Raad van de
Europese Unie

Brussel, 23 december 2016
(OR. en)

15813/16

Interinstitutioneel dossier:
2016/0408 (COD)

SIRIS 177
FRONT 502
SCHENGEN 21
COMIX 862
CODEC 1944

VOORSTEL

van:	de heer Jordi AYET PUIGARNAU, directeur, namens de secretaris-generaal van de Europese Commissie
ingekomen:	22 december 2016
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
Nr. Comdoc.:	COM(2016) 882 final
Betreft:	Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van Verordening (EU) nr. 515/2014 en tot intrekking van Verordening (EG) nr. 1987/2006

Hierbij gaat voor de delegaties document COM(2016) 882 final.

Bijlage: COM(2016) 882 final

EUROPESE
COMMISSIE

Brussel, 21.12.2016
COM(2016) 882 final

2016/0408 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van Verordening (EU) nr. 515/2014 en tot intrekking van Verordening (EG) nr. 1987/2006

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

De afgelopen twee jaar heeft de Europese Unie gewerkt aan een gelijktijdige aanpak van de afzonderlijke uitdagingen op het gebied van migratiebeheer, geïntegreerd beheer van de EU-buitengrenzen en bestrijding van terrorisme en grensoverschrijdende misdaad. Om krachtig op deze uitdagingen te reageren en om een echte en doeltreffende Veiligheidsunie tot stand te brengen, is het van essentieel belang dat de lidstaten zowel onderling als met de betrokken EU-agentschappen op een effectieve manier informatie uitwisselen.

Het Schengeninformatiesysteem (SIS) is het meest succesvolle instrument voor een doeltreffende samenwerking tussen immigratie-, politie-, douane- en gerechtelijke autoriteiten in de EU en de geassocieerde Schengenlanden. De bevoegde autoriteiten in de lidstaten, zoals politie, grenswacht en douane, moeten toegang hebben tot kwalitatief hoogwaardige informatie over de personen of voorwerpen die zij controleren, met duidelijke instructies over wat er in elk specifiek geval moet gebeuren. Dit grootschalige informatiesysteem vormt de kern voor de samenwerking op Schengenniveau en speelt een cruciale rol bij het vergemakkelijken van het vrije verkeer van personen in het Schengengebied. De bevoegde autoriteiten kunnen in het systeem gegevens invoeren en raadplegen over gezochte personen, personen die wellicht geen recht op binnenkomst en verblijf in de EU hebben, vermiste personen – met name kinderen – en mogelijk gestolen, verduisterde of vermiste voorwerpen. Het SIS bevat niet alleen informatie over specifieke personen of voorwerpen, maar ook duidelijke instructies voor de bevoegde autoriteiten over wat zij met die personen of voorwerpen moeten doen zodra deze worden aangetroffen.

In 2016, drie jaar na de inwerkingtreding van de tweede generatie van het SIS, heeft de Commissie het systeem uitgebreid geëvalueerd[1]. Het SIS komt uit deze evaluatie naar voren als een echt operationeel succes. De nationale bevoegde autoriteiten hebben in 2015 bijna 2,9 miljard keer personen en voorwerpen getoetst aan data in het SIS, en meer dan 1,8 miljoen aanvullende informatie-elementen uitgewisseld. Dit neemt niet weg dat de doeltreffendheid en efficiëntie van het systeem, uitgaande van deze positieve ervaring, moeten worden verbeterd, zoals is aangekondigd in het werkprogramma van de Commissie voor 2017. Met dat doel voor ogen komt de Commissie, naar aanleiding van de reeds genoemde evaluatie, met een eerste reeks van drie voorstellen om het SIS te verbeteren en het gebruik ervan uit te breiden, en werkt zij tegelijkertijd voort aan een betere interoperabiliteit van bestaande en toekomstige systemen voor rechtshandhaving en grensbeheer, in aansluiting op de lopende werkzaamheden van de deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit.

Deze voorstellen hebben betrekking op het gebruik van het systeem (a) voor grensbeheer, (b) voor politiële samenwerking en justitiële samenwerking in strafzaken, en (c) voor terugkeer van illegaal verblijvende onderdanen van derde landen. De eerste twee voorstellen vormen

---

[1] Verslag aan het Europees Parlement en aan de Raad over de evaluatie van het Schengeninformatiesysteem van de tweede generatie (SIS II) in overeenstemming met artikel 24, lid 5, artikel 43, lid 3, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006 en artikel 59, lid 3, en artikel 66, lid 5, van Besluit 2007/533/JBZ, en een bijbehorend werkdocument van de diensten van de Commissie. (PB …).

samen de rechtsgrondslag voor de instelling, de werking en het gebruik van het SIS. Het voorstel inzake het gebruik van het SIS voor de terugkeer van illegaal verblijvende onderdanen van derde landen vormt een aanvulling op het voorstel inzake grensbeheer en de daarin opgenomen bepalingen. Het voorstel bevat een nieuwe signaleringscategorie en draagt bij aan de uitvoering en monitoring van Richtlijn 2008/115/EG[2].

Omdat niet alle lidstaten in dezelfde mate betrokken zijn bij het EU-beleid op het gebied van vrijheid, veiligheid en recht (de zogenoemde "variabele geometrie"), moeten drie afzonderlijke rechtsinstrumenten worden vastgesteld, die echter naadloos op elkaar zullen aansluiten, zodat het systeem optimaal kan werken en gebruikt worden.

Parallel met deze werkzaamheden heeft de Commissie in april 2016 een proces van reflectie over "sterkere en slimmere informatiesystemen voor grenzen en veiligheid"[3] opgestart om het informatiebeheer op EU-niveau te versterken en te verbeteren. De overkoepelende doelstelling bestaat erin te waarborgen dat de bevoegde autoriteiten stelselmatig beschikken over de nodige informatie uit verschillende informatiesystemen. Met het oog daarop heeft de Commissie de bestaande informatiearchitectuur doorgelicht op informatielacunes en blinde vlekken die terug te voeren zijn op gebrekkig functioneren van de bestaande systemen en op versnippering in de algemene EU-architectuur voor gegevensbeheer. De Commissie heeft ter ondersteuning van deze werkzaamheden een deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit opgericht en bij het opstellen van deze eerste reeks voorstellen rekening gehouden met de tussentijdse bevindingen van deze groep wat de kwaliteit van de gegevens betreft[4]. In zijn toespraak van september 2016 over de toestand van de Unie heeft voorzitter Juncker beklemtoond hoe belangrijk het is de bestaande tekortkomingen in het informatiebeheer weg te werken en de interoperabiliteit en interconnectiviteit van de bestaande informatiesystemen te verbeteren.

De deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit zal haar bevindingen in de eerste helft van 2017 voorleggen en naar aanleiding daarvan zal de Commissie zich medio 2017 buigen over een tweede reeks voorstellen om de interoperabiliteit tussen het SIS en andere IT-systemen verder te verbeteren. Een andere belangrijke component van deze werkzaamheden is de herziening van Verordening (EU) nr. 1077/2011[5] betreffende het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA). De Commissie zal hierover waarschijnlijk afzonderlijke voorstellen indienen, eveneens in de loop van 2017. Voor het aanpakken van de huidige uitdagingen op het gebied van veiligheid is het belangrijk te investeren in snelle, doeltreffende en kwalitatieve informatie-uitwisseling en een daarop afgestemd informatiebeheer, en te zorgen voor de interoperabiliteit van de databanken en informatiesystemen van de EU.

Het huidige rechtskader voor de tweede generatie van het SIS – betreffende het gebruik van het systeem voor grenscontroles van onderdanen van derde landen – is gebaseerd op

---

2 Richtlijn 2008/115/EG van het Europees Parlement en de Raad van 16 december 2008 over gemeenschappelijke normen en procedures in de lidstaten voor de terugkeer van onderdanen van derde landen die illegaal op hun grondgebied verblijven (PB L 348 van 24.12.2008, blz. 98).

3 COM(2016) 205 final van 6.4.2016.

4 Besluit van de Commissie 2016/C 257/03 van 17.6.2016.

5 Verordening (EU) nr. 1077/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (PB L 286 van 1.11.2011, blz. 1).

Verordening (EG) nr. 1987/2006[6], een instrument van de voormalige eerste pijler. Dit voorstel vervangt[7] het rechtsinstrument dat nu van kracht is, en heeft tot doel:

- de lidstaten ertoe te verplichten een signalering in het SIS in te voeren telkens wanneer overeenkomstig Richtlijn 2008/115/EG een inreisverbod is uitgevaardigd voor een illegaal verblijvende onderdaan van een derde land;

- wat de overlegprocedure betreft, de nationale procedures voor het gebruik van het SIS te harmoniseren, om situaties te vermijden waarin een onderdaan van een derde land voor wie een inreisverbod geldt, houder is van een geldige, door een lidstaat afgegeven verblijfstitel;

- technische wijzigingen aan te brengen om de beveiliging te verbeteren en de administratieve lasten te helpen verminderen;

- het volledige gebruikstraject van het SIS aan te pakken, dus niet alleen het centrale systeem en de nationale systemen, maar ook de behoeften van de eindgebruikers, door ervoor te zorgen dat zij de voor hun taken benodigde gegevens ontvangen en aan alle beveiligingsvoorschriften voldoen wanneer zij SIS-data verwerken.

De voorstellen zijn bedoeld om het bestaande systeem verder te ontwikkelen en te verbeteren, veeleer dan om een nieuw systeem in te voeren. De herziening van het SIS zal het optreden van de Europese Unie in het kader van de Europese agenda's voor migratie en veiligheid ondersteunen en versterken. Met de herziening wordt gevolg gegeven aan:

(1) de resultaten van het werk aan de implementatie van het SIS gedurende de afgelopen drie jaar, waarbij technische wijzigingen aan het centrale SIS zijn aangebracht om een aantal bestaande signaleringscategorieën uit te breiden en nieuwe functies te integreren;

(2) aanbevelingen voor technische en procedurele wijzigingen die zijn opgesteld naar aanleiding van een uitgebreide evaluatie van het SIS[8];

(3) vragen van eindgebruikers van het SIS om technische verbeteringen aan te brengen, en

(4) de tussentijdse bevindingen van de deskundigengroep op hoog niveau voor informatiesystemen en interoperabiliteit[9] met betrekking tot de kwaliteit van de gegevens.

Aangezien dit voorstel onlosmakelijk verbonden is met het voorstel van de Commissie voor een verordening inzake de instelling, de werking en het gebruik van het SIS op het gebied van

---

6 Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 381 van 28.12.2006, blz. 4).

7 In punt 2 "Keuze van het instrument" wordt uitgelegd waarom is besloten de vigerende wetgeving te vervangen in plaats van deze te herschikken.

8 Verslag aan het Europees Parlement en aan de Raad over de evaluatie van het Schengeninformatiesysteem van de tweede generatie (SIS II) in overeenstemming met artikel 24, lid 5, artikel 43, lid 3, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006 en artikel 59, lid 3, en artikel 66, lid 5, van Besluit 2007/533/JBZ, en een bijbehorend werkdocument van de diensten van de Commissie. (PB …).

9 Deskundigengroep op hoog niveau – Verslag van de voorzitter van 21 december 2016.

politiële samenwerking en justitiële samenwerking in strafzaken, overlappen de twee teksten elkaar gedeeltelijk, onder meer waar het gaat om maatregelen inzake het volledige gebruikstraject van het SIS van begin tot eind (dus niet alleen de werking van het centrale systeem en de nationale systemen, maar ook de behoeften van de eindgebruikers), om versterkte maatregelen voor de bedrijfscontinuïteit, om maatregelen inzake kwaliteit, bescherming en beveiliging van de gegevens, en om bepalingen inzake monitoring, evaluatie en rapportage. Het gebruik van biometrische gegevens is eveneens in beide voorstellen aan de orde[10].

Als gevolg van de escalatie van de migratie- en vluchtelingencrisis in 2015 is de behoefte aan doeltreffende maatregelen tegen irreguliere migratie aanzienlijk toegenomen. In het *EU-actieplan inzake terugkeer*[11] kondigde de Commissie aan dat zij zou voorstellen de lidstaten ertoe te verplichten alle inreisverboden in het SIS in te voeren, om te helpen voorkomen dat onderdanen van derde landen die het grondgebied van de lidstaten niet mogen binnenkomen en er niet mogen verblijven, opnieuw het Schengengebied binnenkomen. Inreisverboden die overeenkomstig Richtlijn 2008/115/EG zijn uitgevaardigd, gelden voor het hele Schengengebied en kunnen bijgevolg aan de buitengrenzen ook worden uitgevoerd door de autoriteiten van een andere lidstaat dan die welke het verbod heeft uitgevaardigd. In de bestaande Verordening (EG) nr. 1987/2006 is alleen de mogelijkheid, maar niet de verplichting, opgenomen om signaleringen met het oog op weigering van toegang en verblijf op basis van inreisverboden in het SIS in te voeren. Door de invoering van alle inreisverboden in het SIS verplicht te stellen, kan een grotere mate van doeltreffendheid en harmonisatie worden bereikt.

- **Samenhang met de huidige bepalingen op dit beleidsgebied alsook met bestaande en toekomstige rechtsinstrumenten**

Dit voorstel is volledig in overeenstemming met en afgestemd op de bepalingen van Richtlijn 2008/115/EG inzake het uitvaardigen en uitvoeren van inreisverboden. Derhalve vult het de bestaande bepalingen over inreisverboden aan en draagt het bij tot de doeltreffende uitvoering van deze verboden aan de buitengrenzen, door de toepassing van de verplichtingen uit hoofde van de terugkeerrichtlijn te vergemakkelijken en te voorkomen dat de betrokken onderdanen van derde landen opnieuw het Schengengebied binnenkomen.

- **Samenhang met andere beleidsterreinen van de Unie**

Dit voorstel is nauw verbonden met en vormt een aanvulling op ander beleid van de Unie, meer bepaald inzake:

(1) **interne veiligheid**, omdat het SIS bijdraagt tot het voorkomen van de binnenkomst van onderdanen van derde landen die een bedreiging vormen voor de veiligheid;

(2) **gegevensbescherming**, in de zin dat dit voorstel borg staat voor de bescherming van de grondrechten van personen van wie persoonsgegevens in het SIS worden verwerkt.

(3) Voorts is het voorstel nauw verbonden met en een aanvulling op bestaande wetgeving van de Unie, meer bepaald inzake:

---

[10] Zie punt 5 "Overige elementen" voor een gedetailleerde toelichting bij de wijzigingen die in dit voorstel zijn opgenomen.

[11] COM(2015) 453 final.

(4) **beheer van de buitengrenzen**, in de zin dat dit voorstel de lidstaten helpt om hun deel van de EU-buitengrenzen te controleren en om het EU-systeem voor buitengrenstoezicht doeltreffender te maken;

(5) een doeltreffend **terugkeerbeleid** van de EU, door middel van het verbeteren en versterken van het EU-systeem om op te sporen en te voorkomen dat onderdanen van derde landen na hun terugkeer opnieuw het Schengengebied binnenkomen. Dit voorstel zou bijdragen tot een van de voornaamste doelstellingen van de Europese migratieagenda[12]: het ontmoedigen van irreguliere migratie naar de EU;

(6) **de Europese grens- en kustwacht**, (i) door het personeel van het Agentschap de mogelijkheid te bieden risicoanalyses uit te voeren, (ii) door de centrale ETIAS-eenheid in het Agentschap toegang tot het SIS te geven met het oog op de toepassing van het voorgestelde Europees systeem voor reisinformatie en -autorisatie (ETIAS)[13] en (iii) door de Europese grens- en kustwachtteams, de teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken en leden van de ondersteuningsteams voor migratiebeheer, binnen de grenzen van hun mandaat, het recht te geven op toegang tot en bevraging van de in het SIS ingevoerde gegevens via een daartoe geïnstalleerde technische interface;

(7) **Europol**, vanwege de voorgestelde uitbreiding van de rechten op toegang tot en bevraging van de in het SIS ingevoerde gegevens binnen de grenzen van het mandaat van Europol.

