van de verwerking van persoonsgegevens wordt uitgevoerd overeenkomstig de toepasselijke internationale auditnormen. Een verslag van die audit wordt toegezonden aan het Europees Parlement, de Raad, de Commissie, de lidstaten en het betrokken agentschap van de Unie. Voordat de verslagen worden aangenomen, worden Europol en eu-LISA in de gelegenheid gesteld opmerkingen te maken.
2. eu-LISA en Europol verstrekken de door de Europese Toezichthouder voor gegevensbescherming gevraagde informatie, verlenen de Europese Toezichthouder voor gegevensbescherming toegang tot alle documenten waarom hij verzoekt en tot hun in de artikelen 40 en 45 bedoelde logbestanden en verlenen de Europese toezichthouder voor gegevensbescherming te allen tijde toegang tot al hun gebouwen en terreinen.

Artikel 61

Samenwerking tussen de toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming

1. De toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming werken, elk binnen hun respectieve bevoegdheidsgebieden en binnen het kader van hun respectieve verantwoordelijkheden, actief met elkaar samen en zorgen voor gecoördineerd toezicht op de toepassing van deze verordening, met name wanneer de Europese Toezichthouder voor gegevensbescherming of een toezichthoudende autoriteit grote verschillen tussen praktijken van de lidstaten of potentieel onrechtmatige gegevensdoorgiften via de communicatiekanalen van Prüm II constateert.
2. In de in lid 1 van dit artikel bedoelde gevallen wordt gezorgd voor gecoördineerd toezicht in overeenstemming met artikel 62 van Verordening (EU) 2018/1725.
3. Uiterlijk op [twee jaar na de ingebruikneming van de router en Epris] en vervolgens om de twee jaar zendt het Europees Comité voor gegevensbescherming een gezamenlijk verslag van zijn activiteiten uit hoofde van dit artikel toe aan het Europees Parlement, de Raad, de Commissie, Europol en eu-LISA. Het verslag bevat voor elke lidstaat een hoofdstuk dat door de toezichthoudende autoriteit van de betrokken lidstaat wordt opgesteld.

Artikel 62

Verstrekking van persoonsgegevens aan derde landen en internationale organisaties

Gegevens die uit hoofde van deze verordening worden verwerkt, worden niet op geautomatiseerde wijze doorgegeven of ter beschikking gesteld aan derde landen of internationale organisaties.

HOOFDSTUK 7

VERANTWOORDELIJKHEDEN

Artikel 63

Verantwoordelijkheden van de lidstaten

1. Elke lidstaat is verantwoordelijk voor:
 - a) de aansluiting op de infrastructuur van de router;
 - b) de integratie van de bestaande nationale systemen en infrastructuur met de router;
 - c) de organisatie, het beheer, de werking en het onderhoud van de bestaande nationale infrastructuur en de aansluiting daarvan op de router;
 - d) de aansluiting op de infrastructuur van Epris;
 - e) de integratie van de bestaande nationale systemen en infrastructuur met Epris;
 - f) de organisatie, het beheer, de werking en het onderhoud van de bestaande nationale infrastructuur en de aansluiting daarvan op Epris;
 - g) het beheer en de regelingen op grond waarvan de naar behoren gemachtigde personeelsleden van de bevoegde nationale instanties overeenkomstig deze verordening toegang hebben tot de

- router en de opstelling en regelmatige bijwerking van een lijst van de betrokken personeelsleden en hun profielen;
- h) het beheer en de regelingen op grond waarvan de naar behoren gemachtigde personeelsleden van de bevoegde nationale instanties overeenkomstig deze verordening toegang hebben tot Epris en de opstelling en regelmatige bijwerking van een lijst van de betrokken personeelsleden en hun profielen;
 - i) het beheer en de regelingen op grond waarvan de naar behoren gemachtigde personeelsleden van de bevoegde nationale instanties overeenkomstig deze verordening toegang hebben tot Eucaris en de opstelling en regelmatige bijwerking van een lijst van de betrokken personeelsleden en hun profielen;
 - j) de manuele bevestiging van een match als bedoeld in artikel 6, lid 3, artikel 7, lid 3, artikel 13, lid 2, artikel 22, lid 2, en artikel 26, lid 2;
 - k) het verzekeren van de beschikbaarheid van de gegevens die nodig zijn voor de uitwisseling van gegevens overeenkomstig artikel 6, artikel 7, artikel 13, artikel 18, artikel 22 en artikel 26;
 - l) de uitwisseling van informatie overeenkomstig artikel 6, artikel 7, artikel 13, artikel 18, artikel 22 en artikel 26;
 - m) het wissen van gegevens die van een aangezochte lidstaat zijn ontvangen, binnen 48 uur nadat de aangezochte lidstaat heeft gemeld dat de verstrekte persoonsgegevens onjuist, niet meer actueel of onrechtmatig doorgegeven zijn;
 - n) de naleving van de bij deze verordening vastgestelde vereisten inzake gegevenskwaliteit.

2. Elke lidstaat is verantwoordelijk voor het aansluiten van zijn bevoegde nationale autoriteiten op de router, Epris en Eucaris.

Artikel 64

Verantwoordelijkheden van Europol

1. Europol is verantwoordelijk voor het beheer van de toegang van zijn naar behoren gemachtigde personeelsleden tot de router, Epris en Eucaris overeenkomstig deze verordening, en voor de daarvoor geldende regelingen.
2. Europol is ook verantwoordelijk voor de verwerking van bevragingen van Europolgegevens door de router. Europol past zijn informatiesystemen dienovereenkomstig aan.
3. Europol is verantwoordelijk voor alle technische aanpassingen van de infrastructuur van Europol die vereist zijn om de verbinding met de router en met Eucaris tot stand te brengen.
4. Europol is verantwoordelijk voor de ontwikkeling van Epris in samenwerking met de lidstaten. Epris voorziet in de in de artikelen 42 tot en met 46 vastgestelde functionaliteiten.

Europol zorgt voor het technisch beheer van Epris. Het technisch beheer van Epris omvat alle taken en technische oplossingen die nodig zijn om de centrale infrastructuur van Epris 24 uur per dag en zeven dagen per week overeenkomstig deze verordening te laten functioneren en ononderbroken diensten te laten verlenen aan de lidstaten. Het omvat ook de onderhoudswerkzaamheden en technische ontwikkelingen die nodig zijn voor een toereikende technische kwaliteit van de werking van Epris, in

het bijzonder wat betreft de tijd die nodig is voor het raadplegen van de nationale databanken overeenkomstig de technische specificaties.

5. Europol verzorgt opleidingen voor het technisch gebruik van Epris.

6. Europol is verantwoordelijk voor de in de artikelen 49 en 50 bedoelde procedures.

Artikel 65

Verantwoordelijkheden van eu-LISA gedurende de ontwerp- en ontwikkelingsfase van de router

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

2. De router wordt door eu-LISA gehost op zijn technische locaties en voorziet in de in deze verordening beschreven functies overeenkomstig de voorwaarden inzake beveiliging, beschikbaarheid, kwaliteit en prestaties bedoeld in artikel 66, lid 1.

3. eu-LISA is verantwoordelijk voor de ontwikkeling van de router en voor alle technische aanpassingen die nodig zijn voor de werking van de router.

eu-LISA heeft geen toegang tot persoonsgegevens die via de router worden verwerkt.

eu-LISA bepaalt het ontwerp van de fysieke architectuur van de router, met inbegrip van de communicatie-infrastructuur en de technische specificaties alsmede de evolutie daarvan met betrekking tot de centrale infrastructuur en de beveiligde communicatie-infrastructuur. Dit ontwerp wordt vastgesteld door de raad van bestuur, na een gunstig advies van de Commissie. eu-LISA voert ook alle noodzakelijke aanpassingen aan de interoperabiliteitscomponenten uit die voortvloeien uit de instelling van de router overeenkomstig deze verordening.

eu-LISA ontwikkelt en implementeert de router zo spoedig mogelijk nadat de Commissie de in artikel 37, lid 6, bedoelde maatregelen heeft vastgesteld.

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

4. Tijdens de ontwerp- en ontwikkelingsfase komt de in artikel 54 van Verordening (EU) 2019/817 en artikel 54 van Verordening (EU) 2019/818 bedoelde programmabestuurraad inzake interoperabiliteit regelmatig bijeen. De programmabestuurraad zorgt voor passend beheer van de ontwerp- en ontwikkelingsfase van de router.

Maandelijks brengt de programmabestuurraad schriftelijk verslag uit over de voortgang van het project aan de raad van bestuur van eu-LISA. De programmabestuurraad heeft geen beslissingsbevoegdheid, noch een mandaat om de leden van de raad van bestuur van eu-LISA te vertegenwoordigen.

Tot de ingebruikneming van de router komt de in artikel 77 bedoelde adviesgroep op gezette tijden bijeen. Zij brengt na elke bijeenkomst verslag uit aan de programmabestuurraad. Zij ondersteunt de programmabestuurraad met technische deskundigheid en houdt de voortgang van de voorbereidingen van de lidstaten bij.

Verantwoordelijkheden van eu-LISA na de ingebruikneming van de router

1. Na de ingebruikneming van de router is eu-LISA verantwoordelijk voor het technisch beheer van de centrale infrastructuur van de router, met inbegrip van het onderhoud en de technische ontwikkelingen ervan. eu-LISA zorgt er in samenwerking met de lidstaten voor dat de beste beschikbare technologie wordt gebruikt, onder voorbehoud van een kosten-batenanalyse. eu-LISA is ook verantwoordelijk voor het technisch beheer van de noodzakelijke communicatie-infrastructuur.

Het technisch beheer van de router omvat alle taken en technische oplossingen die nodig zijn om de router 24 uur per dag en zeven dagen per week overeenkomstig deze verordening te laten functioneren en ononderbroken diensten te laten verlenen aan de lidstaten en aan Europol. Het omvat ook de onderhoudswerkzaamheden en technische ontwikkelingen die nodig zijn voor een toereikende technische kwaliteit van de werking van de router, in het bijzonder wat betreft de beschikbaarheid en de tijd die nodig is voor het indienen van verzoeken bij de nationale databanken en de Europolgegevens overeenkomstig de technische specificaties.

De router wordt zodanig ontwikkeld en beheerd dat snelle, efficiënte en gecontroleerde toegang, volledige en ononderbroken beschikbaarheid van de router en een responstijd overeenkomstig de operationele behoeften van de bevoegde instanties van de lidstaten en Europol worden gewaarborgd.

2. Onverminderd artikel 17 van het Statuut van de ambtenaren van de Europese Unie, zoals vastgesteld in Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad⁴², past eu-LISA passende voorschriften inzake het beroepsgeheim of een gelijkwaardige geheimhoudingsplicht toe op zijn personeelsleden die moeten werken met gegevens die zijn opgeslagen in de interoperabiliteitscomponenten. Deze geheimhoudingsplicht blijft ook gelden nadat deze personeelsleden hun functie of dienstverband hebben beëindigd of hun werkzaamheden hebben stopgezet.

eu-LISA heeft geen toegang tot persoonsgegevens die via de router worden verwerkt.

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

HOOFDSTUK 8

WIJZIGINGEN VAN ANDERE BESTAANDE INSTRUMENTEN

Artikel 67

Wijzigingen van Besluit 2008/615/JBZ en Besluit 2008/616/JBZ

1. Wat de door deze verordening gebonden lidstaten betreft, worden de artikelen 2 tot en met 6 en de afdelingen 2 en 3 van hoofdstuk 2 van Besluit 2008/615/JBZ vervangen vanaf de datum waarop de bepalingen van deze verordening met betrekking tot de router van toepassing worden zoals bepaald in artikel 74.

Derhalve worden de artikelen 2 tot en met 6 en de afdelingen 2 en 3 van hoofdstuk 2 van Besluit 2008/615/JBZ geschrapt vanaf de datum waarop de bepalingen van deze verordening met betrekking tot de router van toepassing worden zoals bepaald in artikel 74.

⁴² PB L 56 van 4.3.1968, blz. 1.

2. Wat de door deze verordening gebonden lidstaten betreft, worden de hoofdstukken 2 tot en met 5 en de artikelen 18, 20 en 21 van Besluit 2008/616/JBZ vervangen vanaf de datum waarop de bepalingen van deze verordening met betrekking tot de router van toepassing worden zoals bepaald in artikel 74.

Derhalve worden de hoofdstukken 2 tot en met 5 en de artikelen 18, 20 en 21 van Besluit 2008/616/JBZ geschrapt vanaf de datum waarop de bepalingen van deze verordening met betrekking tot de router van toepassing worden zoals bepaald in artikel 74.

Artikel 68

Wijzigingen van Verordening (EU) 2018/1726

Verordening (EU) 2018/1726 wordt als volgt gewijzigd:

- (1) Het volgende artikel 13 bis wordt ingevoegd:

“Artikel 13 bis

Taken in verband met de router

Met betrekking tot Verordening (EU) .../... van het Europees Parlement en de Raad* [*deze verordening*] voert het Agentschap de hem bij die verordening opgedragen taken uit die verband houden met de router.

* Verordening (EU) [nummer] van het Europees Parlement en de Raad van xy betreffende [officieel vastgestelde benaming] (PB L ...)”

- (2) In artikel 17 wordt lid 3 vervangen door:

“3. De zetel van het Agentschap is in Tallinn, Estland.

De in artikel 1, leden 4 en 5, de artikelen 3 tot en met 8 en de artikelen 9, 11 en 13 bis bedoelde taken in verband met ontwikkeling en operationeel beheer worden verricht in de technische locatie in Straatsburg, Frankrijk.

In Sankt Johann im Pongau, Oostenrijk, wordt een back-uplocatie gevestigd die kan zorgen voor het operationeel blijven van een grootschalig IT-systeem in geval van falen van een dergelijk systeem.”

Artikel 69

Wijzigingen van Verordening (EU) 2019/817

Aan artikel 6, lid 2, van Verordening (EU) 2019/817 wordt het volgende punt d) toegevoegd:

“d) een beveiligde communicatie-infrastructuur tussen het ESP en de router die is opgezet bij Verordening (EU) .../... van het Europees Parlement en de Raad* [*deze verordening*].

* Verordening (EU) [nummer] van het Europees Parlement en de Raad van xy betreffende [officieel vastgestelde benaming] (PB L ...)”

Wijzigingen van Verordening (EU) 2019/818

Verordening (EU) 2019/818 wordt als volgt gewijzigd:

- (1) Aan artikel 6, lid 2, wordt het volgende punt d) toegevoegd:

“d) een beveiligde communicatie-infrastructuur tussen het ESP en de router die is opgezet bij Verordening (EU) .../... van het Europees Parlement en de Raad* [*deze verordening*].

* Verordening (EU) [nummer] van het Europees Parlement en de Raad van xy betreffende [officieel vastgestelde benaming] (PB L ...)”

- (2) In artikel 39 worden de leden 1 en 2 vervangen door:

“1. Er wordt een centraal register voor rapportage en statistieken (CRRS) ingesteld om de doelstellingen van Eurodac, SIS en Ecris-TCN in overeenstemming met de voor die systemen respectievelijk geldende rechtsinstrumenten te ondersteunen en om te voorzien in systeemoverschrijdende statistische gegevens en analytische verslagen voor doeleinden op het gebied van beleid, operationaliteit en gegevenskwaliteit. Het CRRS ondersteunt tevens de doelstellingen van Prüm II.”

“2. eu-LISA zorgt op zijn technische locaties voor het opstellen, implementeren en hosten van het CRRS, met daarin de logisch per Unie-informatiesysteem gescheiden gegevens en statistieken als bedoeld in artikel 74 van Verordening (EU) 2018/1862 en artikel 32 van Verordening (EU) 2019/816. eu-LISA verzamelt tevens de gegevens en statistieken van de router als bedoeld in artikel 65, lid 1, van Verordening (EU) .../...* [*deze verordening*]. Toegang tot het CRRS wordt uitsluitend met het oog op het opstellen van rapporten en statistieken verleend aan de in artikel 74 van Verordening (EU) 2018/1862, artikel 32 van Verordening (EU) 2019/816 en artikel 65, lid 1, van Verordening (EU) .../... [*deze verordening*] bedoelde instanties door middel van gecontroleerde en beveiligde toegang en specifieke gebruikersprofielen.”

HOOFDSTUK 9

SLOTBEPALINGEN

Verslagen en statistieken

1. De naar behoren gemachtigde personeelsleden van de bevoegde lidstatelijke instanties, de Commissie, Europol en eu-LISA mogen, uitsluitend met het oog op het opstellen van verslagen en statistieken, de volgende gegevens inzake de router raadplegen:

- a) het aantal zoekopdrachten van elke lidstaat en van Europol;
- b) het aantal zoekopdrachten voor elke categorie gegevens;
- c) het aantal zoekopdrachten voor elke aangesloten databank;
- d) het aantal matches met de databank van elke lidstaat per gegevenscategorie;
- e) het aantal matches met Europolgegevens per gegevenscategorie;

- f) het aantal bevestigde matches naar aanleiding waarvan kerngegevens werden uitgewisseld; en
- g) het aantal zoekopdrachten via de router in het gemeenschappelijk identiteitsregister.

Het mag niet mogelijk zijn om personen te identificeren op basis van de gegevens.

2. De naar behoren gemachtigde personeelsleden van de bevoegde lidstatelijke instanties, Europol en de Commissie mogen, uitsluitend met het oog op het opstellen van verslagen en statistieken, de volgende gegevens inzake Eucaris raadplegen:

- a) het aantal zoekopdrachten van elke lidstaat en van Europol;
- b) het aantal zoekopdrachten voor elke aangesloten databank; en
- c) het aantal matches met de databank van elke lidstaat.

Het mag niet mogelijk zijn om personen te identificeren op basis van de gegevens.

3. De naar behoren gemachtigde personeelsleden van de bevoegde lidstatelijke instanties, de Commissie en eu-LISA mogen, uitsluitend met het oog op het opstellen van verslagen en statistieken, de volgende gegevens inzake Epris raadplegen:

- a) het aantal zoekopdrachten van elke lidstaat en van Europol;
- b) het aantal zoekopdrachten voor elk aangesloten register; en
- c) het aantal matches met de databank van elke lidstaat.

Het mag niet mogelijk zijn om personen te identificeren op basis van de gegevens.

4. eu-LISA slaat de in die leden bedoelde gegevens op.

De gegevens stellen de in lid 1 bedoelde autoriteiten in staat op maat gesneden verslagen en statistieken te verkrijgen om de doeltreffendheid van de samenwerking op het gebied van rechtshandhaving te verbeteren.

Artikel 72

Kosten

1. De kosten in verband met de instelling en werking van de router en Epris komen ten laste van de algemene begroting van de Unie.

2. De kosten in verband met de integratie van de bestaande nationale infrastructuren en de verbinding daarvan met de router en met Epris, alsmede de kosten in verband met het opzetten van nationale databanken voor gezichtsopnamen en nationale politieregisters voor het voorkomen, opsporen en onderzoeken van strafbare feiten 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) de exploitatie van nationale IT-systemen (exploitanten en contracten voor ondersteuning);
- d) het ontwerp, de ontwikkeling, de implementatie, de exploitatie en het onderhoud van nationale communicatienetwerken.

3. Elke lidstaat draagt de eigen kosten in verband met de administratie, het gebruik en het onderhoud van de in artikel 19, lid 1, vermelde softwaretoepassing Eucaris.

4. Elke lidstaat draagt de eigen kosten in verband met de administratie, het gebruik en het onderhoud van zijn verbindingen met de router en met Epris.

Artikel 73

Kennisgevingen

1. De lidstaten stellen eu-LISA in kennis van de in artikel 36 bedoelde instanties die gebruik kunnen maken van of toegang hebben tot de router.
2. eu-LISA stelt de Commissie in kennis van de succesvolle afsluiting van de in artikel 74, lid 1, punt b), bedoelde test.
3. De lidstaten stellen de Commissie, Europol en eu-LISA in kennis van de nationale contactpunten.

Artikel 74

Ingebruikneming

1. De Commissie stelt door middel van een uitvoeringshandeling de datum vast waarop de lidstaten en de agentschappen van de Unie de router in gebruik mogen nemen, zodra aan de volgende voorwaarden is voldaan:

- a) de in artikel 37, lid 6, bedoelde maatregelen zijn goedgekeurd;
- b) eu-LISA heeft verklaard dat een uitgebreide test van de router, die eu-LISA samen met de lidstatelijke instanties en Europol heeft uitgevoerd, met succes is afgesloten.

In die uitvoeringshandeling stelt de Commissie ook de datum vast waarop de lidstaten en de agentschappen van de Unie de router in gebruik moeten nemen. Die datum valt één jaar na de uit hoofde van de eerste alinea bepaalde datum.

De Commissie kan de datum waarop de lidstaten en de agentschappen van de Unie de router in gebruik moeten nemen, met ten hoogste één jaar uitstellen, indien uit een beoordeling van de implementatie van de router is gebleken dat een dergelijk uitstel noodzakelijk is. De uitvoeringshandeling wordt vastgesteld volgens de procedure van artikel 76, lid 2.

2. De Commissie stelt door middel van een uitvoeringshandeling de datum vast waarop de lidstaten en de agentschappen van de Unie Epris in gebruik mogen nemen, zodra aan de volgende voorwaarden is voldaan:

- a) de in artikel 44, lid 7, bedoelde maatregelen zijn goedgekeurd;
- b) Europol heeft verklaard dat een uitgebreide test van Epris, die Europol samen met de lidstatelijke instanties heeft uitgevoerd, met succes is afgesloten.

3. De Commissie stelt door middel van een uitvoeringshandeling de datum vast vanaf welke Europol, overeenkomstig artikel 49, uit derde landen afkomstige biometrische gegevens ter beschikking van de lidstaten moet stellen, zodra aan de volgende voorwaarden is voldaan:

- a) de router is in gebruik genomen;
- b) Europol heeft verklaard dat een uitgebreide test van de verbinding, die Europol samen met de lidstatelijke instanties en eu-LISA heeft uitgevoerd, met succes is afgesloten.

4. De Commissie stelt door middel van een uitvoeringshandeling de datum vast vanaf welke Europol, overeenkomstig artikel 50, toegang moet krijgen tot in de databanken van de lidstaten opgeslagen gegevens, zodra aan de volgende voorwaarden is voldaan:

- a) de router is in gebruik genomen;
- b) Europol heeft verklaard dat een uitgebreide test van de verbinding, die Europol samen met de lidstatelijke instanties en eu-LISA heeft uitgevoerd, met succes is afgesloten.