Voorts is het voorstel nauw verbonden met en een aanvulling op toekomstige wetgeving van de Unie, meer bepaald inzake:

(8) **het inreis-/uitreissysteem**, waarin een combinatie van gezichtsopnamen en vingerafdrukken wordt voorgesteld als biometrische identificatiemiddelen voor de toepassing van het inreis-uitreissysteem (EES) – een aanpak die in dit voorstel moet worden weerspiegeld;

(9) **het ETIAS**, waarin een grondige veiligheidsbeoordeling, inclusief verificatie in het SIS, wordt voorgesteld voor van de visumplicht vrijgestelde onderdanen van derde landen die naar de EU willen reizen.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

De voorgestelde bepalingen inzake geïntegreerd grensbeheer en illegale immigratie zijn gebaseerd op artikel 77, lid 2, onder b) en d), en artikel 79, lid 2, onder c), van het Verdrag betreffende de werking van de Europese Unie.

• Variabele geometrie

Dit voorstel bouwt voort op de bepalingen van het Schengenacquis die betrekking hebben op grenscontroles. Er moet dan ook rekening worden gehouden met de hierna genoemde gevolgen van de diverse protocollen en overeenkomsten met geassocieerde landen.

---

12 COM(2015) 240 final.

13 COM(2016) 731 final.

Denemarken: overeenkomstig artikel 4 van Protocol nr. 22 bij de Verdragen, betreffende de positie van Denemarken, beslist Denemarken binnen een termijn van zes maanden nadat de Raad over deze verordening heeft beslist of het dit voorstel, dat voortbouwt op het Schengenacquis, in zijn nationale wetgeving opneemt.

Verenigd Koninkrijk en Ierland: overeenkomstig de artikelen 4 en 5 van het Protocol betreffende het Schengenacquis dat is opgenomen in het kader van de Europese Unie en overeenkomstig Besluit 2000/365/EG van de Raad van 29 mei 2000 betreffende het verzoek van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland deel te mogen nemen aan enkele van de bepalingen van het Schengenacquis en Besluit 2002/192/EG van de Raad van 28 februari 2002 betreffende het verzoek van Ierland deel te mogen nemen aan bepalingen van het Schengenacquis, nemen het Verenigd Koninkrijk en Ierland niet deel aan de aanneming van Verordening (EU) 2016/399 (Schengengrenscode), noch aan enig ander rechtsinstrument dat wordt gerekend tot hetgeen algemeen bekend staat als het "Schengenacquis", dat wil zeggen de rechtsinstrumenten ter organisatie en ondersteuning van de afschaffing van het toezicht aan de binnengrenzen en de begeleidende maatregelen betreffende het toezicht aan de buitengrenzen. Deze verordening houdt een ontwikkeling van dit acquis in, en het Verenigd Koninkrijk en Ierland nemen derhalve niet deel aan de aanneming van deze verordening, die dan ook niet bindend voor, noch van toepassing op het Verenigd Koninkrijk en Ierland is.

Bulgarije en Roemenië: deze verordening vormt een rechtsbesluit dat op het Schengenacquis voortbouwt, of anderszins daaraan is gerelateerd in de zin van artikel 4, lid 2, van de Toetredingsakte van 2005. Deze verordening moet worden gelezen in samenhang met Besluit 2010/365/EU van de Raad van 29 juni 2010[14], waarbij de bepalingen van het Schengenacquis die betrekking hebben op het Schengeninformatiesysteem, met inachtneming van bepaalde beperkingen, toepasselijk zijn gemaakt in Bulgarije en Roemenië.

Cyprus en Kroatië: deze verordening vormt een rechtsbesluit dat op het Schengenacquis voortbouwt, of anderszins daaraan is gerelateerd in de zin van respectievelijk artikel 3, lid 2, van de Toetredingsakte van 2003 en artikel 4, lid 2, van de Toetredingsakte van 2011.

Geassocieerde landen: op basis van de respectieve overeenkomsten met IJsland, Noorwegen, Zwitserland en Liechtenstein, waardoor deze landen bij de uitvoering, toepassing en ontwikkeling van het Schengenacquis worden betrokken, zal de voorgestelde verordening voor deze landen bindend zijn.

- **Subsidiariteit**

Met dit voorstel wordt het bestaande SIS, dat sinds 1995 operationeel is, verder ontwikkeld en uitgebouwd. Het oorspronkelijke intergouvernementele kader is per 9 april 2013 vervangen door instrumenten van de Unie (Verordening (EG) nr. 1987/2006 en Besluit 2007/533/JBZ van de Raad). Bij vorige gelegenheden is een uitvoerige subsidiariteitstoets uitgevoerd. Dit initiatief dient om de bestaande bepalingen te verfijnen, de lacunes op te vullen en de operationele procedures te verbeteren.

Gedecentraliseerde oplossingen zijn ontoereikend om een dermate intensieve informatie-uitwisseling tussen de lidstaten in goede banen te leiden. Vanwege de omvang, de gevolgen

[14] Besluit van de Raad van 29 juni 2010 betreffende de toepassing van de bepalingen van het Schengenacquis die betrekking hebben op het Schengeninformatiesysteem in de Republiek Bulgarije en Roemenië (PB L 166 van 1.7.2010, blz. 17).

en de impact van de geplande maatregel kan dit voorstel beter worden verwezenlijkt op het niveau van de Unie.

Het voorstel heeft onder meer tot doel technische verbeteringen aan te brengen om de doeltreffendheid van het SIS te verbeteren en het gebruik van het systeem in alle deelnemende lidstaten te harmoniseren. Omdat deze doelstellingen een grensoverschrijdende dimensie hebben en omdat het waarborgen van een doeltreffende grensoverschrijdende informatie-uitwisseling ter bestrijding van steeds weer andersoortige dreigingen met bepaalde uitdagingen gepaard gaat, bevindt de EU zich in een goede positie om oplossingen aan te dragen die niet voldoende door de lidstaten kunnen worden verwezenlijkt.

Indien de tekortkomingen van het SIS niet worden aangepakt, bestaat het risico dat tal van kansen op een maximale efficiëntie en Europese meerwaarde worden gemist en dat blinde vlekken de bevoegde autoriteiten beletten hun werk te doen. Om een voorbeeld te geven: het ontbreken van geharmoniseerde voorschriften over het wissen van overbodige signaleringen in het systeem kan een hinderpaal worden voor het vrije verkeer van personen – een fundamenteel beginsel van de Unie.

- **Evenredigheid**

Krachtens artikel 5 van het Verdrag betreffende de Europese Unie mag het optreden van de Unie niet verder gaan dan wat nodig is om de doelstellingen van de Verdragen te verwezenlijken. De vorm die voor dit EU-optreden is gekozen, moet het mogelijk maken de doelstellingen van het voorstel te verwezenlijken en het voorstel zo doeltreffend mogelijk ten uitvoer te leggen. Het voorgestelde initiatief is een herziening van de bepalingen van het SIS die betrekking hebben op grenscontroles.

Het voorstel is gebaseerd op de beginselen van "*privacy door ontwerp*". Wat het recht op bescherming van persoonsgegevens betreft, wordt de evenredigheid gewaarborgd door specifieke regels voor het wissen van signaleringen en door de verplichting de verzameling en de opslag van gegevens te beperken tot wat strikt noodzakelijk is voor de werking en de doelstellingen van het systeem. De signaleringen in het SIS bevatten uitsluitend gegevens die nodig zijn om een persoon of voorwerp te identificeren en te lokaliseren en om passende operationele maatregelen te nemen. Nadere gegevens worden verstrekt via de Sirene-bureaus in het kader van de uitwisseling van aanvullende informatie.

Bovendien moeten uit hoofde van het voorstel alle garanties worden geboden en alle mechanismen worden toegepast die nodig zijn om de grondrechten van de persoon op wie de gegevens betrekking hebben (de betrokkene), doeltreffend te beschermen, met name wat diens persoonlijke levenssfeer en persoonsgegevens betreft. Het voorstel bevat ook bepalingen die specifiek bedoeld zijn om de SIS-persoonsgegevens over individuen beter te beveiligen.

Voor de werking van het systeem zijn op EU-niveau geen verdere processen of harmonisatiemaatregelen nodig. De voorgenomen maatregel vereist geen verdere EU-actie om de gestelde doelen te bereiken, en is derhalve evenredig.

- **Keuze van het instrument**

De herziening wordt voorgesteld in de vorm van een verordening ter vervanging van Verordening (EG) nr. 1987/2006. Deze benadering is ook gevolgd voor Besluit 2007/533/JBZ van de Raad en dient, vanwege het intrinsieke verband tussen beide instrumenten, dus tevens te worden toegepast voor Verordening (EG) nr. 1987/2006. Besluit 2007/533/JBZ is aangenomen als een zogenoemd "instrument van de derde pijler" in het kader van het Verdrag

betreffende de Europese Unie. Dergelijke instrumenten werden door de Raad vastgesteld, zonder dat het Europees Parlement hierbij als medewetgever betrokken was. De rechtsgrondslag van het voorstel is opgenomen in het Verdrag betreffende de werking van de Europese Unie (VWEU), omdat met de inwerkingtreding van het Verdrag van Lissabon op 1 december 2009 een einde is gekomen aan de pijlerstructuur. Uit hoofde van de rechtsgrondslag moet de gewone wetgevingsprocedure worden gevolgd. Omdat de bepalingen verbindend zijn en rechtstreeks toepasselijk in elke lidstaat, is de keuze van een verordening als instrument verplicht.

Het met het voorstel beoogde doel – de verdere ontwikkeling en versterking van een bestaand gecentraliseerd systeem voor samenwerking tussen de lidstaten – vereist een gemeenschappelijke architectuur en bindende werkingsvoorschriften. Met betrekking tot de toegang tot het systeem, ook voor rechtshandhavingsdoeleinden, worden bindende regels vastgesteld die gelijk zijn voor alle lidstaten en voor het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht[15] (eu-LISA). eu-LISA is sinds 9 mei 2013 verantwoordelijk voor het operationele beheer van het centrale SIS II en moet er in dat verband voor zorgen dat het centrale SIS 24 uur per dag en 7 dagen per week, volledig operationeel is. Het voorstel bouwt voort op de verantwoordelijkheden van eu-LISA in verband met het SIS.

Voorts worden rechtstreeks toepasselijke voorschriften voorgesteld op grond waarvan de betrokkene zijn eigen gegevens mag inzien en toegang krijgt tot rechtsmiddelen, zonder dat daarvoor verdere uitvoeringsmaatregelen moeten worden vastgesteld.

Derhalve kan alleen voor een verordening als rechtsinstrument worden gekozen.

3. RESULTATEN VAN EX-POSTEVALUATIES, RAADPLEGINGEN VAN BELANGHEBBENDEN EN EFFECTBEOORDELINGEN

• Ex-postevaluaties/geschiktheidscontroles van bestaande wetgeving

Overeenkomstig Verordening (EG) nr. 1987/2006 en Besluit 2007/533/JBZ van de Raad[16] heeft de Commissie drie jaar na de ingebruikneming van het SIS II een algemene evaluatie opgesteld van het centrale SIS II en van de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten.

De evaluatie had specifiek betrekking op de toepassing artikel 24 van Verordening (EG) nr. 1987/2006 en moest uitmonden in voorstellen om dit artikel te wijzigen met het oog op een verdere harmonisatie van de criteria voor opneming van signaleringen.

Uit deze evaluatie kwam nadrukkelijk naar voren dat de rechtsgrondslag van het SIS moest worden aangepast om beter te kunnen reageren op nieuwe uitdagingen in het kader van veiligheid en migratie. Met dat doel voor ogen worden voorstellen gedaan inzake de

---

15 Opgericht bij Verordening (EU) nr. 1077/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (PB L 286 van 1.11.2011, blz. 1).

16 Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 205 van 7.8.2007, blz. 63).

verplichte opneming van inreisverboden in het SIS teneinde deze beter te kunnen uitvoeren, verplicht overleg tussen de lidstaten om het naast elkaar bestaan van een inreisverbod en een verblijfstitel te vermijden, de optie om personen op basis van hun vingerafdrukken te identificeren en te lokaliseren aan de hand van een nieuw automatisch systeem voor identificatie aan de hand van vingerafdrukken, en uitbreiding van de biometrische identificatiemiddelen in het systeem.

Uit de evaluatie bleek ook dat wetswijzigingen nodig zijn om de technische werking van het systeem te verbeteren en nationale processen te stroomlijnen. Door het gebruik van het SIS te vergemakkelijken en onnodige lasten te verminderen, zullen deze maatregelen het SIS efficiënter en doeltreffender maken. Daarnaast worden maatregelen voorgesteld om de kwaliteit van de gegevens en de transparantie van het systeem te verbeteren door de specifieke rapportageverplichtingen van de lidstaten en eu-LISA beter te omschrijven.

De voorgestelde maatregelen zijn gebaseerd op de resultaten van de algemene evaluatie (het evaluatieverslag en het bijbehorende werkdocument van de diensten van de Commissie zijn op 21 december 2016 aangenomen[17]).

Voorts heeft de Commissie in 2014 overeenkomstig artikel 19 van Richtlijn 2008/115/EG (de terugkeerrichtlijn) een mededeling over het terugkeerbeleid van de EU[18] bekendgemaakt, waarin verslag wordt gedaan van de toepassing van die richtlijn. Daarin wordt geconcludeerd dat het potentieel van het SIS voor het terugkeerbeleid verder moet worden vergroot, en dat de herziening van het SIS het mogelijk zal maken het terugkeerbeleid en het SIS dichter bij elkaar te brengen en de kans zal bieden om voor te stellen de lidstaten te verplichten om een op grond van de terugkeerrichtlijn uitgevaardigd inreisverbod in het SIS op te nemen.

- **Raadpleging van belanghebbenden**

Naar aanleiding van haar evaluatie van het SIS heeft de Commissie overeenkomstig de procedure van artikel 51 van Verordening (EG) nr. 1987/2006 de relevante belanghebbenden, waaronder de afgevaardigden die in het SISVIS-comité zitting hebben, verzocht om commentaar en suggesties. De vertegenwoordigers van de lidstaten in dit comité gaan over operationele Sirene-aangelegenheden (grensoverschrijdende samenwerking met betrekking tot het SIS) en technische aangelegenheden op het gebied van ontwikkeling en onderhoud van het SIS en de betrokken Sirene-applicatie.

Als onderdeel van het evaluatieproces werden aan deze gedelegeerden gedetailleerde vragenlijsten voorgelegd. Verduidelijkingen of nadere toelichtingen werden gegeven via e-mail of in gerichte gesprekken.

Dankzij dit interactieve proces konden alle aspecten van een onderwerp op een transparante manier aan de orde worden gesteld. Vervolgens zijn deze kwesties in de loop van 2015 en 2016 door de afgevaardigden in het SISVIS-comité besproken tijdens speciaal daarvoor georganiseerde bijeenkomsten en workshops.

---

17 Verslag aan het Europees Parlement en aan de Raad over de evaluatie van het Schengeninformatiesysteem van de tweede generatie (SIS II) in overeenstemming met artikel 24, lid 5, artikel 43, lid 3, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006 en artikel 59, lid 3, en artikel 66, lid 5, van Besluit 2007/533/JBZ, en een bijbehorend werkdocument van de diensten van de Commissie.

18 COM(2014) 199 final.

De Commissie heeft ook gericht overleg gepleegd met de nationale gegevensbeschermingsautoriteiten en met leden van de coördinatiegroep voor toezicht SIS II op het gebied van gegevensbescherming. De lidstaten hebben aan de hand van een speciale vragenlijst verslag uitgebracht over hun ervaringen met inzageverzoeken van betrokkenen en het werk van de nationale gegevensbeschermingsautoriteiten. Bij het opstellen van het voorstel is rekening gehouden met de antwoorden op de desbetreffende vragenlijst van juni 2015.

Intern heeft de Commissie een horizontale stuurgroep opgezet met vertegenwoordigers van het secretariaat-generaal en van de directoraten-generaal Migratie en Binnenlandse Zaken, Justitie en Consumenten, Personele middelen en veiligheid, en Informatica. Deze groep monitorde het evaluatieproces en gaf sturing waar dat nodig was.