Artikel 75

Overgangsbepalingen en afwijkingen

1. De lidstaten en de agentschappen van de Unie passen de artikelen 21 tot en met 24, artikel 47 en artikel 50, lid 6, toe met ingang van de overeenkomstig artikel 74, lid 1, eerste alinea, bepaalde datum, met uitzondering van de lidstaten die de router niet in gebruik hebben genomen.
2. De lidstaten en de agentschappen van de Unie passen de artikelen 25 tot en met 28 en artikel 50, lid 4, toe met ingang van de overeenkomstig artikel 74, lid 2, bepaalde datum.
3. De lidstaten en de agentschappen van de Unie passen artikel 49 toe met ingang van de overeenkomstig artikel 74, lid 3, bepaalde datum.
4. De lidstaten en de agentschappen van de Unie passen artikel 50, leden 1, 2, 3, 5 en 7, toe met ingang van de overeenkomstig artikel 74, lid 4, bepaalde datum.

Artikel 76

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. Indien door het comité geen advies wordt uitgebracht, neemt de Commissie de ontwerpsluitvoeringshandeling niet aan en is artikel 5, lid 4, derde alinea, van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 77

Adviesgroep

De taken van de adviesgroep inzake interoperabiliteit van eu-LISA strekken zich uit tot de router. De adviesgroep inzake interoperabiliteit levert aan eu-LISA expertise met betrekking tot de router, in het bijzonder bij de opstelling van het jaarlijkse werkprogramma en het jaarlijkse activiteitenverslag.

Artikel 78

Praktische handleiding

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

Monitoring en evaluatie

1. eu-LISA en Europol zorgen ervoor dat er procedures voorhanden zijn om respectievelijk de ontwikkeling van de router en van Epris te monitoren in het licht van de doelstellingen op het gebied van planning en kosten, en de werking van de router en van Epris te monitoren in het licht van de doelstellingen op het gebied van de technische resultaten, de kosteneffectiviteit, de beveiliging en de kwaliteit van de dienstverlening.

2. Uiterlijk *[een jaar na de inwerkingtreding van deze verordening]*, en vervolgens ieder jaar tijdens de ontwikkelingsfase van de router, brengt eu-LISA respectievelijk aan het Europees Parlement en de Raad verslag uit over de stand van zaken van de ontwikkeling van de router. In dat verslag wordt gedetailleerde informatie opgenomen over de gemaakte kosten en informatie over eventuele risico's die van invloed kunnen zijn op de totale kosten die overeenkomstig artikel 72 ten laste komen van de algemene begroting van de Unie.

Wanneer de ontwikkeling van de router is afgerond, dient eu-LISA bij het Europees Parlement en de Raad een verslag in waarin uitvoerig wordt uiteengezet hoe de doelstellingen, met name die welke betrekking hebben op planning en kosten, zijn bereikt en waarin eventuele afwijkingen worden gerechtvaardigd.

3. Uiterlijk *[een jaar na de inwerkingtreding van deze verordening]* en vervolgens ieder jaar tijdens de ontwikkelingsfase van Epris brengt Europol aan het Europees Parlement en de Raad verslag uit over de stand van de voorbereidingen voor de uitvoering van deze verordening en over de stand van zaken bij de ontwikkeling van Epris, met inbegrip van gedetailleerde informatie over de gemaakte kosten en informatie over eventuele risico's die van invloed kunnen zijn op de totale kosten die overeenkomstig artikel 72 ten laste komen van de algemene begroting van de Unie.

Wanneer de ontwikkeling van Epris is afgerond, dient Europol bij het Europees Parlement en de Raad een verslag in waarin uitvoerig wordt uiteengezet hoe de doelstellingen, met name die welke betrekking hebben op planning en kosten, zijn bereikt en waarin eventuele afwijkingen worden gerechtvaardigd.

4. Met het oog op het technisch onderhoud hebben eu-LISA en Europol toegang tot de vereiste informatie over de in de router respectievelijk in Epris uitgevoerde gegevensverwerkingsverrichingen.

5. Twee jaar na de ingebruikneming van de router, en vervolgens om de twee jaar, brengt eu-LISA aan het Europees Parlement, de Raad en de Commissie verslag uit over de technische werking en de beveiliging van de router.

6. Twee jaar na de ingebruikneming van Epris, en vervolgens om de twee jaar, brengt Europol aan het Europees Parlement, de Raad en de Commissie verslag uit over de technische werking en de beveiliging van Epris.

7. Drie jaar na de ingebruikneming van de router en Epris zoals bedoeld in artikel 74, en vervolgens om de vier jaar, verricht de Commissie een algemene evaluatie van Prüm II, met inbegrip van:

- a) een beoordeling van de toepassing van deze verordening;
- b) een toetsing van de bereikte resultaten aan de doelstellingen van deze verordening en een beoordeling van de gevolgen ervan voor de grondrechten;
- c) het effect, de effectiviteit en de efficiëntie van de activiteiten en werkmethoden van Prüm II in het licht van zijn doelstellingen, mandaat en taken;
- d) een beoordeling van de beveiliging van Prüm II.

De Commissie zendt het verslag van de evaluatie toe aan het Europees Parlement, de Raad, de Europese Toezichthouder voor gegevensbescherming en het Bureau van de Europese Unie voor de grondrechten.

8. De lidstaten en Europol verstrekken eu-LISA en de Commissie de informatie die nodig is om de in de leden 2 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.

9. De lidstaten verstrekken Europol en de Commissie de informatie die nodig is om de in de leden 3 en 6 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.

10. De lidstaten, eu-LISA en Europol verstrekken de Commissie de informatie die nodig is om de in lid 7 bedoelde evaluaties op te stellen. De lidstaten delen de Commissie ook het aantal bevestigde matches met de databank van elke lidstaat per gegevenscategorie mee.

Artikel 80

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*.

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

Gedaan te Brussel,

Voor het Europees Parlement
De voorzitter

Voor de Raad
De voorzitter

FINANCIEEL MEMORANDUM

1. KADER VAN HET WETGEVINGSINITIATIEF

1.1. Titel van het wetgevingsinitiatief

Voorstel voor een verordening van het Europees Parlement en de Raad betreffende geautomatiseerde gegevensuitwisseling ten behoeve van politieke samenwerking ("Prüm II") en tot wijziging van de Besluiten 2008/615/JBZ en 2008/616/JBZ van de Raad en de Verordeningen (EU) 2018/1726, (EU) 2019/817 en (EU) 2019/818 van het Europees Parlement en de Raad

1.2. Betrokken beleidsterrein(en)

Beleidssterrein: Binnenlandse Zaken

Activiteit: veiligheid

1.3. Het voorstel betreft

- ☐ een nieuwe actie
- ☐ een nieuwe actie na een proefproject / voorbereidende actie⁴³
- ☒ de verlenging van een bestaande actie
- ☐ een samenvoeging van één of meer acties tot een andere / een nieuwe actie

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

Dit initiatief is genomen in reactie op dringende operationele behoeften en naar aanleiding van verzoeken van de Raad om een herziening van de Prüm-besluiten⁴⁴ te overwegen teneinde het toepassingsgebied ervan uit te breiden en de nodige technische en wettelijke vereisten te actualiseren. Het initiatief zal naar verwachting de geautomatiseerde uitwisseling van gegevens in het kader van het Prüm-kader versterken met het oog op het verlenen van bijstand aan de rechtshandavingsinstanties van de lidstaten die belast zijn met criminaliteitsbestrijding.

1.4.2. Specifieke doelstelling(en)

Met het initiatief worden de volgende doelstellingen nagestreefd:

- 1) **Specifieke doelstelling I:** voorzien in een technische oplossing voor efficiënte geautomatiseerde uitwisseling van gegevens tussen rechtshandavingsinstanties, teneinde deze op de hoogte te stellen van relevante gegevens die beschikbaar zijn in de nationale databank van een andere lidstaat;
- 2) **Specifieke doelstelling II:** ervoor zorgen dat een grotere hoeveelheid relevante gegevens (namelijk gezichtsopnamen en politiegegevens) afkomstig uit de nationale databanken in andere lidstaten beschikbaar is voor alle bevoegde rechtshandavingsinstanties in de EU;

⁴³ In de zin van artikel 58, lid 2, punt a) of b), van het Financieel Reglement.

⁴⁴ Besluiten 2008/615/JBZ en 2008/616/JBZ van de Raad.

- 3) **Specifieke doelstelling III:** ervoor zorgen dat relevante gegevens (in termen van gegevensbronnen) afkomstig uit de databank van Europol beschikbaar zijn voor de nationale rechtshandavingsinstanties en dat Europol de gegevens waarover het beschikt, ten volle benut;
- 4) **Specifieke doelstelling IV:** rechtshandavingsinstanties efficiënte toegang bieden tot de feitelijke gegevens die overeenkomen met een “hit” in de nationale databank van een andere lidstaat of Europol.

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

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

Het initiatief zal de vastgestelde problemen doeltreffend aanpakken en het huidige Prüm-kader versterken met krachtige gerichte aanvullende vermogens voor betere steunverlening aan de lidstaten, en wel door verbetering van de informatie-uitwisseling, met als einddoel dat strafbare feiten en terroristische misdrijven worden voorkomen en onderzocht met volledige inachtneming van de grondrechten.

De uiteindelijke begunstigden van alle voorkeursopties zijn de **burgers**, die direct en indirect baat zullen hebben bij **betere misdaadbestrijding en minder criminaliteit**. Wat efficiëntie betreft, zijn de belangrijkste begunstigden de **nationale rechtshandavingsinstanties**. Het initiatief voorziet in efficiënte oplossingen voor uitdagingen die anders tegen hogere kosten of met geringere efficiëntie zouden moeten worden aangepakt.

1.4.4. Prestatie-indicatoren

Vermeld de indicatoren voor de monitoring van de voortgang en de beoordeling van de resultaten

Met de ontwikkeling van de router en Epris zal worden begonnen zodra aan de voorwaarden is voldaan, dat wil zeggen zodra het wetgevingsvoorstel is goedgekeurd door de medewetgevers en de technische voorwaarden zijn vervuld. De werkzaamheden aan de router vormen een nieuw project, maar met de werkzaamheden aan Epris wordt voortgebouwd op het huidige ADEP.EPRIS-project.

Specifieke doelstelling: bedrijfsklaar zijn tegen de gestelde termijn

Uiterlijk in 2023 wordt het voorstel ter vaststelling toegezonden aan de medewetgevers. Op basis van de ervaring met het tijdsplan voor andere voorstellen wordt aangenomen dat het vaststellingsproces in 2024 zal worden afgerond.

Uitgaande van die veronderstelling wordt begin 2025 (=T0) gehanteerd als startpunt voor de ontwikkeling en als referentiepunt voor de berekening van perioden aan de hand van de duur ervan, en niet de absolute data. Als de medewetgevers de voorstellen op een later tijdstip vaststellen, verschuift het gehele tijdschema mee.

De ontwikkeling van de router en van Epris zal naar verwachting plaatsvinden in de loop van 2025 en 2026, en de ingebruikneming is gepland voor 2027.

Aan de hand van de volgende hoofdindicatoren kunnen de verwezenlijking van de specifieke doelstellingen en de prestaties ten aanzien daarvan worden gemonitord:

Specifieke doelstelling I: voorzien in een technische oplossing voor efficiënte geautomatiseerde uitwisseling van gegevens.

- het aantal verzoeken voor zoekopdrachten dat de router per tijdvak kan afhandelen (use cases executed);

- het aantal verzoeken voor zoekopdrachten dat Epris per tijdvak kan afhandelen (use cases executed).

Specifieke doelstelling II: ervoor zorgen dat een grotere hoeveelheid relevante gegevens beschikbaar is.

- het aantal verzoeken om zoekopdrachten met gezichtsopnamen;

- het aantal verzoeken om zoekopdrachten met politiegegevens;

- het aantal matches op zoekopdrachten met gezichtsopnamen;
- het aantal matches op zoekopdrachten met politiegegevens.

Specifieke doelstelling III: ervoor zorgen dat relevante gegevens (in termen van gegevensbronnen) afkomstig uit de databank van Europol beschikbaar zijn voor de nationale rechtshandavingsinstanties en dat Europol de gegevens waarover het beschikt, ten volle benut.

- het aantal verzoeken om bevraging van biometrische gegevens afkomstig van Europol uit derde landen;
- het aantal matches bij Europol met uit derde landen afkomstige biometrische gegevens;
- het aantal verzoeken om zoekopdrachten van Europol;
- het aantal matches naar aanleiding van zoekopdrachten van Europol.

Specifieke doelstelling IV: rechtshandavingsinstanties efficiënte toegang bieden tot de feitelijke gegevens die overeenkomen met een “hit” in de nationale databank van een andere lidstaat of Europol.

- het aantal matches naar aanleiding van verzoeken om zoekopdrachten, vergeleken met het aantal keren dat om uitwisseling van kerngegevens is verzocht.

1.5. Motivering van het wetgevingsinitiatief

1.5.1. *Behoeft(e)n waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitvoering van het wetgevingsinitiatief*

De uitvoering van het wetgevingsinitiatief vereist technische en procedurele maatregelen op EU- en nationaal niveau, die ervoor moeten zorgen dat de uitvoering kan beginnen zodra de herziene wetgeving in werking treedt. De relevante – met name personele – middelen moeten in de loop van de tijd worden opgehoogd in overeenstemming met de maatregelen.

De belangrijkste vereisten na de inwerkingtreding van het voorstel zijn als volgt.

Opzetten van de Prümrouter

voldoen aan de doelstelling om Prüm II-gebruikers in staat te stellen d.m.v. één verbinding een verzoek naar databanken van alle lidstaten en Europolgegevens te sturen voor zoekopdrachten met biometrische gegevens;

voorzien in een nieuw follow-upproces op EU-niveau waarbij na een “hit” semi-geautomatiseerde uitwisseling van feitelijke gegevens plaatsvindt.

Opzetten/uitbreiden van Epris

voldoen aan de doelstelling om Prüm II-gebruikers in staat te stellen d.m.v. één verbinding een verzoek naar databanken van alle lidstaten en Europolgegevens te sturen voor zoekopdrachten met biometrische gegevens.

De lidstaten in staat stellen nieuwe categorieën gegevens uit te wisselen

Uitwisseling van gezichtsopnamen en politiegegevens via Prüm II mogelijk maken.

De lidstaten in staat stellen uit derde landen afkomstige gegevens automatisch bij Europol te controleren via het Prümkader

De lidstaten in staat stellen biometrische gegevens uit derde landen te controleren via Prüm II.

Europol in staat stellen gegevens uit derde landen te vergelijken met de nationale databanken van de lidstaten

Europol in staat stellen aan de hand van gegevens uit derde landen de databanken van de lidstaten te doorzoeken via Prüm II.

Aangezien alle doelstellingen moeten worden verwezenlijkt, bestaat een volledige oplossing uit een combinatie van al het bovenstaande.

- 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 deelname van de Unie” verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die door een optreden van alleen de lidstaat zou zijn gecreëerd.*

Zware criminaliteit en terrorisme zijn transnationaal van aard. Maatregelen op nationaal niveau alleen zijn derhalve onvoldoende om deze doeltreffend te bestrijden. De lidstaten kiezen er daarom voor om in EU-verband samen te werken om de dreiging van zware criminaliteit en terrorisme aan te pakken.

De steeds veranderende veiligheidsdreigingen, die worden aangewakkerd door de uiteenlopende manieren waarop criminelen gebruikmaken van de mogelijkheden die de digitale transformatie, globalisering en mobiliteit bieden, vragen ook om doeltreffende steun op EU-niveau voor het werk van de nationale rechtshandhavingsinstanties. Dankzij het optreden van de EU kan de steun aan de lidstaten bij de bestrijding van zware criminaliteit en terrorisme op doeltreffende wijze worden opgevoerd om gelijke tred te houden met de ontwikkeling van de dreigingen.

Het voorstel zal aanzienlijke schaalvoordelen opleveren, doordat taken en diensten die efficiënter op EU-niveau kunnen worden uitgevoerd, worden overgeheveld van het nationale niveau naar Europol. Het voorstel voorziet daarom in efficiënte oplossingen voor problemen die anders, tegen hogere kosten, zouden moeten worden aangepakt met 27 afzonderlijke oplossingen op nationaal niveau, terwijl andere problemen vanwege hun transnationale aard in het geheel niet op nationaal niveau kunnen worden aangepakt.

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

Uit de evaluatie van de Prüm-besluiten is het volgende gebleken:

- Het Prümkader is relevant in het licht van de huidige en toekomstige behoeften en uitdagingen op het gebied van veiligheid en meer bepaald strafrechtelijk onderzoek. De samenwerking en uitwisseling van informatie tussen de rechtshandhavingsinstanties van de lidstaten en de mogelijkheid van het doorzoeken en vergelijken van DNA-gegevens, vingerafdrukgegevens en voertuigregistratiegegevens in databanken van andere lidstaten met het oog op het voorkomen en onderzoeken van strafbare feiten worden van het allergrootste belang geacht voor de bescherming van de binnenlandse veiligheid in de EU en de veiligheid van de burgers.

- Het concept van de Prüm-besluiten beantwoordt aan de behoeften van rechediensten, slachtoffers van misdrijven, forensische specialisten, databankbeheerders en juristen met betrekking tot de categorieën gegevens die in het Prüm-kader beschikbaar zijn.
- Door te voorkomen dat elke lidstaat bilateraal moet worden geraadpleegd, levert de geautomatiseerde uitwisseling van gegevens binnen het Prüm-kader efficiëntiewinst op bij de uitwisseling van rechtshandavingsinformatie, in die mate dat de uitwisseling sneller verloopt en de administratieve lasten tot op zekere hoogte afnemen. Deze voordelen blijken op te wegen tegen de investeringen die nodig zijn voor de uitvoering van het Prüm-kader. Het geautomatiseerde Prüm-systeem levert bovendien aanzienlijke besparingen op de arbeidstijd op. Er blijven echter administratieve lasten in verband met de verificatie van hits en rapportage, alsmede de ontvangst/verzending van informatie in de tweede fase.
- Sinds de vaststelling van de Prüm-besluiten in 2008 hebben zich ook aanzienlijke ontwikkelingen en veranderingen voorgedaan wat betreft het rechtskader van de EU, de operationele behoeften en de technische en forensische mogelijkheden. Er zijn op EU-niveau en op internationaal niveau diverse initiatieven en systemen ontwikkeld om de uitwisseling van informatie tussen rechtshandavingsinstanties te vergemakkelijken. De Prüm-besluiten zijn grotendeels complementair met andere relevante internationale en EU-wetgeving, waaronder het interoperabiliteitskader. Er zijn ook complementaire elementen met enkele van de centrale informatiesystemen van de EU, die voor uiteenlopende doeleinden zijn opgezet. Er kunnen potentiële synergieën worden vastgesteld met betrekking tot Europol en het interoperabiliteitskader.
- De uitvoering van de Prüm-besluiten verloopt echter traag. Momenteel, bijna tien jaar na de uitvoeringsdeadline van 26 augustus 2011, hebben nog steeds niet alle lidstaten de evaluatieprocedure afgerond en zijn sommige bilaterale verbindingen niet tot stand gekomen wegens de technische complexiteit en de aanzienlijke financiële en personele middelen die ermee gemoeid zijn. Daardoor kunnen zoekopdrachten in sommige lidstaten niet worden uitgevoerd als de desbetreffende bilaterale verbinding niet tot stand is gebracht. Dit belemmert het vermogen om criminelen te identificeren en grensoverschrijdende verbanden tussen misdrijven op te sporen, hetgeen de uitwisseling van informatie en de werking van het Prüm-systeem belemmert.
- Het feit dat de follow-up van hits binnen het Prüm-kader plaatsvindt krachtens het nationale recht en derhalve buiten het toepassingsgebied van de Prüm-besluiten valt, is ook genoemd als een probleem dat de werking van het Prüm-systeem belemmert. Door de uiteenlopende nationale regels en procedures is de uitwisseling van follow-upinformatie na een hit gefragmenteerd, in die zin dat het soms weken of zelfs maanden duurt om de relevante informatie naar aanleiding van een hit te ontvangen.

1.5.4. *Verenigbaarheid met het meerjarige financiële kader en eventuele synergie met andere passende instrumenten*

De op EU-niveau vereiste investeringen zijn verenigbaar met het meerjarig financieel kader 2021–2027. De financiering vindt plaats in het kader van de rubriek Veiligheid en defensie en de rubriek Migratie en grenzen.

1.5.5. *Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking*

In de ter financiering van het Prüm II-kader vereiste kredieten is niet voorzien in het kader van de MFK-toewijzingen aan Europol en eu-LISA, aangezien dit een nieuw voorstel betreft

waarvoor op dat moment nog geen bedragen bekend waren. Voorgesteld wordt de toewijzingen aan Europol en eu-LISA voor de jaren 2024, 2025, 2026 en 2027 te verhogen door overeenkomstige verlagingen van respectievelijk het Fonds voor interne veiligheid (ISF) en het Instrument voor grensbeheer en visumbeleid (BMVI).

1.6. Duur en financiële gevolgen van het wetgevingsinitiatief

☐ **beperkte geldigheidsduur**

☐ Voorstel/initiatief van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ

☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ

☒ **onbeperkte geldigheidsduur**

Uitvoering met een opstartperiode van 2024 tot en met 2026,
gevolgd door een volledige uitvoering.

1.7. Beheersvorm(en)⁴⁵

☒ **Direct beheer** door de Commissie

☒ 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:

☐ internationale organisaties en hun agentschappen (geef aan welke);

☐ de EIB en het Europees Investeringsfonds;

☒ de in de artikelen 70 en 71 bedoelde organen;

☐ publiekrechtelijke organen;

☐ privaatrechtelijke organen met een openbare dienstverleningstaak, 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.

Opmerkingen

Blok	Ontwikkelings- fase	Operationele fase	Beheersvorm	Uitvoerder
Ontwikkeling en onderhoud (van de router en Epris)	X	X	Indirect	eu-LISA Europol
Aanpassing van de Europoldatabanken	X	X	Indirect	Europol

⁴⁵ 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>

Blok	Ontwikkelings- fase	Operationele fase	Beheersvorm	Uitvoerder
Ontwikkeling of verbetering van bestaande nationale databanken, integratie van nationale systemen	X	X	Gedeeld (of direct)	COM + lidstaten

De ontwikkelingsfase begint in 2024 en duurt tot de oplevering van ieder onderdeel van het initiatief, vanaf 2024 tot en met 2027.

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 met het oog op de aansluiting op de router en Epris en zullen zij de nodige maatregelen moeten treffen om de uitwisseling van gezichtsopnamen en politiegegevens te waarborgen.

3. Indirect beheer: eu-LISA en Europol zullen zorgen voor het onderdeel ontwikkeling van de IT-componenten van het project, d.w.z. respectievelijk de router en Epris. Dit omvat alle noodzakelijke wijzigingen van hun bestaande architectuur om voor de in het voorstel beschreven capaciteiten te waarborgen.