In de evaluatiebevindingen zijn tevens gegevens verwerkt die tijdens evaluatiebezoeken aan de lidstaten zijn verzameld in het kader van een nauwgezet onderzoek naar het praktische gebruik van het SIS. Dit materiaal bestaat onder meer uit besprekingen en gesprekken met systeemgebruikers, personeel van Sirene-bureaus en nationale bevoegde autoriteiten.

Daarnaast zijn de voor terugkeer bevoegde autoriteiten van de lidstaten verzocht om in het kader van de Contactgroep Terugkeerrichtlijn van de Commissie, tijdens de vergaderingen van 16 november 2015, 18 maart 2016 en 20 juni 2016, commentaar en suggesties aan te dragen, met name over de gevolgen van een eventuele verplichting om in het SIS alle inreisverboden op te nemen die overeenkomstig Richtlijn 2008/115/EG zijn uitgevaardigd.

Naar aanleiding van die opmerkingen worden in deze verordening maatregelen voorgesteld om de technische en operationele efficiëntie en doeltreffendheid van het systeem te verbeteren.

- **Bijeenbrengen en benutten van deskundigheid**

Naast de resultaten van de raadpleging van de belanghebbenden zijn ook de bevindingen van vier door de Commissie uitbestede studies in het voorstel verwerkt:

- Technische beoordeling van het SIS (Kurt Salmon)[19]

  Deze beoordeling legt de vinger op de belangrijkste knelpunten in de werking van het SIS, brengt de behoeften voor de toekomst in kaart en wijst vooral op de noodzaak de bedrijfscontinuïteit te optimaliseren en de algehele architectuur af te stemmen op de vereiste capaciteitsuitbreiding.

- Effectbeoordeling van mogelijke verbeteringen van de SIS II-architectuur op het gebied van ICT (Kurt Salmon)[20]

  Deze studie beoordeelt de huidige kosten van de werking van het SIS op nationaal niveau en evalueert twee mogelijke technische scenario's om het systeem te verbeteren. Beide scenario's bevatten een reeks technische voorstellen die vooral gericht zijn op verbeteringen in het centrale systeem en de algehele architectuur.

---

19 European Commission FINAL REPORT — SIS II technical assessment.

20 European Commission FINAL REPORT — ICT Impact Assessment of Possible Improvements to the SIS II Architecture 2016.

- "Effectbeoordeling van technische verbeteringen van de SIS II-architectuur op het gebied van ICT – eindverslag van 10 november 2016 (Wavestone)[21]

In deze studie wordt nagegaan wat de implementatie van een nationale kopie de lidstaten kost. Hiervoor worden drie scenario's geanalyseerd: een volledig gecentraliseerd systeem, een gestandaardiseerde N.SIS-toepassing die door eu-LISA wordt ontwikkeld en de lidstaten ter beschikking wordt gesteld, en een afzonderlijke N.SIS-toepassing met gemeenschappelijke technische normen.

- Studie over de haalbaarheid en de gevolgen van het opzetten, in het kader van het Schengeninformatiesysteem, van een EU-wijd systeem voor het uitwisselen van gegevens over en het monitoren van de naleving van terugkeerbesluiten (PwC)[22]

Deze studie beoordeelt de haalbaarheid en de technische en operationele gevolgen van de wijzigingsvoorstellen om het gebruik van het SIS te versterken met als doel de terugkeer van irreguliere migranten te bevorderen en te voorkomen dat zij het Schengengebied opnieuw binnenkomen.

- **Effectbeoordeling**

De Commissie heeft geen effectbeoordeling uitgevoerd.

De drie hierboven genoemde onafhankelijke beoordelingen zijn als basis gebruikt om de gevolgen van een wijziging van het systeem uit technisch oogpunt in kaart te brengen. Bovendien heeft de Commissie twee evaluaties van het Sirene-handboek opgesteld sinds 2013, d.w.z. sinds de ingebruikneming van het SIS II op 9 april 2013 en het van kracht worden van Besluit 2007/533/JBZ. Dit evaluatieproces omvat een tussentijdse herziening die geleid heeft tot de invoering van een nieuw Sirene-handboek[23] op 29 januari 2015. Voorts heeft de Commissie een catalogus van beste praktijken en aanbevelingen[24] vastgesteld. Bovendien brengen eu-LISA en de lidstaten geregeld technische verbeteringen aan in het systeem. Er wordt van uitgegaan dat deze mogelijkheden inmiddels zijn uitgeput en dat de rechtsgrondslag aan een volledige herziening toe is. Om echt duidelijkheid te verschaffen over de toepassing van eindgebruikersystemen en om nadere bepalingen over het wissen van signaleringen vast te stellen, is meer nodig dan louter een verbetering van de tenuitvoerlegging en de uitvoering.

Voorts heeft de Commissie overeenkomstig artikel 24, lid 5, artikel 43, lid 3, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006 en artikel 59, lid 3, en artikel 66, lid 5, van Besluit 2007/533/JBZ een algemene evaluatie van het SIS opgesteld en een bijbehorend werkdocument van de diensten van de Commissie bekendgemaakt. De voorgestelde

---

21 European Commission FINAL REPORT — ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report", 10 november 2016, (Wavestone).

22 Study on the feasibility and implications of setting up within the framework of the SIS and EU-wide system for exchanging data on and monitoring compliance with return decisions, 4 april 2015, PwC.

23 Uitvoeringsbesluit (EU) 2015/219 van de Commissie van 29 januari 2015 tot vervanging van de bijlage bij Uitvoeringsbesluit 2013/115/EU tot vaststelling van het Sirene-handboek en andere uitvoeringsmaatregelen voor het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 44 van 18.2.2015, blz. 75).

24 Aanbeveling van de Commissie voor de opstelling van een catalogus van aanbevelingen en beste praktijken voor de juiste toepassing van het Schengeninformatiesysteem van de tweede generatie (SIS II) en de uitwisseling van aanvullende informatie door de bevoegde autoriteiten van de lidstaten die SIS II uitvoeren en toepassen (C(2015) 9169/1).

maatregelen zijn gebaseerd op de resultaten van de algemene evaluatie (het evaluatieverslag en het bijbehorende werkdocument van de diensten van de Commissie zijn op 21 december 2016 aangenomen).

Op grond van het Schengenevaluatiemechanisme dat is vastgesteld in Verordening (EU) nr. 1053/2013[25], kan de werking van het SIS in de lidstaten op gezette tijden uit juridisch en operationeel oogpunt worden geëvalueerd. De evaluaties worden gezamenlijk door de Commissie en de lidstaten uitgevoerd. Via dit mechanisme doet de Raad aanbevelingen aan afzonderlijke lidstaten op basis van de evaluaties die in het kader van de meerjarenprogramma's en jaarprogramma's zijn opgesteld. Deze aanbevelingen zijn per definitie ad hoc van toepassing en kunnen bijgevolg niet de plaats innemen van juridisch bindende regels die tegelijkertijd van toepassing zijn op alle lidstaten die gebruikmaken van het SIS.

In het SISVIS-comité zijn regelmatig praktische operationele en technische kwesties aan de orde. Niettegenstaande de nuttige rol van deze bijeenkomsten in de samenwerking tussen de Commissie en de lidstaten bieden de resultaten van deze besprekingen (tenzij het gaat om wetswijzigingen) geen oplossing voor problemen als gevolg van, bijvoorbeeld, uiteenlopende nationale praktijken.

De in deze verordening voorgestelde wijzigingen hebben geen significante gevolgen voor de economie of het milieu. Op sociaal vlak daarentegen wordt van deze veranderingen wel een significant positief effect verwacht, aangezien zij zorgen voor meer veiligheid, door een betere identificatie mogelijk te maken van personen die zich van een valse identiteit bedienen, criminelen van wie de identiteit na het plegen van een ernstige misdaad onbekend is gebleven, en irreguliere migranten die misbruik maken van de ruimte zonder binnengrenstoezicht. De impact van deze wijzigingen op de grondrechten en de bescherming van gegevens is in beschouwing genomen en wordt verder toegelicht in het volgende punt (Grondrechten).

Het voorstel is opgesteld aan de hand van het omvangrijke corpus aan gegevens dat is verzameld toen, naar aanleiding van de algemene evaluatie van het SIS van de tweede generatie, werd onderzocht of het systeem naar behoren werkte en waar het eventueel kon verbeterd. Bovendien is een studie verricht naar de weerslag van de kosten, om te garanderen dat werd gekozen voor de meest passende en evenredige nationale architectuur.

- **Grondrechten en gegevensbescherming**

Dit voorstel is bedoeld om een bestaand systeem te ontwikkelen en te verbeteren, veeleer dan om een nieuw systeem in te voeren, en bouwt bijgevolg voort op belangrijke en doeltreffende garanties die nu reeds worden geboden. Dit neemt niet weg dat het voorgestelde systeem gevolgen kan hebben voor de grondrechten van een persoon, aangezien het naast de gebruikelijke persoonsgegevens ook nog andere categorieën gevoelige biometrische gegevens zal verwerken. Deze gevolgen zijn grondig onderzocht en er zijn aanvullende garanties opgenomen om de verzameling en verdere verwerking van gegevens te beperken tot wat strikt noodzakelijk en operationeel vereist is, en om de toegang tot die gegevens te beperken tot degenen die deze uit operationele noodzaak moeten verwerken. Het voorstel voorziet in duidelijke termijnen voor de bewaring van de gegevens, alsook in de uitdrukkelijke erkenning

[25] Verordening (EU) nr. 1053/2013 van 7 oktober 2013 betreffende de instelling van een evaluatiemechanisme voor de controle van en het toezicht op de toepassing van het Schengenacquis en houdende intrekking van het besluit van 16 september 1998 tot oprichting van de Permanente Schengenbeoordelings- en toepassingscommissie (PB L 295 van 6.11.2013, blz. 27).

en vaststelling van het recht van personen op inzage van hen betreffende gegevens en op rectificatie en wissing van die gegevens in overeenstemming met hun grondrechten (zie het deel over gegevensbescherming en veiligheid).

Het voorstel zet de bescherming van de grondrechten kracht bij, door de voorschriften voor het wissen van een signalering in wetgeving te verankeren en een evenredigheidsbeoordeling in te voeren voor het verlengen van een signalering. De ruime en solide waarborgen inzake het gebruik van biometrische identificatiemiddelen moeten voorkomen dat onschuldige personen problemen ondervinden.

De verplichting het volledige traject van het systeem te beveiligen staat borg voor een betere bescherming van de daarin opgeslagen gegevens. Dankzij de invoering van een duidelijke procedure voor incidentenbeheer en de verbetering van de bedrijfscontinuïteit van het SIS is dit voorstel volledig in overeenstemming met het Handvest van de grondrechten van de Europese Unie[26], en dat niet alleen met betrekking tot het recht op de bescherming van persoonsgegevens. Ook de veiligheid van personen in de samenleving gaat erop vooruit wanneer het SIS verder wordt ontwikkeld en doeltreffend zijn werk kan blijven doen.

Inzake biometrische identificatiemiddelen worden belangrijke wijzigingen voorgesteld. Naast vingerafdrukken zouden ook handpalmafdrukken moeten worden verzameld en opgeslagen indien aan de wettelijke vereisten wordt voldaan. Logbestanden van vingerafdrukken worden overeenkomstig artikel 24 gekoppeld aan alfanumerieke SIS-signaleringen. In de toekomst zou het mogelijk moeten zijn deze dactyloscopische gegevens (vinger- en handpalmafdrukken) te doorzoeken aan de hand van vingerafdrukken die op een plaats delict zijn aangetroffen, op voorwaarde dat het delict als een terroristisch misdrijf of ander ernstig strafbaar feit wordt beschouwd, en met een hoge mate van waarschijnlijkheid kan worden vastgesteld dat de afdrukken die van de dader zijn. Indien de documenten van een persoon geen uitsluitsel geven over diens identiteit, zouden de bevoegde autoriteiten de vingerafdrukken van die persoon moeten toetsen aan de vingerafdrukken die zijn opgeslagen in de SIS-databank.

Op grond van het voorstel moeten extra gegevens worden verzameld en opgeslagen (zoals gegevens over de persoonlijke identificatiedocumenten) die het voor de functionarissen in het veld gemakkelijker maken de identiteit van een persoon vast te stellen.

Het voorstel waarborgt het recht van de betrokkene op beschikbare effectieve rechtsmiddelen om besluiten aan te vechten, waaronder een doeltreffende voorziening in rechte overeenkomstig artikel 47 van het Handvest van de grondrechten.

4. GEVOLGEN VOOR DE BEGROTING

Het SIS is één integraal informatiesysteem. Bijgevolg moeten de bedragen voor de uitgaven als genoemd in twee van de voorstellen (het onderhavige en het voorstel voor een verordening betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken) worden beschouwd als één bedrag, en niet als twee afzonderlijke bedragen. De informatie over de budgettaire gevolgen van de wijzigingen die nodig zijn voor de tenuitvoerlegging van beide voorstellen, is gebundeld in één financieel memorandum.

---

[26] Handvest van de grondrechten van de Europese Unie (2012/C 326/02).

Omdat het derde voorstel (inzake de terugkeer van illegaal verblijvende onderdanen van derde landen) een aanvulling op de twee andere vormt, worden de desbetreffende budgettaire gevolgen afzonderlijk behandeld in een apart financieel memorandum dat uitsluitend betrekking heeft op de instelling van deze specifieke signaleringscategorie.

Op basis van een beoordeling van al het werk dat aan het netwerk, aan het centrale SIS (door eu-LISA) en in de lidstaten moet worden verricht, wordt ervan uitgegaan dat voor de twee voorgestelde verordeningen een totaalbedrag van 64,3 miljoen EUR nodig zal zijn voor de periode 2018-2020.

Dit bedrag is inclusief de kosten voor het vergroten van de bandbreedte van het TESTA-NG-netwerk, dat als gevolg van deze voorstellen meer verwerkingsvermogen en capaciteit nodig heeft voor de doorzending van vingerafdrukbestanden en gezichtsopnamen (9,9 miljoen EUR). Eveneens verrekend in het hierboven genoemde bedrag zijn de kosten in verband met personeels- en operationele uitgaven (17,6 miljoen EUR). eu-LISA heeft de Commissie meegedeeld dat de aanwerving van 3 nieuwe arbeidscontractanten gepland is voor januari 2018 en de ontwikkelingsfase dus op tijd van start kan gaan om de ingebruikneming van de bijgewerkte functies van het SIS in 2020 te waarborgen. Voor de toepassing van deze voorstellen moet het centrale SIS technisch worden aangepast om een aantal bestaande signaleringscategorieën uit te breiden en nieuwe functies in te bouwen. Deze aanpassingen zijn in aanmerking genomen in het financieel memorandum bij dit voorstel.

Bovendien heeft de Commissie een studie verricht naar de weerslag van de kosten die dit voorstel op nationaal niveau met zich meebrengt[27]. Deze kosten worden geraamd op 36,8 miljoen EUR en moeten worden vergoed in de vorm van een aan de lidstaten uit te keren forfaitair bedrag. Elke lidstaat zal 1,2 miljoen EUR ontvangen om zijn nationale systeem overeenkomstig de voorgestelde vereisten te upgraden, onder meer voor het opzetten van een gedeeltelijke nationale kopie wanneer dit nog niet is gebeurd, of voor een back-upsysteem.

Gepland wordt de rest van de begroting die in het Fonds voor interne veiligheid is geoormerkt voor slimme grenzen, te herprogrammeren om de upgrades en functies die in de twee verordeningen worden voorgesteld, te implementeren. De ISF-grenzenverordening[28] is het financiële instrument waarin het budget voor de tenuitvoerlegging van het slimmegrenzenpakket is opgenomen. In artikel 5 van de verordening is bepaald dat 791 miljoen EUR wordt aangewend door middel van een programma voor het opzetten van IT-systemen ter beheersing van de migratiestromen over de buitengrenzen onder de voorwaarden als bepaald in artikel 15. 480 miljoen EUR daarvan is gereserveerd voor de ontwikkeling van het inreis-uitreissysteem en 210 miljoen EUR voor de ontwikkeling van het Europees systeem voor reisinformatie en -autorisatie (ETIAS). De rest zal gedeeltelijk worden gebruikt ter dekking van de kosten die gepaard gaan met de in de twee SIS-voorstellen opgenomen wijzigingen.

---

27 Wavestone "ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report", 10 november 2016, Scenario 3 Distinct N.SIS II Implementation.

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

5. OVERIGE ELEMENTEN

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

De Commissie, de lidstaten en eu-LISA zullen het gebruik van het SIS geregeld evalueren en monitoren om ervoor te zorgen dat het systeem doeltreffend en efficiënt blijft functioneren. Voor de uitvoering van de voorgestelde technische en operationele maatregelen zal de Commissie worden bijgestaan door het SISVIS-comité.

In artikel 54, leden 7 en 8, van het verordeningsvoorstel is bovendien een procedure voor een regelmatige evaluatie en herziening vastgelegd.

eu-LISA moet om de twee jaar verslag uitbrengen aan het Europees Parlement en de Raad over de technische werking – inclusief beveiliging – van het SIS, de communicatie-infrastructuur ter ondersteuning van het SIS, en de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten.

Voorts dient de Commissie om de vier jaar een algemene evaluatie van het SIS en de uitwisseling van informatie tussen de lidstaten op te stellen, die zij moet meedelen aan het Parlement en de Raad. In deze evaluatie wordt nagegaan:

- hoe de bereikte resultaten zich verhouden tot de doelstellingen;
- of de uitgangspunten voor het systeem nog gelden;
- hoe de verordening wordt toegepast op het centrale systeem;
- hoe het staat met de beveiliging van het centrale systeem;
- welke de gevolgen zijn voor de toekomstige werking van het systeem.

eu-LISA krijgt nu ook tot taak dagelijkse, maandelijkse en jaarlijkse statistieken over het gebruik van het SIS te verstrekken, wat ervoor zorgt dat niet alleen het systeem zelf continu wordt gemonitord, maar ook de mate waarin het voldoet aan de beoogde doelstellingen.

- **Toelichting bij de specifieke bepalingen van het voorstel**

Overlappingen tussen dit voorstel en het voorstel voor een verordening inzake de instelling, de werking en het gebruik van het SIS op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken

- Algemene bepalingen (artikelen 1 –3)
- Technische architectuur en werkwijze van het SIS (artikelen 4 – 14)
- Taken van eu-LISA (artikelen 15 – 18)
- Recht op toegang tot signaleringen en bewaring van signaleringen (artikelen 29, 30, 31, 33 en 34)
- Algemene regels voor de verwerking en bescherming van gegevens (artikelen 36 – 53)

- Monitoring en statistieken (artikel 54)

Volledig gebruikstraject van het SIS

Het SIS wordt over heel Europa door meer dan 2 miljoen eindgebruikers bij de bevoegde autoriteiten gebruikt en vormt een doeltreffend instrument voor de uitwisseling van informatie. De voorgestelde regels bestrijken het volledige werkingstraject van het systeem – d.w.z. het centrale, door eu-LISA operationeel beheerde SIS, de nationale systemen en de applicaties voor de eindgebruikers – en hebben dus niet alleen betrekking op de systemen zelf (centraal en nationaal), maar ook op de technische en operationele behoeften van de eindgebruikers.

Krachtens artikel 9, lid 2, moeten de eindgebruikers de gegevens ontvangen die zij voor de uitvoering van hun taken nodig hebben (met name alle gegevens die vereist zijn om de betrokkene te identificeren en om de gevraagde maatregel uit te voeren). Bovendien zorgt deze bepaling voor harmonisatie van de nationale systemen, door een blauwdruk vast te stellen voor de implementatie van het SIS door de lidstaten. Krachtens artikel 6 moet elke lidstaat ervoor zorgen dat de SIS-gegevens ononderbroken beschikbaar zijn voor de eindgebruikers, zodat de kans op storingen wordt beperkt en de operationele voordelen zodoende worden geoptimaliseerd.

Artikel 10, lid 3, garandeert dat de beveiliging van de gegevensverwerking ook de activiteiten op het gebied van de gegevensverwerking door de eindgebruiker omvat. Krachtens artikel 14 moeten de lidstaten ervoor zorgen dat personeelsleden die toegang hebben tot het SIS, regelmatig en permanent worden bijgeschoold over de regels voor gegevensbeveiliging en -bescherming.

Als gevolg van de opneming van deze maatregelen biedt dit voorstel een meer omvattende dekking van het volledige werkingstraject van het SIS, met regels en verplichtingen die gelden voor de miljoenen eindgebruikers over heel Europa. Het doeltreffendst is het SIS als de lidstaten ervoor zorgen dat eindgebruikers die een nationale immigratie- of politiedatabank mogen bevragen, parallel daarmee ook telkens het SIS bevragen. Op die manier kan het SIS zijn beoogde functie als voornaamste compenserende maatregel in het gebied zonder binnengrenstoezicht vervullen en kunnen de lidstaten de grensoverschrijdende dimensie van de criminaliteit en de mobiliteit van criminelen beter aanpakken. Deze parallelle bevraging moet in overeenstemming zijn met artikel 4 van Richtlijn (EU) 2016/680[29].

Bedrijfscontinuïteit

De voorstellen versterken de bepalingen met betrekking tot de bedrijfscontinuïteit, zowel op nationaal niveau als voor eu-LISA (artikelen 4, 6, 7 en 15) en moeten ervoor zorgen dat het SIS operationeel en toegankelijk blijft voor het personeel in het veld, ook wanneer het systeem problemen ondervindt.

Gegevenskwaliteit

[29] 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 (PB L 119 van 4.5.2016, blz. 89).

Het voorstel gaat uit van het beginsel dat de lidstaat, die de eigenaar is van de gegevens, ook verantwoordelijk is voor de accuraatheid van de in het SIS opgenomen gegevens (artikel 39). Dit neemt niet weg dat een centraal, door eu-LISA beheerd mechanisme moet worden opgezet om lidstaten in de gelegenheid te stellen signaleringen waarvan de gegevens in de verplichte velden kwalitatief twijfelachtig zijn, geregeld te herzien. Daarom geeft artikel 15 van het voorstel eu-LISA de bevoegdheid om op gezette tijden verslag over de gegevenskwaliteit uit te brengen aan de lidstaten. Een gegevensregister voor het opstellen van statistische verslagen en verslagen over gegevenskwaliteit kan daarbij van dienst zijn (artikel 54). Deze verbeteringen grijpen terug op de tussentijdse bevindingen van de deskundigengroep op hoog niveau voor informatiesystemen en interoperabiliteit.

Foto's, gezichtsopnamen, dactyloscopische gegevens en DNA-profielen

De mogelijkheid om een persoon te identificeren door het systeem te bevragen aan de hand van vingerafdrukken, is al vastgelegd in artikel 22 van Verordening (EG) nr. 1987/2006 en Besluit 2007/533/JBZ. Deze voorstellen maken deze bevraging verplicht indien de identiteit van de persoon op geen andere manier kan worden vastgesteld. Momenteel is het gebruik van gezichtsopnamen alleen toegestaan om de identiteit van een persoon na een alfanumerieke opzoeking te bevestigen, en dus niet als basis voor een bevraging. Bovendien maken wijzigingen in de artikelen 22 en 28 het mogelijk om, zodra zulks technisch haalbaar is, gezichtsopnamen, foto's en handpalmafdrukken te gebruiken om het systeem te bevragen en personen te identificeren. Dactyloscopie is de wetenschappelijke studie van vingerafdrukken als identificatie-instrument. Handpalmafdrukken, aldus deskundigen op het gebied van de dactyloscopie, zijn uniek en bevatten, net als vingerafdrukken, referentiepunten die accurate en definitieve vergelijkingen mogelijk maken. Handpalmafdrukken kunnen net als vingerafdrukken worden gebruikt om de identiteit van een persoon vast te stellen. Het nemen van handpalmafdrukken, naast de tien gerolde en de tien platte vingerafdrukken, behoort al tientallen jaren tot de vaste werkmethoden van de politie. Handpalmafdrukken worden vooral gebruikt voor het identificeren van personen die al dan niet opzettelijk de toppen van hun vingers hebben beschadigd, hetzij om te vermijden dat zij worden geïdentificeerd of dat hun vingerafdrukken worden genomen, hetzij als gevolg van een ongeval of zware handenarbeid. Tijdens de besprekingen over de technische voorschriften van het SIS AFIS deelden de lidstaten mee dat men er in een aanzienlijk aantal gevallen in slaagt irreguliere migranten die hun vingertoppen opzettelijk hebben beschadigd om identificatie te voorkomen, alsnog te identificeren aan de hand van door de autoriteiten van de lidstaten genomen handpalmafdrukken.

Het gebruik van gezichtsopnamen voor identificatiedoeleinden zal ervoor zorgen dat het SIS beter aansluit op de voorstellen voor het inreis-/uitreissysteem van de EU, e-gates en zelfbedieningsloketten. Deze functie zal alleen beschikbaar zijn in reguliere grensdoorlaatposten.

Toegang van autoriteiten tot het SIS — institutionele gebruikers

In dit deel wordt beschreven wat er voor de EU-agentschappen (institutionele gebruikers) veranderd is op het gebied van toegangsrechten. De toegangsrechten voor de bevoegde nationale autoriteiten zijn niet gewijzigd.

Europol (artikel 30) en het Europees Grens- en kustwachtagentschap – en de bijbehorende teams, teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken, en leden van het ondersteuningsteam voor migratiebeheer – alsmede de centrale ETIAS-eenheid binnen het Agentschap (artikelen 31 en 32) hebben toegang tot het SIS en de

SIS-gegevens die zij nodig hebben. Passende waarborgen zorgen voor een adequate bescherming van de gegevens in het systeem (onder meer door deze instanties uitsluitend toegang te geven tot de gegevens die zij nodig hebben om hun taken uit te voeren – artikel 33).

Als gevolg van de wijzigingen krijgt Europol, met het oog op een optimaal gebruik van het SIS bij het uitvoeren van zijn taken, tevens toegang tot signaleringen met het oog op weigering van toegang, en worden er nieuwe bepalingen toegevoegd om het Europees Grens- en kustwachtagentschap en zijn teams toegang tot het systeem te verschaffen bij de uitvoering van de verschillende activiteiten in het kader van hun mandaat ter ondersteuning van de lidstaten. In het kader van het voorstel van de Commissie voor een verordening van het Europees Parlement en de Raad tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS)[30] zal de centrale ETIAS-eenheid van het Europees Grens- en kustwachtagentschap via het ETIAS in het SIS verifiëren of de betrokken onderdaan van een derde land die een reisautorisatie aanvraagt, in het SIS is gesignaleerd. Met het oog daarop krijgt de centrale ETIAS-eenheid ook toegang tot het SIS[31].

Krachtens artikel 29, lid 3, hebben de nationale visumautoriteiten, in het kader van de uitvoering van hun taken, toegang tot signaleringen inzake documenten die zijn afgegeven overeenkomstig Verordening 2008/… betreffende de instelling, de werking en het gebruik van het SIS op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken.

Hierdoor krijgen deze instanties toegang tot het SIS en de SIS-gegevens die zij voor hun taken nodig hebben en wordt tegelijkertijd op passende wijze gewaarborgd dat de in het systeem opgenomen gegevens behoorlijk worden beschermd (onder meer door in artikel 35 te bepalen dat deze instanties uitsluitend toegang krijgen tot de gegevens die zij nodig hebben om hun taken uit te voeren).

Weigering van toegang en verblijf

Momenteel kan een lidstaat krachtens artikel 24, lid 3, van de SIS II-verordening een signalering in het SIS opnemen ten aanzien van personen voor wie een inreisverbod geldt in verband met een overtreding van de nationale wetsbepalingen inzake immigratie. Op grond van de hier voorgestelde herziene versie van artikel 24, lid 3, moet in het SIS een signalering worden opgenomen telkens wanneer overeenkomstig Richtlijn 2008/115/EG een inreisverbod is uitgevaardigd voor een illegaal verblijvende onderdaan van een derde land. In het herziene artikel wordt tevens bepaald wanneer en onder welke voorwaarden een dergelijke signalering moet worden opgenomen nadat de onderdaan van het derde land het grondgebied van de lidstaten in overeenstemming met de terugkeerverplichting heeft verlaten. Deze bepaling is ingevoegd om te voorkomen dat inreisverboden zichtbaar zijn in het SIS terwijl de betrokken onderdaan van het derde land zich nog op het grondgebied van de EU bevindt. Een inreisverbod verbiedt de betrokkene het grondgebied van de lidstaten opnieuw binnen te komen, en kan dus pas van kracht worden na de terugkeer van deze persoon naar een derde land. Tegelijkertijd moeten de lidstaten ervoor zorgen dat het tijdstip van terugkeer volledig samenvalt met het tijdstip waarop de signalering met het oog op weigering van toegang en verblijf in het SIS wordt geactiveerd.

---

30 COM(2016) 731 final.

31 Meer bepaald op grond van de artikelen 24 en 27 van deze verordening.

Dit voorstel houdt nauw verband met het voorstel van de Commissie[32] betreffende het gebruik van het SIS voor de terugkeer van illegaal verblijvende onderdanen van derde landen, waarin wordt vastgesteld volgens welke voorwaarden en procedures signaleringen inzake terugkeerbesluiten moeten worden opgenomen in het SIS. Naast een mechanisme om te monitoren of onderdanen van derde landen ten aanzien van wie een terugkeerbesluit is uitgevaardigd, het grondgebied van de EU daadwerkelijk verlaten, bevat dat voorstel ook een waarschuwingsmechanisme voor gevallen waarin de betrokken regels niet in acht worden genomen. Artikel 26 beschrijft de overlegprocedure die de lidstaten moeten volgen wanneer zij signaleringen met het oog op weigering van toegang en verblijf aantreffen of willen opnemen die onverenigbaar zijn met besluiten van andere lidstaten, bijvoorbeeld tot verlening van een geldige verblijfstitel. Deze regels zijn bedoeld om tegenstrijdige instructies voor dergelijke gevallen te voorkomen dan wel op te heffen, en tevens als duidelijk richtsnoer voor zowel de eindgebruikers (inzake de maatregelen die zij in dergelijke situaties moeten nemen) als de autoriteiten van de lidstaten (inzake het al dan niet wissen van een signalering).

Artikel 27 (het vroegere artikel 26 van Verordening (EG) nr. 1987/2006) betreft de tenuitvoerlegging van de EU-sanctieregeling voor onderdanen van derde landen ten aanzien van wie overeenkomstig artikel 29 van het Verdrag betreffende de Europese Unie een beperkende maatregel is genomen om de toegang tot het EU-grondgebied te beletten. Aangezien de opneming van zulke signaleringen alleen mogelijk is aan de hand van de minimumgegevens die nodig zijn om een persoon te identificeren, meer bepaald achternaam en geboortedatum, moest een verplichting in die zin worden opgelegd. Het feit dat Verordening (EG) nr. 1987/2006 vrijstelling verleende van de verplichting de geboortedatum op te nemen, heeft aanzienlijke problemen veroorzaakt, aangezien overeenkomstig de technische regels en de zoekparameters van het systeem geen signalering in het SIS kan worden gecreëerd zonder een geboortedatum. Aangezien artikel 27 onontbeerlijk is voor een doeltreffende EU-sanctieregeling, is de evenredigheidsvereiste in dit verband niet van toepassing.

Omwille van een betere samenhang met Richtlijn 2008/115/EG is de terminologie betreffende het doel van de signalering (weigering van toegang en verblijf) in overeenstemming gebracht met de formulering in de richtlijn.

Onderscheid tussen personen met vergelijkbare kenmerken

Om te garanderen dat gegevens naar behoren worden verwerkt en opgeslagen, en om het risico op overlapping en verkeerde identificatie te beperken, wordt in artikel 41 bepaald welke procedure moet worden gevolgd wanneer bij het opnemen van een nieuwe signalering blijkt dat het SIS al een signalering met vergelijkbare kenmerken bevat.

Bescherming en beveiliging van gegevens

Dit voorstel verduidelijkt wie verantwoordelijk is voor de preventie van, rapportage over en reactie op incidenten die de beveiliging of de integriteit van de SIS infrastructuur en van de in het SIS opgenomen gegevens of aanvullende informatie kunnen aantasten (artikelen 10, 16 en 40).