Tijdens de operationele fase zullen eu-LISA en Europol alle technische activiteiten uitvoeren die verband houden met het onderhoud van respectievelijk de router en Epris.

Europol zal zorgen voor de ontwikkeling en het onderhoud van zijn systemen om de beschikbaarheid van Europolgegevens in de context van het Prüm-kader te waarborgen.

2. BEHEERSMAATREGELEN

2.1. Regels inzake monitoring en rapportage

Vermeld frequentie en voorwaarden.

eu-LISA en Europol zorgen ervoor dat er procedures voorhanden zijn om respectievelijk de ontwikkeling van de router en van Epris te monitoren in het licht van de doelstellingen op het gebied van planning en kosten, en de werking van de router en van Epris te monitoren in het licht van de doelstellingen op het gebied van de technische resultaten, de kosteneffectiviteit, de beveiliging en de kwaliteit van de dienstverlening.

Uiterlijk een jaar na de vaststelling van de voorgestelde verordening, en vervolgens ieder jaar tijdens de ontwikkelingsfase van de router, brengt eu-LISA aan het Europees Parlement en de Raad verslag uit over de stand van zaken van de ontwikkeling van de router. In dat verslag wordt gedetailleerde informatie opgenomen over de gemaakte kosten en informatie over eventuele risico's die van invloed kunnen zijn op de totale kosten die ten laste komen van de algemene begroting van de Unie.

Wanneer de ontwikkeling van de router is afgerond, dient eu-LISA bij het Europees Parlement en de Raad een verslag in waarin uitvoerig wordt uiteengezet hoe de doelstellingen, met name die welke betrekking hebben op planning en kosten, zijn bereikt en waarin eventuele afwijkingen worden gerechtvaardigd.

Uiterlijk een jaar na de vaststelling van de voorgestelde verordening en vervolgens ieder jaar tijdens de ontwikkelingsfase van Epris brengt Europol aan het Europees Parlement en de Raad verslag uit over de stand van de voorbereidingen voor de uitvoering van deze verordening en over de stand van zaken bij de ontwikkeling van Epris, met inbegrip van gedetailleerde informatie over de gemaakte kosten en informatie over eventuele risico's die van invloed kunnen zijn op de totale kosten die ten laste komen van de algemene begroting van de Unie.

Wanneer de ontwikkeling van Epris is afgerond, dient Europol bij het Europees Parlement en de Raad een verslag in waarin uitvoerig wordt uiteengezet hoe de doelstellingen, met name die welke betrekking hebben op planning en kosten, zijn bereikt en waarin eventuele afwijkingen worden gerechtvaardigd.

Met het oog op het technisch onderhoud hebben eu-LISA en Europol toegang tot de vereiste informatie over de in de router respectievelijk in Epris uitgevoerde gegevensverwerkingsverrichtingen.

Twee jaar na de ingebruikneming van de router, en vervolgens om de twee jaar, brengt eu-LISA aan het Europees Parlement, de Raad en de Commissie verslag uit over de technische werking en de beveiliging van de router.

Twee jaar na de ingebruikneming van Epris, en vervolgens om de twee jaar, brengt Europol aan het Europees Parlement, de Raad en de Commissie verslag uit over de technische werking en de beveiliging van Epris.

Drie jaar na de ingebruikneming van alle onderdelen van de voorgestelde verordening, en vervolgens om de vier jaar, verricht de Commissie een algemene evaluatie van Prüm II, met inbegrip van:

- a) een beoordeling van de toepassing van deze verordening;
- b) een toetsing van de bereikte resultaten aan de doelstellingen van deze verordening en een beoordeling van de gevolgen ervan voor de grondrechten;

c) het effect, de effectiviteit en de efficiëntie van de activiteiten en werkmethoden van Prüm II in het licht van zijn doelstellingen, mandaat en taken;

d) een beoordeling van de beveiliging van Prüm II;

De Commissie zendt het verslag van de evaluatie toe aan het Europees Parlement, de Raad, de Europese Toezichthouder voor gegevensbescherming en het Bureau van de Europese Unie voor de grondrechten.

De lidstaten en Europol verstrekken eu-LISA en de Commissie de informatie die nodig is om de bovengenoemde 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.

De lidstaten verstrekken Europol en de Commissie de informatie die nodig is om de bovengenoemde 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.

De lidstaten, eu-LISA en Europol verstrekken de Commissie de informatie die nodig is om de evaluaties te verrichten.

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. *Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken*

De volgende risicofactoren zijn vastgesteld:

- beperkte operationele middelen als gevolg van toenemende gegevensstromen en zich voortdurend ontwikkelende criminele activiteiten;
- vermeerdering van het aantal taken en verzoeken voor zowel eu-LISA als Europol;
- onvoldoende financiële en personele middelen om aan de operationele behoeften te voldoen;
- onvoldoende ICT-middelen, leidend tot vertragingen bij noodzakelijke ontwikkelingen en updates van het kernsysteem;
- risico's in verband met de verwerking van persoonsgegevens door Europol en de noodzaak om de procedurele en technische waarborgen regelmatig te evalueren en aan te passen om de bescherming van persoonsgegevens en de grondrechten te waarborgen;
- onderlinge afhankelijkheden tussen de voorbereidingen van eu-LISA voor de router en de voorbereidingen van de lidstaten en Europol voor het opzetten van een technische interface voor de verzending van gegevens via de router.

Deze risico's kunnen worden beperkt door technieken voor projectbeheer toe te passen en onder meer in de ontwikkelingsprojecten en qua personeelsbezetting te zorgen voor voldoende ruimte om pieken in het werk op te vangen. De projectinspanning wordt namelijk meestal geraamd uitgaande van een gelijkmatig over de tijd gespreide werklast, terwijl deze in 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, zoals met name:

1. het risico dat de contractant onvoldoende middelen uittrekt voor het project of een systeem ontwerpt en ontwikkelt dat onvoldoende geavanceerd is;
2. het risico dat de contractant, om de kosten te drukken, de administratieve technieken en methoden voor grootschalige IT-projecten niet volledig in acht neemt;
3. 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 verifiëren en nauw contact met hen te onderhouden. Tot slot kunnen voor het uiterste geval strenge sanctie- en contractbeëindigingsclausules worden bedongen en zo nodig toegepast.

Europol maakt gebruik van een internecontrolekader dat is gebaseerd op dat van de Europese Commissie en op het integrale internecontrolekader van het oorspronkelijke Committee of Sponsoring Organisations. In het enkelvoudig programmeringsdocument moet informatie worden opgenomen over de internecontrolesystemen, en in het geconsolideerde jaarlijkse activiteitenverslag moet informatie worden opgenomen over de efficiëntie en doeltreffendheid van de internecontrolesystemen, onder andere wat betreft risicobeoordeling. In het geconsolideerde jaarlijkse activiteitenverslag over 2019 wordt vermeld dat op basis van de analyse van de internecontrolecomponenten en -beginselen die in de loop van 2019 aan de hand van zowel kwantitatieve als kwalitatieve elementen zijn gemonitord, het oordeel over het internecontrolesysteem van Europol luidt dat het systeem aanwezig is en op geïntegreerde wijze functioneert in het agentschap.

Voor de door eu-LISA uitgevoerde begroting is een specifiek internecontrolekader vereist dat gebaseerd is op het internecontrolekader van de Europese Commissie. Het enkelvoudig programmeringsdocument moet informatie verschaffen over de internecontrolesystemen, terwijl het geconsolideerd jaarlijks activiteitenverslag informatie moet bevatten over de doeltreffendheid en efficiëntie van de internecontrolesystemen, ook wat risicobeoordelingen betreft. In het geconsolideerde jaarlijkse activiteitenverslag over 2019 wordt vermeld dat het management van het Agentschap redelijke zekerheid heeft dat er passende interne controles plaatsvinden en dat deze functioneren zoals bedoeld. Grote risico's zijn gedurende het hele jaar op de juiste wijze vastgesteld en beheerd. Deze zekerheid wordt voorts bevestigd door de resultaten van de interne en externe controles die zijn uitgevoerd.

Zowel voor Europol als voor eu-LISA wordt ook voorzien in een aanvullend niveau van intern toezicht door de interne-auditcapaciteit van Europol, op basis van een jaarlijks auditplan dat met name rekening houdt met de risicobeoordeling bij Europol. De interne-auditcapaciteit helpt Europol bij het verwezenlijken van zijn doelstellingen door een systematische en gedisciplineerde aanpak te hanteren voor het beoordelen van de effectiviteit van de risicobeheer-, controle- en governanceprocessen en door aanbevelingen te doen voor het verbeteren daarvan.

Bovendien wordt door de Europese Toezichthouder voor gegevensbescherming (EDPS) en de functionaris voor gegevensbescherming in beide agentschappen (een onafhankelijke functie die rechtstreeks verbonden is aan het secretariaat van de raad van bestuur) toezicht gehouden op de verwerking van persoonsgegevens door de agentschappen.

Tot slot zorgt DG HOME als partner-DG van Europol en eu-LISA jaarlijks voor een risicobeheerexercitie om potentiële grote risico's in verband met de activiteiten van de agentschappen in kaart te brengen en te beoordelen. Over als kritiek beschouwde risico's wordt

jaarlijks gerapporteerd in het beheersplan van DG HOME en in een actieplan zijn risicobeperkende maatregelen opgenomen.

2.2.2. *Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting).*

De Commissie rapporteert over de verhouding tussen de controlekosten en de waarde van de desbetreffende financiële middelen. Volgens het jaarlijkse activiteitenverslag 2020 van DG HOME bedroeg die verhouding 0,21 % voor entiteiten belast met indirect beheer en gedecentraliseerde agentschappen, waaronder eu-LISA.

De Europese Rekenkamer heeft de wettigheid en regelmatigheid van de jaarrekeningen van zowel Europol als eu-LISA voor 2019 bevestigd, wat betekent dat het foutenpercentage minder dan 2 % bedroeg. Er zijn geen aanwijzingen dat het foutenpercentage de komende jaren zal stijgen.

Bovendien voorziet artikel 80 van zowel het financieel reglement van Europol als dat van eu-LISA in de mogelijkheid dat het agentschap internecontrolecapaciteit deelt met andere organen van de Unie die op hetzelfde beleidsterrein werkzaam zijn, indien het niet kosteneffectief is om voor één orgaan van de Unie over een afzonderlijke interne-auditcapaciteit te beschikken.

2.3. **Maatregelen ter voorkoming van fraude en onregelmatigheden**

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen, bijvoorbeeld in het kader van de fraudebestrijdingsstrategie.

De fraudebestrijdingsmaatregelen staan in artikel 35 van Verordening (EU) nr. 1077/2011.

De maatregelen ter bestrijding van fraude, corruptie en andere onwettige activiteiten worden onder meer beschreven in artikel 66 van de Europolverordening en in titel X van het financieel reglement van Europol.

Europol neemt met name deel aan de fraudepreventieactiviteiten van het Europees Bureau voor fraudebestrijding en stelt de Commissie onverwijld in kennis van vermoede fraude en andere financiële onregelmatigheden, overeenkomstig zijn interne strategie voor fraudebestrijding.

De raad van bestuur heeft in 2020 een actualisering van de fraudebestrijdingsstrategie van Europol goedgekeurd.

De maatregelen met betrekking tot het bestrijden van fraude, corruptie en andere illegale activiteiten worden onder meer beschreven in artikel 50 van de verordening betreffende eu-LISA en in titel X van het financieel reglement van eu-LISA.

eu-LISA neemt met name deel aan de fraudepreventieactiviteiten van het Europees Bureau voor fraudebestrijding en stelt de Commissie onverwijld in kennis van gevallen van vermoedelijke fraude en andere financiële onregelmatigheden — overeenkomstig zijn interne fraudebestrijdingsstrategie.