Artikel 12 bevat bepalingen over het bijhouden en doorzoeken van logbestanden met het relaas van de signaleringen.

---

[32] COM(2016) …

Artikel 15, lid 3, is identiek aan artikel 15, lid 3, van Verordening (EG) nr. 1987/2006 en bepaalt dat de Commissie verantwoordelijk blijft voor het contractuele beheer van de communicatie-infrastructuur, met inbegrip van begrotingsuitvoeringstaken en aanschaf en vernieuwing. Deze taken zullen aan eu-LISA worden overgedragen in het kader van de tweede reeks voorstellen, die is gepland voor juni 2017.

De reeds bestaande, aan de lidstaten opgelegde eis om voorafgaand aan de opneming van een signalering de evenredigheid daarvan na te gaan, wordt bij artikel 21 uitgebreid tot besluiten over het al dan niet verlengen van de geldigheidsduur van een signalering. Nieuw in dit verband is dat de lidstaten op grond van artikel 24, lid 2, onder c), verplicht worden om onder alle omstandigheden een signalering te creëren voor personen van wie de activiteiten vallen onder de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van de Raad inzake terrorismebestrijding.

Gegevenscategorieën en gegevensverwerking

Om de eindgebruikers meer en accuratere informatie ter beschikking te stellen, zodat de gevraagde maatregel gemakkelijker en sneller kan worden uitgevoerd, en om de gesignaleerde persoon beter te kunnen identificeren, wordt voorgesteld het aantal toegestane gegevens (artikel 20) over gesignaleerde personen uit te breiden met de volgende informatie:

- of de persoon betrokken is bij activiteiten die vallen onder de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van de Raad;
- of de signalering verband houdt met een EU-burger of een andere persoon die rechten inzake vrij verkeer geniet die gelijkwaardig zijn aan die van de EU-burgers;
- of een besluit tot toegangsweigering is gebaseerd op bepalingen in artikel 24 of in artikel 27;
- het soort strafbaar feit (voor signaleringen krachtens artikel 24, lid 2);
- gegevens van het identiteits- of reisdocument van de persoon;
- kleurenkopie van het identiteits- of reisdocument van de persoon;
- foto's en gezichtsopnamen;
- vingerafdrukken en handpalmafdrukken.

De beschikbaarheid van adequate gegevens is van essentieel belang voor de accurate identificatie van personen die bij een grensdoorlaatpost worden gecontroleerd, die worden onderworpen aan een interne controle of die een verblijfsvergunning aanvragen. Een niet-accurate identificatie kan aanleiding geven tot problemen op het gebied van de grondrechten, of tot een situatie waarin geen passende follow-upmaatregelen kunnen worden genomen omdat men niet op de hoogte is van het bestaan of de inhoud van een signalering.

Met betrekking tot het achterliggende besluit zijn er vier gronden voor het verstrekken van informatie: een eerdere veroordeling als bedoeld in artikel 24, lid 2, onder a), een ernstige veiligheidsdreiging als bedoeld in artikel 24, lid 2, onder b), een inreisverbod als bedoeld in artikel 24, lid 3, en een beperkende maatregel als bedoeld in artikel 27. Om ervoor te zorgen

dat bij een treffer passende maatregelen worden genomen, moet bovendien worden opgegeven of de signalering verband houdt met een EU-burger of een persoon die rechten inzake vrij verkeer geniet die gelijkwaardig zijn aan die van de burgers van de EU. De beschikbaarheid van adequate gegevens is van essentieel belang voor de accurate identificatie van personen die bij een grensdoorlaatpost worden gecontroleerd, die worden onderworpen aan een interne controle of die een verblijfsvergunning aanvragen. Een niet-accurate identificatie kan aanleiding geven tot problemen op het gebied van de grondrechten, of tot een situatie waarin geen passende follow-upmaatregelen kunnen worden genomen omdat men niet op de hoogte is van het bestaan of de inhoud van een signalering.

De lijst van persoonsgegevens die in het SIS mogen worden opgenomen en verwerkt met het oog op de behandeling van gevallen van identiteitsmisbruik, wordt uitgebreid (artikel 42), aangezien de beschikbaarheid van meer gegevens de identificatie van het slachtoffer en de pleger van het identiteitsmisbruik vergemakkelijkt. De uitbreiding van deze bepaling brengt geen risico met zich mee, aangezien al deze gegevens slechts met de instemming van het slachtoffer van het identiteitsmisbruik mogen worden opgenomen. De bestaande lijst gegevens wordt aangevuld met:

- gezichtsopnamen;
- handpalmafdrukken;
- gegevens van identiteitsdocumenten;
- het adres van het slachtoffer;
- de naam van de vader en de moeder van het slachtoffer.

Krachtens artikel 20 moet in de signaleringen meer informatie worden opgenomen dan tot dusverre het geval was. De toegevoegde categorieën hebben onder meer betrekking op de reden voor de weigering van toegang en verblijf, en op nadere gegevens van de persoonlijke identificatiedocumenten van de betrokkenen. Dankzij deze extra informatie kan de betrokken persoon beter worden geïdentificeerd en kunnen de eindgebruikers met meer kennis van zaken een besluit nemen. Ter bescherming van de eindgebruikers die de controles uitvoeren, zal het SIS ook aangeven of de gesignaleerde persoon valt onder een van de categorieën als bedoeld in de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van de Raad inzake terrorismebestrijding[33].

In het voorstel wordt duidelijk gemaakt dat lidstaten gegevens die door een andere lidstaat zijn ingevoerd, niet naar andere nationale gegevensbestanden mogen kopiëren (artikel 37).

Bewaring

In artikel 34 wordt de termijn voor het toetsen van signaleringen vastgesteld. De maximale bewaartermijn voor signaleringen met het oog op weigering van toegang en verblijf is in overeenstemming gebracht met de mogelijke maximumduur van inreisverboden die overeenkomstig artikel 11 van Richtlijn 2008/115/EG worden uitgevaardigd. Dat betekent dat de maximale bewaartermijn vijf jaar bedraagt. De lidstaten kunnen evenwel kortere termijnen vaststellen.

---

[33] Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding (PB L 164 van 22.6.2002, blz. 3).

Wissen

Artikel 35 bepaalt onder welke voorwaarden signaleringen moeten worden gewist en brengt zodoende meer uniformiteit in de nationale procedures op dit gebied. Krachtens de bijzondere bepalingen van artikel 35 kan het personeel van de Sirene-bureaus signaleringen die niet langer nodig zijn, proactief wissen, indien geen antwoord is ontvangen van de bevoegde autoriteiten.

Rechten van betrokkenen op inzage van hun gegevens, rectificatie van onjuiste gegevens en wissing van onrechtmatig opgeslagen gegevens

De nadere bepalingen over de rechten van de betrokkenen zijn niet gewijzigd, aangezien de bestaande regels reeds een hoog niveau van bescherming waarborgen en in overeenstemming zijn met Verordening (EU) 2016/679[34] en Richtlijn 2016/680[35]. Voorts wordt in artikel 48 bepaald onder welke omstandigheden de lidstaten kunnen besluiten geen informatie aan de betrokkenen mee te delen. Een dergelijke maatregel moet gebaseerd zijn op een van de in het artikel vastgestelde redenen en dient overeenkomstig het nationale recht evenredig en noodzakelijk te zijn.

Statistieken

Om een overzicht te geven van de toegepaste rechtsmiddelen, voorziet artikel 49 in een standaard statistisch systeem voor jaarlijkse rapportage over het aantal:

- door betrokkenen ingediende verzoeken om inzage;
- verzoeken om onjuiste gegevens te rectificeren en onrechtmatig opgeslagen gegevens te wissen;
- bij rechtbanken aanhangig gemaakte zaken;
- zaken waarin de rechtbank de verzoeker in het gelijk heeft gesteld, en
- opmerkingen over zaken waarin ten aanzien van een door het signalerende land gecreëerde signalering onherroepelijke beslissingen door rechtbanken of instanties van andere lidstaten zijn vastgesteld die wederzijds zijn erkend.

Monitoring en statistieken

Artikel 54 bepaalt welke monitoringregelingen voorhanden moeten zijn om het SIS naar behoren te toetsen aan de voor het systeem vastgestelde doelstellingen. Daartoe krijgt eu-

[34] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

[35] 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 (PB L 119 van 4.5.2016, blz. 89).

LISA tot taak dagelijkse, maandelijkse en jaarlijkse statistieken te verstrekken over de manier waarop het systeem wordt gebruikt.

Krachtens artikel 54, lid 5, moet eu-LISA statistische verslagen opstellen en voorleggen aan de lidstaten, de Commissie, Europol en het Europees Grens- en kustwachtagentschap, en kan de Commissie verzoeken om aanvullende statistische verslagen en verslagen over gegevenskwaliteit betreffende de communicatie in het kader van het SIS en Sirene.

Krachtens artikel 54, lid 6, moet een centraal gegevensregister worden opgezet en beheerd, als onderdeel van het werk van eu-LISA op het gebied van monitoring van de werking van het SIS. Via dit register krijgen daartoe bevoegde personeelsleden van de lidstaten, de Commissie, Europol en het Europees Grens- en kustwachtagentschap toegang tot de in artikel 54, lid 3, bedoelde gegevens die nodig zijn voor het opstellen van de vereiste statistieken.

2016/0408 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van Verordening (EU) nr. 515/2014 en tot intrekking van Verordening (EG) nr. 1987/2006

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 77, lid 2, onder b) en d), en artikel 79, lid 2, onder c),

Gezien het voorstel van de Europese Commissie,

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

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Het Schengeninformatiesysteem (SIS) is een essentieel instrument voor de toepassing van de bepalingen van het Schengenacquis zoals dat is opgenomen in het kader van de Europese Unie. Het SIS is een van de belangrijkste compenserende maatregelen die bijdragen tot de handhaving van een hoog niveau van veiligheid in de ruimte van vrijheid, veiligheid en recht in de Europese Unie door ondersteuning te bieden bij de operationele samenwerking tussen kustwacht, politie, douane en andere rechtshandhavingsautoriteiten, voor strafzaken bevoegde gerechtelijke instanties en immigratieautoriteiten.

(2) Het SIS is ingesteld op grond van de bepalingen van titel IV van de Overeenkomst van 19 juni 1990 ter uitvoering van het te Schengen gesloten akkoord van 14 juni 1985 tussen de regeringen van de staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek, betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen[36] (de Schengenuitvoeringsovereenkomst). De ontwikkeling van het SIS van de tweede generatie (SIS II) is toevertrouwd aan de Commissie krachtens Verordening (EG) nr. 2424/2001 van de Raad[37] en Besluit 2001/886/JBZ van de Raad[38], en het SIS II is ingesteld bij Verordening (EG) nr. 1987/2006[39] en Besluit 2007/533/JBZ van de

---

36 PB L 239 van 22.9.2000, blz. 19. Overeenkomst gewijzigd bij Verordening (EG) nr. 1160/2005 van het Europees Parlement en de Raad (PB L 191 van 22.7.2005, blz. 18).

37 PB L 328 van 13.12.2001, blz. 4.

38 Besluit 2001/886/JBZ van de Raad van 6 december 2001 betreffende de ontwikkeling van een Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 328 van 13.12.2001, blz. 1).

39 Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 381 van 28.12.2006, blz. 4).

Raad[40]. Het SIS II heeft het bij de Schengenuitvoeringsovereenkomst ingestelde SIS vervangen.

(3) Drie jaar na de ingebruikneming van het SIS II heeft de Commissie het systeem geëvalueerd overeenkomstig artikel 24, lid 5, artikel 43, lid 5, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006 en artikel 59 en artikel 66, lid 5, van Besluit 2007/533/JBZ. Het evaluatieverslag en het bijbehorende werkdocument van de diensten van de Commissie zijn op 21 december 2016 aangenomen[41]. De aanbevelingen die in die documenten worden gedaan, moeten adequaat tot uiting komen in deze verordening.

(4) Deze verordening vormt de noodzakelijke rechtsgrondslag voor het SIS met betrekking tot aangelegenheden die vallen onder het toepassingsgebied van titel V, hoofdstuk 2, van het Verdrag betreffende de werking van de Europese Unie. Verordening (EU) 2018/... van het Europees Parlement en de Raad betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken[42] vormt de noodzakelijke rechtsgrondslag voor het SIS met betrekking tot aangelegenheden die vallen onder het toepassingsgebied van titel V, hoofdstukken 4 en 5, van het Verdrag betreffende de werking van de Europese Unie.

(5) Het feit dat afzonderlijke instrumenten zijn vastgesteld als rechtsgrondslag voor het SIS doet geen afbreuk aan het beginsel dat het SIS één integraal informatiesysteem vormt, dat als zodanig moet functioneren. Een aantal bepalingen van deze instrumenten dient bijgevolg identiek te zijn.

(6) De doelstellingen, de technische architectuur en de financiering van het SIS moeten worden omschreven, er moeten voorschriften betreffende het volledige werkingstraject en het gebruik van het systeem worden vastgesteld, en de verantwoordelijkheden dienen te worden gedefinieerd, evenals de in het systeem op te nemen categorieën gegevens, het doel van en de criteria voor de opneming van de gegevens, de autoriteiten die toegang hebben tot de gegevens, het gebruik van biometrische identificatiemiddelen en verdere voorschriften inzake gegevensverwerking.

(7) Het SIS omvat een centraal systeem (het centrale SIS) en nationale systemen met een volledige of gedeeltelijke kopie van de SIS-databank. Aangezien het SIS het belangrijkste instrument voor de uitwisseling van informatie in Europa is, moet het systeem zowel op centraal als op nationaal niveau ononderbroken operationeel zijn. Daarom moet elke lidstaat een volledige of gedeeltelijke kopie van de SIS-databank en een back-up daarvan opzetten.

(8) Er moet een handboek worden bijgehouden met gedetailleerde voorschriften voor de uitwisseling van bepaalde aanvullende informatie over de in de signalering gevraagde

---

40 Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 205 van 7.8.2007, blz. 63).

41 Verslag aan het Europees Parlement en aan de Raad over de evaluatie van het Schengeninformatiesysteem van de tweede generatie (SIS II) in overeenstemming met artikel 24, lid 5, artikel 43, lid 3, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006 en artikel 59, lid 3, en artikel 66, lid 5, van Besluit 2007/533/JBZ, en een bijbehorend werkdocument van de diensten van de Commissie.

42 Verordening (EU) 2018/...

maatregel. De nationale autoriteiten van elke lidstaat (de Sirene-bureaus) moeten zorgen voor de uitwisseling van deze informatie.

(9) Met het oog op de efficiënte uitwisseling van aanvullende informatie over de in de signalering gevraagde maatregel, dient de werking van de Sirene-bureaus te worden versterkt door nadere voorschriften vast te stellen inzake de beschikbare middelen, de opleiding van gebruikers en de tijd om te reageren op verzoeken van andere Sirene-bureaus.

(10) Het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht[43] (het Agentschap) wordt belast met het operationele beheer van de centrale componenten van het SIS. Om het Agentschap in staat te stellen de financiële en personele middelen in te zetten die nodig zijn voor een alomvattend operationeel beheer van het centrale SIS, moeten de taken van het Agentschap nauwkeurig worden omschreven, met name wat de technische aspecten van de uitwisseling van aanvullende informatie betreft.

(11) Onverminderd de verantwoordelijkheid van de lidstaten voor de accuraatheid van de in het SIS opgenomen gegevens, dient het Agentschap de verantwoordelijkheid te krijgen om de gegevenskwaliteit te verbeteren door een centraal instrument voor het monitoren van de gegevenskwaliteit in te voeren, en om op gezette tijden verslag uit te brengen aan de lidstaten.

(12) Om het gebruik van het SIS voor het analyseren van trends in migratiedruk en grensbeheer beter te kunnen monitoren, moet het Agentschap in staat zijn om, zonder gevaar voor de integriteit van de gegevens, een geavanceerde capaciteit te ontwikkelen voor statistische rapportage aan de lidstaten, de Commissie, Europol en het Europees Grens- en kustwachtagentschap. Hiertoe moet een centraal statistisch register worden opgezet. De statistieken die worden opgesteld, mogen geen persoonsgegevens bevatten.

(13) Er dienen gegevenscategorieën aan het SIS te worden toegevoegd zodat de eindgebruikers met kennis van zaken en zonder tijdverlies een besluit kunnen nemen op basis van een signalering. Daartoe is het van belang dat signaleringen met het oog op weigering van toegang en verblijf informatie bevatten over de beslissing die ten grondslag ligt aan de signalering. Om de identificatie te vergemakkelijken en meervoudige identiteiten op te sporen, moet de signalering bovendien een verwijzing naar het persoonlijke identificatiedocument of -nummer bevatten en, indien beschikbaar, een kopie van dat document.

(14) Voor een bevraging gebruikte gegevens mogen niet in het SIS worden opgeslagen, tenzij het gaat om logbestanden om de rechtmatigheid van de bevraging te verifiëren, de rechtmatigheid van de gegevensverwerking te monitoren, interne monitoring uit te voeren, de goede werking van N.SIS te waarborgen en de integriteit en beveiliging van de gegevens te garanderen.

(15) Het SIS moet de verwerking van biometrische gegevens mogelijk maken om de betrouwbare identificatie van de desbetreffende personen te vergemakkelijken. In

---

[43] Opgericht bij Verordening (EU) nr. 1077/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (PB L 286 van 1.11.2011, blz. 1).

hetzelfde verband moet het SIS ook de mogelijkheid bieden om gegevens van personen van wie de identiteit is misbruikt, te verwerken (om problemen als gevolg van verkeerde identificatie te voorkomen), mits daarbij passende waarborgen worden geboden, met name de instemming van de betrokken persoon en een strikte beperking van de doeleinden waarvoor dergelijke gegevens rechtmatig kunnen worden verwerkt.

(16) De lidstaten moeten het voor eindgebruikers technisch mogelijk maken om telkens wanneer zij een nationale politie- of immigratiedatabank mogen bevragen, een parallelle bevraging uit te voeren in het SIS overeenkomstig artikel 4 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad[44]. Dit moet ervoor zorgen dat het SIS zijn functie als voornaamste compenserende maatregel in het gebied zonder binnengrenstoezicht kan vervullen en dat de grensoverschrijdende dimensie van de criminaliteit en de mobiliteit van criminelen beter wordt aangepakt.

(17) Er moet worden vastgesteld onder welke voorwaarden dactyloscopische gegevens en gezichtsopnamen mogen worden gebruikt voor identificatiedoeleinden. Het gebruik van gezichtsopnamen voor identificatiedoeleinden in het SIS moet mede borg staan voor consistentie in grenstoezichtprocedures waar voor de identificatie en de verificatie van de identiteit dactyloscopische gegevens en gezichtsopnamen moeten worden gebruikt. In geval van twijfel over de identiteit van een persoon moet bevraging aan de hand van dactyloscopische gegevens verplicht zijn. Het gebruik van gezichtsopnamen voor identificatiedoeleinden is alleen toegestaan in het kader van regulier grenstoezicht bij zelfbedieningsloketten en e-gates.

(18) Het toetsen van op een plaats delict aangetroffen vingerafdrukken aan de in het SIS opgeslagen dactyloscopische gegevens moet worden toegestaan indien met een hoge mate van waarschijnlijkheid kan worden vastgesteld dat de afdrukken die van de dader van het terroristische misdrijf of andere ernstige strafbare feit zijn. Onder ernstige strafbare feiten worden de strafbare feiten verstaan in de zin van Kaderbesluit 2002/584/JBZ van de Raad[45], en onder terroristische misdrijven de krachtens het nationale recht strafbare feiten in de zin van Kaderbesluit 2002/475/JBZ van de Raad[46].

(19) Het moet voor de lidstaten mogelijk zijn signaleringen in het SIS te koppelen. Het koppelen van twee of meer signaleringen door een lidstaat mag geen gevolgen hebben voor de gevraagde maatregel, de bewaartermijn voor de signaleringen of het recht op toegang tot de signaleringen.

(20) Er kan een hoger niveau van doeltreffendheid, harmonisatie en samenhang worden bereikt door te eisen dat alle inreisverboden die de bevoegde autoriteiten van de

---

44 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).

45 Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002 betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten (PB L 190 van 18.7.2002, blz. 1).

46 Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding (PB L 164 van 22.6.2002, blz. 3).

lidstaten overeenkomstig Richtlijn 2008/115/EG[47] hebben uitgevaardigd, in het SIS worden opgenomen, en door gemeenschappelijke regels vast te stellen voor het opnemen van een dergelijke signalering na de terugkeer van een illegaal verblijvende onderdaan van een derde land. De lidstaten moeten alle nodige maatregelen nemen om ervoor te zorgen dat het tijdstip waarop de onderdaan van het derde land het Schengengebied verlaat, volledig samenvalt met het tijdstip waarop de signalering in het SIS wordt geactiveerd. Op die manier moet worden gewaarborgd dat de inreisverboden bij de doorlaatposten aan de buitengrenzen doeltreffend worden uitgevoerd en afdoende wordt voorkomen dat de betrokken personen het Schengengebied terug binnenkomen.

(21) Er moeten bindende regels worden vastgesteld voor overleg tussen nationale autoriteiten wanneer een onderdaan van een derde land in het bezit is of kan komen van een in een bepaalde lidstaat afgegeven geldige verblijfstitel of andere machtiging tot verblijf, en een andere lidstaat voornemens is deze onderdaan van een derde land te signaleren met het oog op weigering van toegang en verblijf, of zulks reeds heeft gedaan. Dergelijke situaties leiden tot grote onzekerheid bij grenswachters en politie- en immigratieautoriteiten. Daarom dient een bindende termijn voor spoedig overleg te worden bepaald waarbinnen een definitief resultaat moet worden bereikt, teneinde te voorkomen dat personen die een dreiging vormen, het Schengengebied binnenkomen.

(22) Deze verordening laat de toepassing van Richtlijn 2004/38/EG[48] onverlet.

(23) Signaleringen mogen niet langer in het SIS worden bewaard dan nodig is voor het met de signalering nagestreefde doel. Om de administratieve lasten voor de autoriteiten die betrokken zijn bij de verwerking van persoonsgegevens voor andere doeleinden, te beperken, moet de maximale bewaartermijn voor signaleringen met het oog op weigering van toegang en verblijf in overeenstemming worden gebracht met de mogelijke maximumduur van inreisverboden die overeenkomstig Richtlijn 2008/115/EG worden uitgevaardigd. Derhalve moet de bewaartermijn voor signaleringen van personen worden vastgesteld op maximaal vijf jaar. In de regel moeten signaleringen van personen na vijf jaar automatisch worden gewist in het SIS. Besluiten om signaleringen van personen te bewaren, dienen gebaseerd te zijn op een uitvoerige individuele beoordeling. De lidstaten moeten signaleringen van personen binnen de vastgestelde periode controleren en statistieken bijhouden van het aantal signaleringen van personen waarvan de bewaartermijn is verlengd.

(24) Voor het opnemen van de datum waarop een SIS-signalering verstrijkt en het verlengen van de geldigheidsduur van een SIS-signalering moet de evenredigheidsvereiste in acht worden genomen, in de zin dat moet worden onderzocht of een concreet geval gepast, relevant en belangrijk genoeg is om opneming van een signalering in het SIS te rechtvaardigen. In het geval van strafbare feiten in de zin van de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van de

---

47 Richtlijn 2008/115/EG van het Europees Parlement en de Raad van 16 december 2008 over gemeenschappelijke normen en procedures in de lidstaten voor de terugkeer van onderdanen van derde landen die illegaal op hun grondgebied verblijven (PB L 348 van 24.12.2008, blz. 98).

48 Richtlijn 2004/38/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende het recht van vrij verkeer en verblijf op het grondgebied van de lidstaten voor de burgers van de Unie en hun familieleden (PB L 158 van 30.4.2004, blz. 77).

Raad[49] moet voor de betrokken onderdanen van derde landen altijd een signalering van weigering met het oog op toegang en verblijf worden gecreëerd, rekening houdend met het hoge dreigingsniveau en de algemene negatieve gevolgen van dergelijke activiteiten.

(25) De integriteit van de SIS-gegevens is van essentieel belang. Daarom moeten voldoende waarborgen worden geboden ten aanzien van de beveiliging van het volledige verwerkingstraject, zowel op centraal als op nationaal niveau. De instanties die betrokken zijn bij de gegevensverwerking, moeten zich houden aan de beveiligingseisen die in deze verordening worden vastgesteld, en moeten een uniforme procedure voor het melden van incidenten volgen.

(26) De overeenkomstig deze verordening in het SIS verwerkte gegevens mogen niet worden doorgegeven aan of ter beschikking worden gesteld van derde landen of internationale organisaties.

(27) Met het oog op een efficiëntere besluitvorming van de immigratieautoriteiten over het recht van onderdanen van derde landen om het grondgebied van de lidstaten binnen te komen en er te verblijven, alsook over de terugkeer van illegaal verblijvende onderdanen van derde landen, dient aan deze autoriteiten toegang tot het SIS te worden verleend in het kader van deze verordening.

(28) Wanneer autoriteiten van de lidstaten in het kader van deze verordening persoonsgegevens verwerken, is Verordening (EU) 2016/679[50] van toepassing, tenzij Richtlijn (EU) 2016/680[51] van toepassing is. Wanneer de instellingen en organen van de Unie bij het uitvoeren van hun taken in het kader van deze verordening persoonsgegevens verwerken, is Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van toepassing[52]. De bepalingen van Richtlijn (EU) 2016/680, Verordening (EU) 2016/679 en Verordening (EG) nr. 45/2001 moeten in deze verordening waar nodig nader worden gespecificeerd. Met betrekking tot de verwerking van persoonsgegevens door Europol is Verordening (EU) 2016/794 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving[53] (de Europol-verordening) van toepassing.

---

49 Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding (PB L 164 van 22.6.2002, blz. 3).

50 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

51 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 (PB L 119 van 4.5.2016, blz. 89).

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

53 Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad (PB L 135 van 25.5.2016, blz. 53).

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

(30) De lidstaten en het Agentschap moeten beveiligingsplannen bijhouden om de uitvoering van hun verplichtingen op het gebied van beveiliging te vereenvoudigen, en met elkaar samenwerken om beveiligingsvraagstukken vanuit een gemeenschappelijke invalshoek te benaderen.

(31) De nationale onafhankelijke toezichthoudende autoriteiten moeten monitoren of de lidstaten de persoonsgegevens in het kader van deze verordening rechtmatig verwerken. Er moeten bepalingen worden vastgesteld inzake de rechten van betrokkenen op inzage van hun in het SIS opgeslagen persoonsgegevens en op rectificatie en wissing van die gegevens, alsmede inzake de rechtsmiddelen voor de nationale gerechten en de wederzijdse erkenning van besluiten in dat verband. De lidstaten moeten hieromtrent jaarlijkse statistieken verstrekken.

(32) De toezichthoudende autoriteiten moeten erop toezien dat ten minste om de vier jaar een audit van de gegevensverwerking in hun N.SIS wordt uitgevoerd overeenkomstig internationale auditnormen. De audit moet worden uitgevoerd door de toezichthoudende autoriteiten of moet door de nationale toezichthoudende autoriteiten rechtstreeks worden uitbesteed aan een onafhankelijke auditor op het gebied van gegevensbescherming. De onafhankelijke auditor dient zijn werkzaamheden uit te voeren onder de controle en de verantwoordelijkheid van de nationale toezichthoudende autoriteiten, die derhalve zelf opdracht voor de audit moeten geven, een duidelijk omschreven doel, reikwijdte en methode voor de audit moeten vaststellen en met betrekking tot de audit en de eindresultaten richtsnoeren moeten uitvaardigen en toezicht moeten uitoefenen.

(33) Verordening (EU) 2016/794 (de Europol-verordening) bepaalt dat Europol ondersteuning en versterking biedt voor het optreden van de bevoegde autoriteiten van de lidstaten en hun onderlinge samenwerking bij de bestrijding van terrorisme en andere vormen van zware criminaliteit, en in dat verband analyses en dreigingsevaluaties verstrekt. Om het werk van Europol, met name in het kader van het Europees Centrum tegen migrantensmokkel, te vergemakkelijken, dient Europol toegang te krijgen tot de in deze verordening bedoelde signaleringscategorieën. Het Europees Centrum tegen migrantensmokkel speelt een belangrijke strategische rol in de bestrijding van activiteiten die irreguliere migratie faciliteren, en moet toegang krijgen tot signaleringen van personen wie de toegang tot en het verblijf op het grondgebied van een lidstaat is geweigerd op strafrechtelijke gronden of vanwege niet-naleving van de voorwaarden voor toegang en verblijf.

(34) Om de kloof op het gebied van informatie-uitwisseling over terrorisme en met name over buitenlandse terroristische strijders – in welk geval het monitoren van bewegingen van essentieel belang is — te overbruggen, moeten de lidstaten met Europol informatie over met terrorisme verband houdende activiteiten, treffers en gerelateerde gegevens uitwisselen en parallel daarmee een signalering opnemen in het SIS. Dit moet het Europees Centrum voor terrorismebestrijding van Europol in staat stellen te verifiëren of in de databanken van Europol aanvullende contextuele informatie beschikbaar is, en hoogwaardige analyses op te stellen die bijdragen aan het

ontwrichten van terroristische netwerken en, waar mogelijk, aan het voorkomen van aanslagen.

(35) Met het oog op een optimaal gebruik van het SIS moeten duidelijke regels worden vastgesteld voor het verwerken en downloaden van SIS-gegevens door Europol, met dien verstande dat de bescherming van de gegevens daarbij wordt gewaarborgd overeenkomstig deze verordening en Verordening (EU) 2016/794. Wanneer bij bevraging van het SIS door Europol blijkt dat een lidstaat een signalering heeft opgenomen, mag Europol de gevraagde maatregel niet uitvoeren. Europol dient in zulke gevallen de betrokken lidstaat op de hoogte te brengen zodat deze de follow-up van de zaak op zich kan nemen.

(36) In het kader van Verordening (EU) 2016/1624 van het Europees Parlement en de Raad[54] moet de ontvangende lidstaat leden van de Europese grens- en kustwachtteams en door het Europees Grens- en kustwachtagentschap ingezette teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken, toestaan Europese databanken te raadplegen wanneer dat noodzakelijk is voor de verwezenlijking van de operationele doelstellingen als vastgesteld in het operationele plan inzake grenscontroles, grensbewaking en terugkeer. Andere ter zake relevante agentschappen van de Unie, meer bepaald het Europees Ondersteuningsbureau voor asielzaken en Europol, kunnen deskundigen aan de ondersteuningsteams voor migratiebeheer toevoegen die geen personeelslid van deze agentschappen van de Unie zijn. Het inzetten van de Europese grens- en kustwachtteams, de teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken en de ondersteuningsteams voor migratiebeheer heeft tot doel technische en operationele versterking te bieden aan lidstaten die daarom verzoeken, met name aan lidstaten die worden geconfronteerd met onevenredig grote uitdagingen op het gebied van migratie. De Europese grens- en kustwachtteams, de teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken en de ondersteuningsteams voor migratiebeheer hebben voor de uitvoering van hun taken toegang nodig tot het SIS via een technische interface van het Europees Grens- en kustwachtagentschap die wordt aangesloten op het centrale SIS. Wanneer bij bevraging van het SIS door het team of de teams van personeelsleden blijkt dat een lidstaat een signalering heeft uitgevaardigd, voert het betrokken team- of personeelslid de gevraagde maatregel alleen uit indien de ontvangende lidstaat daartoe toestemming heeft verleend. In zulke gevallen moeten de betrokken lidstaten op de hoogte worden gebracht met het oog op verdere follow-up van de zaak.