DG HOME heeft daarnaast als partner-DG zijn eigen fraudebestrijdingsstrategie ontwikkeld en uitgevoerd op basis van de door OLAF verstrekte methodologie. Gedecentraliseerde agentschappen, waaronder Europol en eu-LISA, vallen onder het toepassingsgebied van de strategie. In het jaarlijks activiteitenverslag 2020 van DG HOME werd geconcludeerd dat de processen inzake fraudepreventie en -opsporing naar tevredenheid functioneerden en derhalve bijdroegen tot de zekerheid ten aanzien van de verwezenlijking van de doelstellingen van de interne controle.

3. **GERAAMDE FINANCIËLE GEVOLGEN VAN HET WETGEVINGSINITIATIEF**

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	GK/NGK ⁴⁶	van EVA-landen ⁴⁷	van kandidaat-lidstaten ⁴⁸	van derde landen	in de zin van artikel 21, lid 2, punt b), van het Financieel Reglement

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgave	Bijdrage			
	Nummer	GK/ NGK	van EVA-landen	van kandidaat-lidstaten	van derde landen	in de zin van artikel 21, lid 2, punt b), van het Financieel Reglement
5	12.02.01 – Fonds voor interne veiligheid	GK	NEE	NEE	NEE	NEE
5	12.01.01. – Ondersteunende uitgaven voor het Fonds voor interne veiligheid	NGK	NEE	NEE	NEE	NEE
5	12.10.01 – Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol)	NGK	NEE	NEE	NEE	NEE
4	11.10.02 – Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van de ruimte van vrijheid, veiligheid en recht (eu-LISA)	NGK	NEE	NEE	NEE	NEE

⁴⁶ GK = gesplitste kredieten / NGK = niet-gesplitste kredieten.

⁴⁷ EVA: Europese Vrijhandelsassociatie.

⁴⁸ Kandidaat-lidstaten en, in voorkomend geval, aspirant-kandidaten van de Westelijke Balkan.

3.2. **Geraamde gevolgen voor de uitgaven**

3.2.1. *Samenvatting van de geraamde gevolgen voor de uitgaven*

miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	5	Veiligheid en defensie
---	----------	-------------------------------

Europol			Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	TOTAAL
Titel 1: Personeelsuitgaven	Vastleggingen	(1)		0,551	1,102	0,847	0,847	3,347
	Betalingen	(2)		0,551	1,102	0,847	0,847	3,347
Titel 2: Infrastructuur- en operationele uitgaven	Vastleggingen	(1a)		1,49	1,052	0,516	0,516	3,574
	Betalingen	(2a)		1,49	1,052	0,516	0,516	3,574
Titel 3: Operationele uitgaven	Vastleggingen	(3a)						
	Betalingen	(3b)						
TOTAAL kredieten voor Europol	Vastleggingen	=1+1a +3a		2,041	2,154	1,363	1,363	6,921
	Betalingen	=2+2a +3b		2,041	2,154	1,363	1,363	6,921

Opmerking: de in het kader van dit voorstel gevraagde extra kredieten voor Europol zullen worden gedekt uit het Fonds voor interne veiligheid (ISF) onder rubriek 5.

miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	4	– Migratie en grenzen
---	----------	------------------------------

eu-LISA			Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	TOTAAL
Titel 1: Personeelsuitgaven	Vastleggingen	(1)		0,456	0,988	1,52	1,45	4,414
	Betalingen	(2)		0,456	0,988	1,52	1,45	4,414
Titel 2: Infrastructuur- en operationele uitgaven	Vastleggingen	(1a)		4,15	3,55	1,4	0	9,1
	Betalingen	(2a)		4,15	3,55	1,4	0	9,1
Titel 3: Operationele uitgaven	Vastleggingen	(3a)		0	0	1	1,2	2,2
	Betalingen	(3b)		0	0	1	1,2	2,2
TOTAAL kredieten voor eu-LISA	Vastleggingen	=1+1a +3a		4,606	4,538	3,92	2,65	15,714
	Betalingen	=2+2a +3b		4,606	4,538	3,92	2,65	15,714

Opmerking: de in het kader van dit voorstel gevraagde extra kredieten voor eu-LISA zullen worden gedekt uit het instrument voor grensbeheer en visumbeleid (BMVI) onder rubriek 4.

Rubriek van het meerjarig financieel kader	5	Weerbaarheid, veiligheid en defensie
---	---	--------------------------------------

DG HOME			Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	TOTAAL
Fonds voor interne veiligheid	Vastleggingen	(1)		13,64	40	40		93,64
	Betalingen	(2)		4,68	6,55	9,39		34,65
TOTAAL kredieten voor DG HOME	Vastleggingen			13,64	40	40		93,64
	Betalingen			4,68	6,55	9,39		34,65

Opmerking: De in het kader van dit voorstel gevraagde kredieten zullen worden gedekt door de kredieten waarin reeds is voorzien in de arbeidskrachtenenquête die ten grondslag ligt aan de ISF-verordening. In het kader van dit wetgevingsvoorstel worden geen extra financiële of personele middelen gevraagd.

De kosten per lidstaat omvatten:

- modernisering van hun infrastructuur om de uitwisseling van webdiensten te ondersteunen en de verbinding met de centrale router tot stand te brengen, hetgeen inhoudt dat inspanningen moeten worden geleverd om de nieuwe architecturomgeving te analyseren en te definiëren;
- modernisering van hun infrastructuur om de uitwisseling van webdiensten te ondersteunen en de verbinding met de centrale router tot stand te brengen;
- configuratie van een systeem voor de uitwisseling van webdiensten en het opzetten van de verbinding met de centrale router;
- ontwerp van een nieuwe nationale architectuur en van specificaties om de toegang tot nationale gegevens te waarborgen via de ontwikkelde oplossingen (de router en Epris);
- opzetten van een nieuw register of een reeds bestaand register voor de uitwisseling van politiegegevens geschikt maken;
- opzetten van een nieuwe databank voor gezichtsopnamen of een reeds bestaande databank voor gezichtsopnamen geschikt maken voor uitwisseling;
- integratie van de oplossing op nationaal niveau;
- algemene kosten in verband met projectbeheer.

De volgende tabel geeft de kosten per categorie weer:

Vermeld doelstellingen en outputs DG HOME ↓			Jaar 2023		Jaar 2024		Jaar 2025		Jaar 2026		Jaar 2027		TOTAAL	
	Soort	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten	
Router	Verbinden van bestaande databanken met de router			26	2,314	26	6,787	26	6,787			26	15,89	
Gezichtsopnamen	Opzetten van nieuwe databank			13*	2,84	13	8,329	13	8,329			13	19,5	
	Verbinden van de databank met de router			26	2,72	26	7,996	26	7,996			26	18,72	
Politiegegevens	Opzetten van een databank met politiegegevens en verbinding met Epris			26	5,763	26	16,959	26	16,959			26	39,7	
Totaal						13,64		40		40			93,64	

* Geschat aantal lidstaten zonder databank voor gezichtsopnamen

Rubriek van het meerjarig financieel kader	7	“Administratieve uitgaven”					
---	----------	-----------------------------------	--	--	--	--	--

miljoen EUR (tot op drie decimalen)

		Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	TOTAAL	
DG: HOME								
• Personele middelen			0,608	0,684	0,608	0,608	2,508	
• Andere administratieve uitgaven			0,225	0,225	0,186	0,186	0,822	
TOTAAL voor DG HOME	Kredieten							

TOTAAL kredieten onder RUBRIEK 7 van het meerjarig financieel kader	(Totaal vastleggingen = totaal betalingen)		0,833	0,833	0,794	0,794	3,330	
--	---	--	-------	-------	-------	-------	-------	--

miljoen EUR (tot op drie decimalen)

		Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	TOTAAL
TOTAAL kredieten onder de rubrieken 1 tot en met 5 van het meerjarig financieel kader	Vastleggingen		20,287	46,692	45,283	4,013	116,275
	Betalingen		11,329	13,247	14,647	18,059	57,282

3.2.2. 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 beschreven:

Vastleggingskredieten in miljoen EUR (tot op drie decimalen)

Vermeld doelstelling en en outputs			Jaar		Jaar		Jaar		Jaar		Jaar		TOTAAL	
			2023		2024		2025		2026		2027			
↓	Soort	Gem. kosten ⁴⁹	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten
Kosten van Europol (geen verband houdend met personele middelen)														
– Output	Infrastructuur en onderhoud					0,764		0,326		0,226		0,226		1,542
– Output	Contractanten					0,726		0,726		0,290		0,290		2,032
TOTALE KOSTEN						1,490		1,052		0,516		0,516		3,574

⁴⁹ Vanwege hun specifieke operationele aard is het niet mogelijk de exacte eenheidskosten per output vast te stellen, noch het exacte verwachte volume van de output, met name omdat sommige outputs verband houden met rechtshandhavingsactiviteiten die een reactie zijn op onvoorspelbare criminele activiteiten.

3.2.3. *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 beschreven:

Vastleggingskredieten in miljoen EUR (tot op drie decimalen)

Vermeld doelstellin gen en outputs			Jaar		Jaar		Jaar		Jaar		Jaar		TOTAAL	
			2023		2024		2025		2026		2027			
↓	Soort	Gem. kosten ⁵⁰	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten
Kosten van eu-LISA (geen verband houdend met personele middelen)														
– Output	Infrastructuur ⁵¹					1,85		2,15		0,7		0		4,7
– Output	Contractanten ⁵²					1,4		0,7		0,7		0		2,8

⁵⁰ Vanwege hun specifieke operationele aard is het niet mogelijk de exacte eenheidskosten per output vast te stellen, noch het exacte verwachte volume van de output, met name omdat sommige outputs verband houden met rechtshandhavingsactiviteiten die een reactie zijn op onvoorspelbare criminele activiteiten.

⁵¹ Omvat hardware, software, netwerkvoorzieningen, beveiliging.

⁵² Omvat de kosten van professionele diensten, ontwerp en testen.

– Output	Mechanisme voor micromatching					0,9		0,7		0		0		
– Output	Onderhoud					0		0		1		1,2		2,2
TOTALE KOSTEN						4,15		3,55		2,4		1,2		11,3

3.2.4. Geraamde gevolgen voor de personele middelen van Europol

3.2.4.1. Samenvatting

☐ voor het voorstel/initiatief zijn geen administratieve kredieten nodig

☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	TOTAAL
--	--------------	--------------	--------------	--------------	--------------	--------

Tijdelijke functionarissen – baseline						
Tijdelijke functionarissen – aanvulling op de baseline (cumulatief)	0	0,551	1,101	0,847	0,847	3,347
Tijdelijke functionarissen – TOTAAL						
Arbeidscontractanten – baseline						
Gedetacheerde nationale deskundigen – baseline (verzoek ontwerpbegroting 2021)						

TOTAAL – alleen extra kosten	0	0,551	1,101	0,847	0,847	3,347
TOTAAL – m.i.v. baseline en extra kosten						

Personeelsbehoeften (VTE):

	Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027
Tijdelijke functionarissen – baseline	0	9,5	9,5	21,5	19,5
Tijdelijke functionarissen – aanvulling op de baseline (cumulatief)	0	6,5	6,5	5	5
Tijdelijke functionarissen – TOTAAL		16	16	26,5	24,5
Arbeidscontractanten					

Gedetacheerde nationale deskundigen					
TOTAAL	0	16,5	16,5	26,5	24,5

Het aantal personeelsleden dat nodig is om de doelstellingen van dit voorstel te verwezenlijken, is geraamd in samenwerking met Europol. De ramingen houden rekening met de verwachte toename van de werklust, aangezien belanghebbenden mettertijd vaker gebruik gaan maken van de diensten van Europol, alsook met de tijd die Europol nodig heeft om middelen te absorberen. Er moet worden voorkomen dat het agentschap zijn EU-bijdrage en vastleggingskredieten niet tijdig volledig kan uitvoeren.