(37) Krachtens Verordening (EU) 2016/1624 moet het Europees Grens- en kustwachtagentschap risicoanalyses opstellen. Deze risicoanalyses moeten alle aspecten bestrijken die relevant zijn voor het Europese geïntegreerde grensbeheer, met name dreigingen die de werking of de veiligheid van de buitengrenzen kunnen aantasten. Signaleringen die overeenkomstig deze verordening in het SIS worden ingevoerd, met name met het oog op weigering van toegang en verblijf, bevatten relevante informatie voor het beoordelen van mogelijke dreigingen voor de buitengrenzen en moeten derhalve beschikbaar zijn ten behoeve van risicoanalyses die

---

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

door het Europees Grens- en kustwachtagentschap moeten worden opgesteld. Het Europees Grens- en kustwachtagentschap heeft voor de uitvoering van zijn taken op het gebied van risicoanalyses toegang nodig tot het SIS. Overeenkomstig het voorstel van de Commissie voor een verordening van het Europees Parlement en de Raad tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS)[55] moet de centrale ETIAS-eenheid van het Europees Grens- en kustwachtagentschap bovendien via het ETIAS verificaties in het SIS verrichten om de reisautorisatieaanvragen te beoordelen en hiertoe onder meer na te gaan of de betrokken onderdaan van een derde land die een reisautorisatie aanvraagt, in het SIS is gesignaleerd. Met het oog daarop moet de in het Europees Grens- en kustwachtagentschap ingebedde centrale ETIAS-eenheid, voor zover dat voor de uitvoering van haar opdracht vereist is, toegang hebben tot het SIS, meer bepaald tot alle categorieën signaleringen van onderdanen van derde landen te wier aanzien een signalering met het oog op weigering van toegang en verblijf is opgenomen of te wier aanzien een beperkende maatregel is genomen om de toegang tot of de doorreis via het grondgebied van de lidstaten te beletten.

(38) Bepaalde aspecten van het SIS kunnen vanwege hun technische aard, hun gedetailleerdheid en de noodzaak van regelmatige bijwerking niet uitputtend worden geregeld in deze verordening. Het gaat dan bijvoorbeeld over technische voorschriften inzake het opnemen, bijwerken, wissen en opzoeken van gegevens, gegevenskwaliteit en opzoekregels inzake biometrische identificatiemiddelen, regels inzake compatibiliteit en prioriteit van signaleringen, het toevoegen van markeringen (flags), het koppelen van signaleringen, het bepalen van de datum waarop signaleringen binnen de maximumtermijn verstrijken en de uitwisseling van aanvullende informatie. Met betrekking tot deze aspecten moeten uitvoeringsbevoegdheden aan de Commissie worden toegekend. In de technische voorschriften moet aandacht worden besteed aan de vlotte werking van de nationale applicaties.

(39) Teneinde eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend. Deze bevoegdheden moeten worden uitgeoefend overeenkomstig Verordening (EU) nr. 182/2011[56]. Voor de vaststelling van uitvoeringsmaatregelen in het kader van deze verordening en in het kader van Verordening (EU) 2018/xxx (politiële en justitiële samenwerking) dient dezelfde procedure te worden gevolgd.

(40) Met het oog op transparantie moet het Agentschap om de twee jaar een verslag opstellen over de technische werking van het centrale SIS en de communicatie-infrastructuur, met inbegrip van de beveiliging ervan, alsmede over de uitwisseling van aanvullende informatie. Om de vier jaar moet de Commissie een algemene evaluatie opstellen.

(41) Aangezien de doelstellingen van deze verordening, namelijk de instelling en regulering van een gemeenschappelijk informatiesysteem en de uitwisseling van aanvullende informatie, door de aard ervan niet voldoende door de lidstaten kunnen worden verwezenlijkt en derhalve beter door de Unie kunnen worden verwezenlijkt,

---

55 COM(2016) 731 final.

56 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).

kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze doelstellingen te verwezenlijken.

(42) Deze verordening eerbiedigt de grondrechten en neemt de beginselen in acht die met name in het Handvest van de grondrechten van de Europese Unie zijn neergelegd. Deze verordening is met name gericht op het waarborgen van een veilige omgeving voor iedereen die op het grondgebied van de Europese Unie verblijft, en de bescherming van irreguliere migranten tegen uitbuiting en mensenhandel, door identificatie van deze personen, met volledige inachtneming van de bescherming van persoonsgegevens, mogelijk te maken.

(43) Overeenkomstig de artikelen 1 en 2 van het aan het Verdrag betreffende de Europese Unie en aan het VWEU gehechte Protocol nr. 22 betreffende de positie van Denemarken, neemt Denemarken niet deel aan de vaststelling van deze verordening; deze is bijgevolg niet bindend voor, noch van toepassing op deze lidstaat. Aangezien deze verordening voortbouwt op het Schengenacquis, beslist Denemarken overeenkomstig artikel 4 van dit protocol binnen een termijn van zes maanden nadat de Raad deze verordening heeft vastgesteld, of het deze in zijn nationale recht zal omzetten.

(44) Deze verordening houdt een ontwikkeling in van bepalingen van het Schengenacquis waaraan het Verenigd Koninkrijk niet deelneemt, overeenkomstig Besluit 2000/365/EG van de Raad[57]; het Verenigd Koninkrijk neemt derhalve niet deel aan de aanneming van deze verordening, die niet bindend is voor, noch van toepassing is op deze lidstaat.

(45) Deze verordening houdt een ontwikkeling in van de bepalingen van het Schengenacquis waaraan Ierland niet deelneemt, overeenkomstig Besluit 2002/192/EG van de Raad[58]; Ierland neemt derhalve niet deel aan de aanneming van deze verordening, die niet bindend is voor, noch van toepassing is op deze lidstaat.

(46) Wat IJsland en Noorwegen betreft, houdt deze verordening een ontwikkeling in van bepalingen van het Schengenacquis in de zin van de overeenkomst tussen de Raad van de Europese Unie, de Republiek IJsland en het Koninkrijk Noorwegen inzake de wijze waarop IJsland en Noorwegen worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis[59] die vallen onder het gebied dat is bedoeld in artikel 1, onder G, van Besluit 1999/437/EG[60] inzake bepaalde toepassingsbepalingen van die overeenkomst.

(47) Wat Zwitserland betreft, houdt deze verordening een ontwikkeling in van de bepalingen van het Schengenacquis in de zin van de Overeenkomst die is ondertekend door de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis die vallen onder het gebied dat is bedoeld in

---

57 PB L 131 van 1.6.2000, blz. 43.
58 PB L 64 van 7.3.2002, blz. 20.
59 PB L 176 van 10.7.1999, blz. 36.
60 PB L 176 van 10.7.1999, blz. 31.

artikel 1, punt G, van Besluit 1999/437/EG, juncto artikel 4, lid 1, van de Besluiten 2004/849/EG[61] en 2004/860/EG[62].

(48) Wat Liechtenstein betreft, houdt deze verordening een ontwikkeling in van de bepalingen van het Schengenacquis in de zin van het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis[63], die vallen onder het gebied bedoeld in artikel 1, onder A, van Besluit 1999/437/EG van de Raad, juncto artikel 3 van Besluit 2011/349/EU van de Raad[64] en artikel 3 van Besluit 2011/350/EU van de Raad[65].

(49) Wat Bulgarije en Roemenië betreft, vormt deze verordening een rechtsbesluit dat op het Schengenacquis voortbouwt, of anderszins daaraan is gerelateerd in de zin van artikel 4, lid 2, van de Toetredingsakte van 2005, en moet deze verordening worden gelezen in samenhang met Besluit 2010/365/EU van de Raad betreffende de toepassing van de bepalingen van het Schengenacquis die betrekking hebben op het Schengeninformatiesysteem in de Republiek Bulgarije en Roemenië[66].

(50) Wat Cyprus en Kroatië betreft, vormt deze verordening een rechtsbesluit dat op het Schengenacquis voortbouwt, of anderszins daaraan is gerelateerd in de zin van respectievelijk artikel 3, lid 2, van de Toetredingsakte van 2003 en artikel 4, lid 2, van de Toetredingsakte van 2011.

(51) De geraamde kosten voor het upgraden van de nationale SIS-systemen en het implementeren van de nieuwe functies overeenkomstig deze verordening zijn lager

---

61 Besluit 2004/849/EG van de Raad van 25 oktober 2004 betreffende de ondertekening, namens de Europese Gemeenschap, en de voorlopige toepassing van enkele bepalingen van de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis (PB L 368 van 15.12.2004, blz. 26).

62 Besluit 2004/860/EG van de Raad van 25 oktober 2004 betreffende de ondertekening, namens de Europese Gemeenschap, en de voorlopige toepassing van enkele bepalingen van de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis (PB L 370 van 17.12.2004, blz. 78).

63 PB L 160 van 18.6.2011, blz. 21.

64 Besluit 2011/349/EU van de Raad van 7 maart 2011 betreffende de sluiting namens de Europese Unie van het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis, met name betreffende de justitiële samenwerking in strafzaken en de politiële samenwerking (PB L 160 van 18.6.2011, blz. 1).

65 Besluit 2011/350/EU van de Raad van 7 maart 2011 betreffende de sluiting namens de Europese Unie van het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis betreffende de afschaffing van controles aan de binnengrenzen en het verkeer van personen (PB L 160 van 18.6.2011, blz. 19).

66 PB L 166 van 1.7.2010, blz. 17.

dan het saldo van de begroting die in Verordening (EU) nr. 515/2014 van het Europees Parlement en de Raad[67] is uitgetrokken voor slimme grenzen. Overeenkomstig artikel 5, lid 5, onder b), van Verordening (EU) nr. 515/2014 dient het bedrag dat thans voor de ontwikkeling van IT-systemen ter beheersing van de migratiestromen over de buitengrenzen is toegewezen, op grond van deze verordening te worden herbestemd.

(52) Verordening (EG) nr. 1987/2006 moet derhalve worden ingetrokken.

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

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

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1
Algemene doelstelling van het SIS

Het SIS heeft tot doel met behulp van de via dit systeem verstrekte informatie een hoog niveau van veiligheid te garanderen in de ruimte van vrijheid, veiligheid en recht in de Europese Unie, onder meer door handhaving van de openbare orde en veiligheid en vrijwaring van de veiligheid op het grondgebied van de lidstaten, en heeft eveneens tot doel de bepalingen van het derde deel, titel V, hoofdstuk 2, van het Verdrag betreffende de werking van de Europese Unie inzake het verkeer van personen op het grondgebied van de lidstaten toe te passen.

Artikel 2
Toepassingsgebied

1. In deze verordening worden de voorwaarden en procedures vastgesteld voor het opnemen en verwerken van signaleringen in verband met onderdanen van derde landen in het SIS, en voor het uitwisselen van aanvullende informatie en extra gegevens met het oog op weigering van toegang tot en verblijf op het grondgebied van de lidstaten.

2. In deze verordening worden ook bepalingen vastgesteld betreffende de technische architectuur van het SIS, betreffende de verantwoordelijkheden van de lidstaten en van het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, en betreffende algemene gegevensverwerking, de rechten van de betrokken personen en aansprakelijkheid.

Artikel 3
Definities

1. Voor de toepassing van deze verordening wordt verstaan onder:

   (a) "signalering": een in het SIS opgenomen reeks gegevens, inclusief biometrische identificatiemiddelen als bedoeld in artikel 22, aan de hand waarvan de bevoegde autoriteiten een persoon kunnen identificeren met het oog op het uitvoeren van een specifieke maatregel;

   (b) "aanvullende informatie": andere informatie dan de in het SIS opgeslagen signaleringsgegevens, die gerelateerd is aan SIS-signaleringen en die moet worden uitgewisseld:

      (1) om de lidstaten in staat te stellen onderling overleg te plegen of elkaar inlichtingen te verstrekken bij de opneming van een signalering;

(2) na een treffer zodat de passende maatregel kan worden uitgevoerd;

(3) indien de gevraagde maatregel niet kan worden uitgevoerd;

(4) inzake de kwaliteit van de SIS-gegevens;

(5) inzake de compatibiliteit en de prioriteit van signaleringen;

(6) inzake het recht op toegang;

(c) "extra gegevens": de in het SIS opgeslagen en aan SIS-signaleringen gerelateerde gegevens die onmiddellijk ter beschikking van de bevoegde autoriteiten moeten staan wanneer personen over wie gegevens in het SIS zijn opgenomen, worden gelokaliseerd als gevolg van bevragingen van het SIS;

(d) "onderdaan van een derde land": eenieder die geen burger van de Unie in de zin van artikel 20 VWEU is, met uitzondering van personen die krachtens overeenkomsten tussen de Unie of de Unie en haar lidstaten, enerzijds, en derde landen, anderzijds, rechten van vrij verkeer genieten die gelijkwaardig zijn aan de rechten van burgers van de Unie;

(e) "persoonsgegevens": iedere vorm van informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene);

(f) "identificeerbare natuurlijke persoon": een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

(g) "verwerking van persoonsgegevens": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen in logbestanden, ordenen, structureren, opslaan, veranderen of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzenden, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, beperken van de verwerking, wissen of vernietigen van gegevens;

(h) "treffer": van een treffer in het SIS is sprake wanneer:

(1) een gebruiker het systeem bevraagt,

(2) bij de bevraging blijkt dat een andere lidstaat een signalering in het SIS heeft opgenomen,

(3) de gegevens betreffende de signalering in het SIS overeenstemmen met de zoekgegevens, en

(4) naar aanleiding van het voorgaande een verdere maatregel wordt gevraagd;

(i) "signalerende lidstaat": de lidstaat die de signalering in het SIS heeft opgenomen;

(j) "uitvoerende lidstaat": de lidstaat die de gevraagde maatregel uitvoert naar aanleiding van een treffer;

(k) "eindgebruikers": bevoegde autoriteiten die CS-SIS, N.SIS of een technische kopie daarvan rechtstreeks bevragen;

(l) "terugkeer": terugkeer als gedefinieerd in artikel 3, punt 3, van Richtlijn 2008/115/EG;

(m) "inreisverbod": inreisverbod als gedefinieerd in artikel 3, punt 6, van Richtlijn 2008/115/EG;

(n) "dactyloscopische gegevens": gegevens over vingerafdrukken en handpalmafdrukken, die vanwege hun uniciteit en de referentiepunten die zij bevatten, accurate en definitieve vergelijkingen mogelijk maken ten aanzien van de identiteit van een persoon;

(o) "ernstige strafbare feiten": feiten als bedoeld in artikel 2, leden 1 en 2, van Kaderbesluit 2002/584/JBZ van 13 juni 2002[68];

(p) "terroristische misdrijven": overeenkomstig het nationale recht strafbare feiten als bedoeld in de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van 13 juni 2002[69].

Artikel 4
Technische architectuur en werkwijze van het SIS

1. Het SIS bestaat uit:

(a) een centraal systeem (het centrale SIS) bestaande uit:

– een technisch ondersteunende functie (CS-SIS) die een databank, de "SIS-databank", bevat;

– een uniforme nationale interface (NI-SIS);

(b) een nationaal systeem (N.SIS) in elk van de lidstaten, bestaande uit de nationale datasystemen die in verbinding staan met het centrale SIS. Een N.SIS bevat een gegevensbestand (nationale kopie) met een volledige of gedeeltelijke kopie van de SIS-databank en een N.SIS-back-up. N.SIS en de back-up daarvan kunnen tegelijkertijd worden gebruikt om een ononderbroken beschikbaarheid voor de eindgebruikers te waarborgen;

---

68 Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002 betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten (PB L 190 van 18.7.2002, blz. 1).

69 Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding (PB L 164 van 22.6.2002, blz. 3).

(c) een communicatie-infrastructuur tussen CS-SIS en NI-SIS (communicatie-infrastructuur) waarmee een versleuteld virtueel netwerk tot stand wordt gebracht dat specifiek bestemd is voor SIS-gegevens en voor de uitwisseling van gegevens tussen de Sirene-bureaus, als bedoeld in artikel 7, lid 2.

2. SIS-gegevens worden opgenomen, bijgewerkt, gewist en opgezocht via de verschillende N.SIS-systemen. Er is een gedeeltelijke of volledige nationale kopie beschikbaar om op het grondgebied van elk van de lidstaten die een dergelijke kopie gebruiken, geautomatiseerde bevraging mogelijk te maken. De gedeeltelijke nationale kopie bevat ten minste de gegevens als bedoeld in artikel 20, lid 2, onder a) tot en met v), van deze verordening. De N.SIS-gegevensbestanden van andere lidstaten kunnen niet worden bevraagd.