In de personele middelen die vereist zijn om de doelstellingen van dit voorstel te verwezenlijken, zal deels worden voorzien door de bestaande personeelsleden van Europol (baseline) en deels door extra personele middelen (extra personeel in vergelijking met het baselinescenario).

De arbeidskrachtenenquête voorziet niet in een toename van het aantal arbeidscontractanten.

De voor de uitvoering van Prüm II benodigde middelen met betrekking tot Europol kunnen in drie categorieën worden onderverdeeld:

1) ICT-kosten voor de aansluiting op de biometrische router bij eu-LISA, de noodzakelijke ontwikkelingswerkzaamheden met betrekking tot de informatiesystemen van Europol voor het beschikbaar maken van van derden afkomstige gegevens voor zoekopdrachten van lidstaten en om zoekopdrachten in Prüm te integreren met gegevens van derden in de gemeenschappelijke Europolzoekinterface USE-UI;

2) personeelskosten voor het operationele directoraat van Europol voor het uitvoeren van zoekopdrachten in verband met van derden afkomstige gegevens en kosten voor biometrie-experts voor het verifiëren van hits;

3) kosten van het hosten van een centrale router voor politiegegevens. Hieronder vallen ook eenmalige kosten voor hardware (waaronder gescheiden productie- en testomgevingen voor de lidstaten), ICT-personeel voor de ontwikkeling en het wijzigingsmanagement van ADEP.EPRIS-software, tests met de lidstaten, 24/7-helpdesk ter ondersteuning van de lidstaten in geval van problemen. Om de lidstaten volledige steun te kunnen verlenen, moet ICT-personeel met verschillende profielen beschikbaar zijn, bv. voor algemene coördinatie, gebruikersbelangenanalyse, ontwikkeling, testen en systeembeheer. Naar verwachting zal er in het eerste jaar na de ingebruikneming nog iets meer ICT-personeel nodig zijn.

Vanwege de veiligheidseisen en het overeengekomen plafond voor arbeidscontractanten moet het merendeel van de Prümgerelateerde taken worden uitgevoerd door personeel van Europol. Het is de bedoeling dat bepaalde minder gevoelige activiteiten worden uitbesteed aan contractanten (testen, bepaalde ontwikkelingstaken).

Tijdelijke functionarissen in VTE (baseline + extra personeel)	2023	2024	2025	2026	2027
Projectbeheer		1,0	1,0	0,5	0,5

Deskundigen (totaal)		14,5	14,5	18,0	16,0
• <i>biometrie</i>		1,0	1,0	4,0	4,0
• <i>uitvoerend personeel</i>		0,5	0,5	4,0	4,0
• <i>ICT</i>		13,0	13,0	10,0	8,0
Helpdesk ondersteuning/monitoring		0,0	0,0	7,0	7,0
Algemene coördinatie		1,0	1,0	1,0	1,0
Totaal		16,5	16,5	26,5	24,5

3.2.5. Geraamde gevolgen voor de personele middelen van eu-LISA

3.2.5.1. Samenvatting

☐ voor het voorstel/initiatief zijn geen administratieve kredieten nodig

☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader beschreven:

miljoen EUR (tot op drie decimalen)

	Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	TOTAAL
--	--------------	--------------	--------------	--------------	--------------	--------

Tijdelijke functionarissen – baseline						
Tijdelijke functionarissen – aanvulling op de baseline (cumulatief)		0,456	0,988	1,52	1,368	4,332
Tijdelijke functionarissen – TOTAAL						
Arbeidscontractanten – baseline						
Arbeidscontractanten – aanvullend					0,082	0,082
Gedetacheerde nationale deskundigen – baseline (verzoek ontwerpbegroting 2021) ⁵³						

TOTAAL – alleen extra kosten		0,456	0,988	1,52	1,45	4,414
TOTAAL – m.i.v. baseline en extra kosten						

Personeelsbehoeften (VTE):

	Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027
--	--------------	--------------	--------------	--------------	--------------

⁵³ In de ontwerpbegroting 2021 vermelde personeelsbezetting, berekend op basis van de gemiddelde personeelskosten per eenheid die voor de arbeidskrachtenenquête moeten worden gebruikt. De helft van de overeenkomstige jaarlijkse kredieten is berekend voor het jaar waarin personeel wordt aangeworven.

Tijdelijke functionarissen – baseline					
Tijdelijke functionarissen – aanvulling op de baseline (cumulatief)		6	7	10	9
Tijdelijke functionarissen – TOTAAL					
Arbeidscontractanten – baseline					
Arbeidscontractanten – aanvullend					2
Gedetacheerde nationale deskundigen					
TOTAAL		6	7	10	11

Het aantal personeelsleden dat nodig is om de doelstellingen van het nieuwe mandaat uit te voeren, is geraamd in samenwerking met eu-LISA. De ramingen houden rekening met de verwachte toename van de werklust, aangezien belanghebbenden mettertijd vaker gebruik gaan maken van de diensten van eu-LISA, alsook met de tijd die eu-LISA nodig heeft om middelen te absorberen. Er moet worden voorkomen dat het agentschap zijn EU-bijdrage en vastleggingskredieten niet tijdig volledig kan uitvoeren.

Deze ramingen zijn gebaseerd op de volgende personeelsbezetting:

	Fase								
	Analyse en ontwerp			Bouw en ontwikkeling			Werking		
Soort contract	TF	AC	Totaal	TF	AC	Totaal	TF	AC	Totaal
Profiel	Aantal	Aantal		Aantal	Aantal		Aantal	Aantal	
IT-architect	1		1	1		1	1		1
Testmanagement	1		1	1		1	0,5		0,5
Release- en wijzigingsmanagement			0	1		1	1		1
Netwerkbeheerder	1		1	1		1	1		1
Beveiligingsbeheer	2		2	2		2	2		2
Operator ondersteuning eerste niveau (24/7)			0			0		1	1
Administrateur ondersteuning tweede niveau (24/7)			0			0		1	1
Programma- en	1		1	1		1	0,5		0,5

projectmanagement									
Eigenaar product			0	1		1	1		1
Expert biometrie	1		1	1		1	1		1
Systeembeheerder / Infrastructuur	1		1	1		1	1		1
Totaal (AC+TF)	8		8	10		10	9	2	11

Profielen	Jaar 1 (voorbereiding en ontwerp)	Jaar 1	Jaar 2	Jaar 3	Jaar 4	Jaar 5
IT-architect (TF)	1	1	1	1	1	1
Testmanagement (TF)		1	1	0,5	0,5	0,5
Release- en wijzigingsmanagement (TF)			1	1	1	1
Netwerkbbeheer (TF)	1	1	1	1	1	1
Beveiligingsbeheer (TF)	1	1	2	2	2	2
Operator ondersteuning eerste niveau (24/7) – (AC)				1	1	1

Administrateur ondersteuning tweede niveau (24/7) – (AC)				1	1	1
Programma- en projectmanagement (TF)	1	1	1	0,5	0,5	0,5
Eigenaar product (TF)			1	1	1	1
Expert biometrie (TF)	1	1	1	1	1	1
Systeembeheerder / Infrastructuur (TF)	1	1	1	1	1	1
TOTAAL	6	7	10	11	11	11

3.2.5.2. Geraamde behoefte aan personele middelen voor het partner-DG

☐ Voor het voorstel/initiatief zijn geen personele middelen nodig.

☒ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader beschreven:

Raming in een geheel getal (of met ten hoogste 1 decimaal)

	Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)					
XX 01 01 01 (zetel en vertegenwoordigingen van de Commissie)		5	5	4	4
XX 01 01 02 (delegaties)					
XX 01 05 01 (onderzoek door derden)					
10 01 05 01 (eigen onderzoek)					
• Extern personeel (in voltijdequivalenten: VTE)⁵⁴					
XX 01 02 01 (AC, END, INT uit de “totale financiële middelen”)					
XX 01 02 02 (AC, AL, END, INT en JPD in de delegaties)					
XX 01 04 <i>jj</i>⁵⁵	– zetel ⁵⁶				
	– delegaties				
XX 01 05 02 (AC, END, INT – onderzoek door derden)					
10 01 05 02 (AC, END, INT – eigen onderzoek)					
Ander begrotingsonderdeel (te vermelden)					
TOTAAL		5	5	4	4

XX is het beleidsterrein of de begrotingstitel.

Voor de benodigde personele middelen zal deels (3 vte) een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is 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. Het DG zal ook extra personeel nodig hebben (2 vte).

⁵⁴ AC = Agent Contractuel (arbeidscontractant); AL = Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JPD = Junior Professionals in Delegations (jonge deskundige in delegaties).

⁵⁵ Subplafond voor extern personeel uit beleidskredieten (vroegere “BA”-onderdelen).

⁵⁶ Voornamelijk voor de structuurfondsen, het Europees Landbouwfonds voor Plattelandsontwikkeling (Elfpo) en het Europees Visserijfonds (EVF).

Beschrijving van de uit te voeren taken:

Vijf functionarissen voor de follow-up. Dit personeel vervult de taken van de Commissie met betrekking tot de uitvoering van het programma: controle van de conformiteit met het wetgevingsvoorstel, aanpak van nalevingskwesties, rapportage aan het Europees Parlement en de Raad, beoordeling van de vooruitgang van de lidstaten, actualisering van secundaire wetgeving, met inbegrip van eventuele ontwikkelingen op normatief gebied. Aangezien de taken in verband met het programma bovenop de gewone werklast komen, is extra personeel nodig (2 vte). Een van de extra personeelsleden is nodig voor beperkte duur, namelijk alleen tijdens de ontwikkelingsperiode. Het tweede personeelslid is nodig voor het overnemen van de taken van het secretariaat-generaal van de Raad. Dit komt doordat de besluiten van de Raad worden vervangen door een verordening, wat betekent dat de Commissie de taken van het secretariaat-generaal van de Raad moet overnemen, waarvoor 1 vte nodig is.

3.2.6. Verenigbaarheid met het huidig meerjarig financieel kader

- ☐ Het voorstel/initiatief is verenigbaar met het huidig meerjarig financieel kader.
- ☐ Het voorstel/initiatief vereist herprogrammering van de betrokken rubriek van het meerjarig financieel kader.

- ☐ Het voorstel/initiatief vereist toepassing van het flexibiliteitsinstrument of herziening van het meerjarige financiële kader⁵⁷.

Zet uiteen wat nodig is, onder vermelding van de betrokken rubrieken en begrotingsonderdelen en de desbetreffende bedragen.

[...]

3.2.7. Bijdragen van derden

Het voorstel/initiatief voorziet niet in medefinanciering door derden.

Het voorstel/initiatief voorziet in medefinanciering, zoals hieronder geraamd:

miljoen EUR (tot op drie decimalen)

	Jaar N	Jaar N+1	Jaar N+2	Jaar N+3	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			Totaal
Medefinancieringsbron								
TOTAAL medegefinancierde kredieten								

⁵⁷

Zie de artikelen 11 en 17 van Verordening (EU, Euratom) nr. 1311/2013 van de Raad tot bepaling van het meerjarig financieel kader voor de jaren 2014–2020.

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 overige ontvangsten
- ☐ Geef aan of de ontvangsten worden toegewezen aan de begrotingsonderdelen voor uitgaven

miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief ⁵⁸						
		Jaar N	Jaar N+1	Jaar N+2	Jaar N+3	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
Artikel								

Vermeld voor de diverse ontvangsten die worden toegewezen het betrokken begrotingsonderdeel of de betrokken begrotingsonderdelen voor uitgaven.

[...]

Vermeld de wijze van berekening van de gevolgen voor de ontvangsten.

[...]

⁵⁸

Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 20 % aan inningskosten.

BIJLAGE 5

**bij het
BESLUIT VAN DE COMMISSIE**

**inzake de interne regels betreffende de uitvoering van de algemene begroting van de Europese Unie
(afdeling Europese Commissie) ter attentie van de diensten van de Commissie**

**BIJLAGE
bij het FINANCIIEEL MEMORANDUM**

BIJLAGE

bij het FINANCIËEL MEMORANDUM

Benaming van het voorstel:

Voorstel betreffende geautomatiseerde gegevensuitwisseling ten behoeve van politieke samenwerking (“Prüm II”) en tot wijziging van Verordening (EU) 2018/1726, Verordening (EU) 2019/817 en Verordening (EU) 2019/818 en tot intrekking van de Besluiten 2008/615/JBZ en 2008/616/JBZ van de Raad

- 1. NODIG GEACHTE PERSONELE MIDDELEN EN KOSTEN DAARVAN**
- 2. KOSTEN VAN ANDERE ADMINISTRATIEVE UITGAVEN**
- 3. TOTALE ADMINISTRATIEVE KOSTEN**
- 4. VOOR KOSTENRAMINGEN GEBRUIKTE BEREKENINGSMETHODEN**
 - 4.1. Personele middelen**
 - 4.2. Andere administratieve uitgaven**

Deze bijlage moet het financieel memorandum vergezellen wanneer de dienstenoverkoepelende raadpleging van start gaat.

De gegevens in tabelvorm worden gebruikt als bron voor de in het financieel memorandum opgenomen tabellen. Zij zijn voor strikt intern gebruik binnen de Commissie.

(1) Kosten van nodig geachte personele middelen

☐ Voor het voorstel/initiatief zijn geen personele middelen nodig.

☒ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader beschreven:

miljoen EUR (tot op drie decimalen)

RUBRIEK 7 van het meerjarig financieel kader		2024		2025		2026		2027								TOTAAL	
		VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten	VTE	Kredieten
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)																	
20 01 02 01 – Zetel en vertegenwoordigingen van de Commissie	AD	5	0,608	5	0,684	4	0,608	4	0,608							4	2,508
	AST																
20 01 02 03 – EU-delegaties	AD																
	AST																
• Extern personeel ⁵⁹																	
20 02 01 en 20 02 02 – Extern personeel – Zetel en vertegenwoordigingen van de Commissie	AC																
	END																
	INT																
20 02 03 – Extern personeel – EU-delegaties	AC																
	AL																

⁵⁹

AC = Agent Contractuel (arbeidscontractant); AL = Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT = Intérimaire (uitzendkracht); JPD = Junior Professional in Delegations (jonge deskundige in delegaties).

	END																
	INT																
	JPD																
Andere HR- begrotingsonderdelen (te vermelden)																	
Subtotaal HR – RUBRIEK 7		5	0,608	5	0,684	4	0,608	4	0,608							4	2,508

Voor de benodigde personele middelen zal een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is 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.

Voor de benodigde personele middelen zal een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is 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.

(2) Kosten van andere administratieve uitgaven

☐ 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)

RUBRIEK 7 van het meerjarig financieel kader	2024	2025	2026	2027				Totaal
Op de zetel of op het grondgebied van de EU:								
20 02 06 01 – Dienstreizen en representatie	0,035	0,035	0,035	0,035				0,140
20 02 06 02 – Conferenties en vergaderingen	0,125	0,125	0,125	0,125				0,500
20 02 06 03 – comités (Prüm II-comité) ⁶⁰	0,065	0,065	0,026	0,026				0,182
20 02 06 04 – Studies en adviezen								
20 04 – IT-bedrijfsuitgaven ⁶¹								
Andere niet HR-begrotingsonderdelen (<i>indien nodig nader aangeven</i>)								
EU-delegaties								
20 02 07 01 – Dienstreizen, conferenties en representatie								

⁶⁰ Prüm II-comité: circa 10 vergaderingen per jaar in 2024 en 2025 en daarna 4 vergaderingen per jaar, waarvan slechts de helft van de kosten is opgenomen (de andere helft betreft videoconferenties).

⁶¹ Hiervoor is het advies van DG DIGIT – IT Investments Team vereist (zie de mededeling *Guidelines on Financing of Information Technology and Cybersecurity (IT)*, C(2020) 6126 final van 10.9.2020, blz. 7).

20 02 07 02 – Bijscholing van personeel								
20 03 05 – Infrastructuur en logistiek								
Andere niet HR-begrotingsonderdelen (indien nodig nader aangeven)								
Subtotaal Andere – RUBRIEK 7 van het meerjarig financieel kader	0,225	0,225	0,186	0,186				0,822

miljoen EUR (tot op drie decimalen)

Buiten RUBRIEK 7 van het meerjarig financieel kader	2024	2025	2026	2027				Totaal
Uitgaven voor technische en administratieve bijstand (exclusief extern personeel) uit beleidskredieten (vroegere "BA"-onderdelen):								
– zetel								
– EU-delegaties								
Overige beheersuitgaven voor onderzoek								
IT-beleidsuitgaven inzake operationele programma's ⁶²								

⁶² Hiervoor is het advies van DG DIGIT – IT Investments Team vereist (zie de mededeling *Guidelines on Financing of Information Technology and Cybersecurity (IT)*, C(2020) 6126 final van 10.9.2020, blz. 7).

IT-bedrijfsuitgaven inzake operationele programma's ⁶³								
Andere niet HR-begrotingsonderdelen (<i>indien nodig nader aangeven</i>)								
Subtotaal Andere– Buiten RUBRIEK 7 van het meerjarig financieel kader								
Totale andere administratieve uitgaven (alle MFK-rubrieken)	0,225	0,225	0,186	0,186				0,822

⁶³ Dit omvat lokale administratieve systemen en bijdragen aan de cofinanciering van IT-bedrijfssystemen (zie de mededeling *Guidelines on Financing of Information Technology and Cybersecurity (IT)*, C(2020)6126 final van 10.9.2020).

(3) Totale administratieve kosten (alle MFK-rubrieken)

miljoen EUR (tot op drie decimalen)

Samenvatting	2024	2025	2026	2027				Totaal
Rubriek 7 – Personele middelen	0,608	0,684	0,608	0,608				2,508
Rubriek 7 – Andere administratieve uitgaven	0,225	0,225	0,186	0,186				0,822
Subtotaal rubriek 7								
Buiten rubriek 7 – Personele middelen								
Buiten rubriek 7 – Andere administratieve uitgaven								
Subtotaal Overige rubrieken								
TOTAAL RUBRIEK 7 en buiten RUBRIEK 7	0,833	0,833	0,794	0,794				3,330

In de benodigde administratieve kredieten zal worden voorzien door de kredieten die reeds voor het beheer van deze actie zijn toegewezen en/of zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de bestaande budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

4. BEREKENINGSMETHODEN VOOR DE KOSTENRAMINGEN

4.1. Personele middelen

In dit deel wordt de berekeningsmethode toegelicht die is gebruikt om de benodigde personele middelen te ramen (veronderstelde werklast, bijzondere taken (Sysper 2 taakprofielen), personeelscategorieën en overeenkomstige gemiddelde kosten)

RUBRIEK 7 van het meerjarig financieel kader

NB: De gemiddelde kosten van elke personeelscategorie op het hoofdkantoor zijn te vinden op BudgWeb:
https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx

Ambtenaren en tijdelijk personeel:

Overeenkomstig de circulaire van DG BUDG aan RUF/2020/23 van 30.11.2020 (zie bijlage 1, Ares (2020)7207955 van 30.11.2020) vertegenwoordigt 1 AD een kostprijs van 152 000 EUR per jaar. De helft van de overeenkomstige jaarlijkse kredieten wordt berekend voor het jaar waarin personeel wordt aangeworven en afgebouwd.

Voor de benodigde personele middelen zal deels (3 vte) een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is 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. Het DG zal ook extra personeel nodig hebben (2 vte).

Beschrijving van de uit te voeren taken:

Vijf functionarissen voor de follow-up. Dit personeel vervult de taken van de Commissie met betrekking tot de uitvoering van het programma: controle van de conformiteit met het wetgevingsvoorstel, aanpak van nalevingskwesties, rapportage aan het Europees Parlement en de Raad, beoordeling van de vooruitgang van de lidstaten, actualisering van secundaire wetgeving, met inbegrip van eventuele ontwikkelingen op normatief gebied. Aangezien de taken in verband met het programma bovenop de gewone werklast komen, is extra personeel nodig (2 vte). Een van de extra personeelsleden is nodig voor beperkte duur, namelijk alleen tijdens de ontwikkelingsperiode. Het tweede personeelslid is nodig voor het overnemen van de taken van het secretariaat-generaal van de Raad. Dit komt doordat de besluiten van de Raad worden vervangen door een verordening, wat betekent dat de Commissie de taken van het secretariaat-generaal van de Raad moet overnemen, waarvoor 1 vte nodig is.

- Extern personeel

Buiten RUBRIEK 7 van het meerjarig financieel kader

- Alleen uit de begroting voor onderzoek gefinancierde posten

- Extern personeel

4.2. Andere administratieve uitgaven

Verstrek gegevens over de voor elk begrotingsonderdeel gebruikte berekeningsmethode, en meer in het bijzonder over de achterliggende aannamen (bv. aantal vergaderingen per jaar, gemiddelde kosten, enz.)

RUBRIEK 7 van het meerjarig financieel kader

Voor het bijwonen van vergaderingen en conferenties in verband met Prüm zullen naar schatting jaarlijks gemiddeld 35 dienstreizen plaatsvinden, waaronder dienstreizen voor de statutaire vergaderingen (adviesgroep, werkgroepen van zowel eu-LISA als Europol en vergaderingen in verband met Epris en Eucaris). Voor de berekening van de eenheidsprijs per dienstreis wordt uitgegaan van één ambtenaar die voor elke dienstreis gemiddeld twee dagen op reis is. De eenheidsprijs is vastgesteld op 500 EUR per dienstreis per dag.

De eenheidskosten per deskundigenvergadering/conferentie worden vastgesteld op 25 000 EUR voor 50 deelnemers. Naar schatting zullen jaarlijks vijf vergaderingen worden georganiseerd.

De eenheidskosten per comitévergadering worden vastgesteld op 13 000 EUR voor 26 deelnemers, uitgaande van de vergoeding van één deelnemer per lidstaat voor een dienstreis van één dag om de comitévergadering bij te wonen. Naar schatting zullen in 2024 en 2025 jaarlijks tien vergaderingen worden georganiseerd (vijf als fysieke bijeenkomst en vijf als videoconferentie) en vanaf 2026 vier vergaderingen per jaar (twee als fysieke bijeenkomst en twee als videoconferentie).

Buiten RUBRIEK 7 van het meerjarig financieel kader