3. CS-SIS zorgt voor technische toezichts- en beheersfuncties en de CS-SIS-back-up kan alle functies van het belangrijkste CS-SIS overnemen wanneer dit uitvalt. CS-SIS en de back-up ervan bevinden zich op twee technische locaties van het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, dat is opgericht bij Verordening (EU) nr. 1077/2011[70] (het Agentschap). CS-SIS en de back-up ervan kunnen een extra kopie van de SIS-databank bevatten en kunnen gelijktijdig voor operationele doeleinden worden gebruikt, op voorwaarde dat elk van beide systemen afzonderlijk in staat is alle verrichtingen met betrekking tot SIS-signaleringen te verwerken.

4. CS-SIS levert de nodige diensten voor het opnemen en verwerken van SIS-gegevens, inclusief voor bevragingen van de SIS-databank. CS-SIS zorgt voor:

(a) de online bijwerking van de nationale kopieën;

(b) de synchronisatie en de samenhang tussen de nationale kopieën en de SIS-databank;

(c) het proces van de initialisering en het herstel van de nationale kopieën.

(d) ononderbroken beschikbaarheid.

Artikel 5
Kosten

1. De kosten voor de werking, het onderhoud en de verdere ontwikkeling van het centrale SIS en de communicatie-infrastructuur komen ten laste van de algemene begroting van de Europese Unie.

2. Deze kosten omvatten de werkzaamheden in verband met CS-SIS die nodig zijn voor het leveren van de in artikel 4, lid 4, bedoelde diensten.

3. De kosten voor het opzetten, de werking en de verdere ontwikkeling van elk N.SIS komen ten laste van de betrokken lidstaat.

---

[70] Opgericht bij Verordening (EU) nr. 1077/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (PB L 286 van 1.11.2011, blz. 1).

HOOFDSTUK II

VERANTWOORDELIJKHEDEN VAN DE LIDSTATEN

Artikel 6
Nationale systemen

Elke lidstaat is verantwoordelijk voor het opzetten, de werking, het onderhoud en de verdere ontwikkeling van zijn N.SIS en voor het aansluiten van zijn N.SIS op NI-SIS.

Elke lidstaat is verantwoordelijk voor het waarborgen van de ononderbroken werking van N.SIS, de aansluiting van N.SIS op NI-SIS en de ononderbroken beschikbaarheid van SIS-gegevens voor de eindgebruikers.

Artikel 7
N.SIS-instantie en Sirene-bureau

1. Elke lidstaat wijst een autoriteit aan (N.SIS-instantie) die de centrale verantwoordelijkheid voor N.SIS heeft.

   Deze autoriteit is verantwoordelijk voor de goede werking en beveiliging van N.SIS, zorgt voor de toegang van de bevoegde autoriteiten tot het SIS, en neemt de nodige maatregelen ten behoeve van de naleving van de bepalingen van deze verordening. Zij is er tevens verantwoordelijk voor dat alle SIS-functies op adequate wijze ter beschikking van de eindgebruikers worden gesteld.

   Elke lidstaat zendt zijn signaleringen door via zijn N.SIS-instantie.

2. Elke lidstaat wijst de autoriteit (Sirene-bureau) aan die ervoor zorgt dat alle aanvullende informatie overeenkomstig het in artikel 8 bedoelde Sirene-handboek wordt uitgewisseld en beschikbaar is.

   De Sirene-bureaus coördineren ook de verificatie van de kwaliteit van de in het SIS opgenomen informatie. Voor deze taken hebben de Sirene-bureaus toegang tot in het SIS verwerkte gegevens.

3. De lidstaten lichten het Agentschap in over hun N.SIS-instantie en hun Sirene-bureau. Het Agentschap maakt daarvan een lijst bekend, samen met de in artikel 36, lid 8, bedoelde lijst.

Artikel 8
Uitwisseling van aanvullende informatie

1. Aanvullende informatie wordt uitgewisseld overeenkomstig het Sirene-handboek en met gebruikmaking van de communicatie-infrastructuur. De lidstaten verstrekken de technische en personele middelen die nodig zijn om de ononderbroken beschikbaarheid en uitwisseling van aanvullende informatie te waarborgen. Indien de communicatie-infrastructuur niet voorhanden is, kunnen de lidstaten andere afdoende

beveiligde technische middelen gebruiken voor de uitwisseling van aanvullende informatie.

2. Aanvullende informatie wordt alleen gebruikt voor het doel waarvoor zij is verstrekt overeenkomstig artikel 43, tenzij vooraf toestemming is verkregen van de signalerende lidstaat.

3. De Sirene-bureaus verrichten hun taak snel en efficiënt, in het bijzonder door een verzoek zo spoedig mogelijk, en niet later dan twaalf uur na het te hebben ontvangen, te beantwoorden.

4. Nadere voorschriften voor de uitwisseling van aanvullende informatie worden door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure vastgesteld in de vorm van een handboek, "Sirene-handboek" genoemd.

Artikel 9
Naleving van technische en functionele vereisten

1. Bij het opzetten van N.SIS conformeert elke lidstaat zich aan de gemeenschappelijke normen, protocollen en technische procedures die zijn vastgesteld om de compatibiliteit van N.SIS met CS-SIS te waarborgen met het oog op een snelle en efficiënte gegevenstransmissie. Deze gemeenschappelijke normen, protocollen en technische procedures worden door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure vastgesteld en ontwikkeld.

2. De lidstaten zorgen er met behulp van de door CS-SIS geleverde diensten voor dat de gegevens die in de nationale kopie zijn opgeslagen, door middel van in artikel 4, lid 4, bedoelde automatische bijwerkingen, identiek en consistent zijn met de SIS-databank en dat een opzoeking in die nationale kopie een resultaat oplevert dat gelijkwaardig is aan een opzoeking in de SIS-databank. De eindgebruikers ontvangen de gegevens die zij voor de uitvoering van hun taken nodig hebben, met name alle gegevens die vereist zijn om de betrokkene te identificeren en om de gevraagde maatregel uit te voeren.

Artikel 10
Beveiliging - Lidstaten

1. Elke lidstaat neemt passende maatregelen inzake N.SIS, waaronder de vaststelling van een veiligheidsplan, een bedrijfscontinuïteitsplan en een uitwijkplan, opdat:

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

   (b) onbevoegden de toegang tot de voor de verwerking van persoonsgegevens gebruikte gegevensverwerkingsfaciliteiten wordt ontzegd (controle op de toegang tot de faciliteiten);

   (c) wordt voorkomen dat gegevensdragers onrechtmatig worden gelezen, gekopieerd, veranderd of verwijderd (controle op gegevensdragers);

(d) wordt voorkomen dat gegevens onrechtmatig worden ingevoerd en opgeslagen persoonsgegevens onrechtmatig worden geïnspecteerd, gewijzigd of gewist (controle op de opslag);

(e) wordt voorkomen dat geautomatiseerde gegevensverwerkingssystemen door middel van datatransmissieapparatuur door onbevoegden worden gebruikt (controle op de gebruikers);

(f) wordt gewaarborgd dat degenen die bevoegd zijn een geautomatiseerd gegevensverwerkingssysteem te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft, en uitsluitend middels persoonlijke en unieke gebruikersidentiteiten en geheime toegangsprocedures (controle op de toegang tot de gegevens);

(g) wordt gewaarborgd dat alle autoriteiten met toegangsrecht tot het SIS of tot de gegevensverwerkingsfaciliteiten profielen opstellen waarin de taken en verantwoordelijkheden worden omschreven van de personen die bevoegd zijn om toegang te krijgen tot gegevens en gegevens in te voeren, bij te werken, te wissen en te doorzoeken, en dat deze profielen desgevraagd onverwijld ter beschikking worden gesteld van de nationale toezichthoudende autoriteiten als bedoeld in artikel 50, lid 1 (personeelsprofielen);

(h) wordt gewaarborgd dat kan worden geverifieerd en vastgesteld aan welke instanties persoonsgegevens door middel van datatransmissieapparatuur mogen worden doorgezonden (controle op de doorzending);

(i) wordt gewaarborgd dat naderhand kan worden geverifieerd en vastgesteld welke persoonsgegevens wanneer, door wie en voor welk doel in geautomatiseerde gegevensverwerkingssystemen zijn opgenomen (controle op de opneming);

(j) wordt voorkomen, in het bijzonder door middel van passende versleutelingstechnieken, dat bij de doorgifte van persoonsgegevens, alsmede bij het transport van gegevensdragers de gegevens onrechtmatig worden gelezen, gekopieerd, gewijzigd of gewist (controle op het transport);

(k) de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen wordt gemonitord en de nodige organisatorische maatregelen worden genomen met betrekking tot de interne monitoring (interne audit).

2. Voor de beveiliging van de verwerking en uitwisseling van aanvullende gegevens, waaronder de beveiliging van de kantoren van het Sirene-bureau, nemen de lidstaten maatregelen die gelijkwaardig zijn aan die als bedoeld in lid 1.

3. Voor de beveiliging van de verwerking van SIS-gegevens door de in artikel 29 bedoelde autoriteiten nemen de lidstaten maatregelen die gelijkwaardig zijn aan die als bedoeld in lid 1 van dit artikel.

Artikel 11
Vertrouwelijkheid - Lidstaten

Elke lidstaat past, in overeenstemming met zijn nationale recht, de voorschriften inzake het beroepsgeheim of een gelijkwaardige geheimhoudingsplicht toe op iedere persoon en instantie die met SIS-gegevens en aanvullende SIS-informatie moet werken. Deze geheimhoudingsplicht blijft gelden nadat de persoon zijn functie of dienstverband heeft beëindigd of de instantie haar werkzaamheden heeft stopgezet.

Artikel 12
Bijhouden van logbestanden op nationaal niveau

1. De lidstaten zorgen ervoor dat elke toegang tot en uitwisseling van persoonsgegevens in CS-SIS wordt vastgelegd in N.SIS met het oog op controle op de rechtmatigheid van de bevraging, monitoring van de rechtmatigheid van de gegevensverwerking, interne monitoring, de goede werking van N.SIS en de integriteit en beveiliging van de gegevens.

2. De logbestanden bevatten met name het relaas van de signaleringen, de datum en het tijdstip van de gegevensverwerking, het soort voor de bevraging gebruikte gegevens, een verwijzing naar het soort toegezonden gegevens, alsmede de naam van de bevoegde autoriteit en van de persoon die met de verwerking van de gegevens is belast.

3. Als voor de bevraging dactyloscopische gegevens of gezichtsopnamen worden gebruikt overeenkomstig artikel 22, bevatten de logbestanden met name het soort voor de bevraging gebruikte gegevens, een verwijzing naar het soort toegezonden gegevens, alsmede de naam van de bevoegde autoriteit en van de persoon die met de verwerking van de gegevens is belast.

4. De logbestanden worden alleen voor het in lid 1 genoemde doel gebruikt en worden ten vroegste één jaar en ten laatste drie jaar na het creëren ervan gewist.

5. Logbestanden mogen langer worden bewaard indien zij nodig zijn in het kader van lopende monitoringprocedures.

6. De bevoegde nationale autoriteiten die zijn belast met het controleren van de rechtmatigheid van bevragingen, met het monitoren van de rechtmatigheid van de gegevensverwerking, met interne monitoring en met het waarborgen van de goede werking van N.SIS en de gegevensintegriteit en -beveiliging, hebben binnen de grenzen van hun bevoegdheden op verzoek toegang tot deze logbestanden met het oog op het vervullen van hun taken.

Artikel 13
Interne monitoring

De lidstaten zorgen ervoor dat elke autoriteit met toegangsrecht tot SIS-gegevens de nodige maatregelen treft om aan deze verordening te voldoen, en, indien nodig, samenwerkt met de nationale toezichthoudende autoriteit.

Artikel 14
Opleiding van personeel

Alvorens te worden gemachtigd tot de verwerking van in het SIS opgeslagen gegevens, en vervolgens op regelmatige basis, krijgt het personeel van de autoriteiten met toegangsrecht tot het SIS een adequate opleiding over de regels inzake gegevensbeveiliging en -bescherming en de procedures voor gegevensverwerking, zoals uiteengezet in het Sirene-handboek. Het personeel wordt op de hoogte gebracht van alle ter zake doende strafbare feiten en sancties.

HOOFDSTUK III

VERANTWOORDELIJKHEDEN VAN HET AGENTSCHAP

Artikel 15
Operationeel beheer

1. Het Agentschap is verantwoordelijk voor het operationele beheer van het centrale SIS. Het Agentschap zorgt er in samenwerking met de lidstaten voor dat te allen tijde de beste beschikbare technologie wordt gebruikt voor het centrale SIS, uitgaande van een kosten-batenanalyse.

2. Het Agentschap wordt tevens belast met de volgende taken met betrekking tot de communicatie-infrastructuur:

   (a) toezicht;

   (b) beveiliging;

   (c) coördinatie van de betrekkingen tussen de lidstaten en de dienstverlener.

3. De Commissie wordt belast met alle andere taken die betrekking hebben op de communicatie-infrastructuur, met name:

   (a) begrotingsuitvoeringstaken;

   (b) aanschaf en vernieuwing;

   (c) contractuele aangelegenheden.

4. Het Agentschap wordt tevens belast met de volgende taken met betrekking tot de Sirene-bureaus en de communicatie tussen de Sirene-bureaus:

   (a) de coördinatie en het beheer van tests;

   (b) het onderhoud en de bijwerking van de technische specificaties voor de uitwisseling van aanvullende informatie tussen de Sirene-bureaus en de communicatie-infrastructuur, en het beheer van gevolgen van technische wijzigingen die een impact hebben voor zowel het SIS als de uitwisseling van aanvullende informatie tussen de Sirene-bureaus.

5. Het Agentschap ontwikkelt en onderhoudt een mechanisme en procedures voor het uitvoeren van kwaliteitscontroles op de gegevens in CS-SIS en brengt regelmatig verslag uit aan de lidstaten. Het Agentschap rapporteert regelmatig aan de Commissie welke kwesties zijn geconstateerd en welke lidstaten hierbij zijn betrokken. Het mechanisme, de procedures en de uitlegging inzake de naleving op het gebied van gegevenskwaliteit worden door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure vastgesteld en ontwikkeld.

6. Het operationele beheer van het centrale SIS omvat alle taken die nodig zijn om het centrale SIS 24 uur per dag en 7 dagen per week overeenkomstig deze verordening te laten functioneren, met name de voor de goede werking van het systeem onontbeerlijke onderhoudswerkzaamheden en technische ontwikkelingen. Deze taken omvatten tevens testactiviteiten om het centrale SIS en de nationale systemen te laten functioneren overeenkomstig de technische en functionele vereisten als bedoeld in artikel 9 van deze verordening.

Artikel 16
Beveiliging

1. Het Agentschap stelt de nodige maatregelen vast, met inbegrip van een beveiligingsplan, een bedrijfscontinuïteitsplan en een uitwijkplan voor het centrale SIS en de communicatie-infrastructuur, opdat:

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

   (b) onbevoegden de toegang tot de voor de verwerking van persoonsgegevens gebruikte gegevensverwerkingsfaciliteiten wordt ontzegd (controle op de toegang tot de faciliteiten);

   (c) wordt voorkomen dat gegevensdragers onrechtmatig worden gelezen, gekopieerd, veranderd of verwijderd (controle op gegevensdragers);

   (d) wordt voorkomen dat gegevens onrechtmatig worden ingevoerd en opgeslagen persoonsgegevens onrechtmatig worden geïnspecteerd, gewijzigd of gewist (controle op de opslag);

   (e) wordt voorkomen dat geautomatiseerde gegevensverwerkingssystemen door middel van datatransmissieapparatuur door onbevoegden worden gebruikt (controle op de gebruikers);

   (f) wordt gewaarborgd dat degenen die bevoegd zijn een geautomatiseerd gegevensverwerkingssysteem te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft, en uitsluitend middels persoonlijke en unieke gebruikersidentiteiten en geheime toegangsprocedures (controle op de toegang tot de gegevens);

   (g) profielen worden opgesteld waarin de taken en verantwoordelijkheden worden omschreven van de personen die bevoegd zijn om toegang te krijgen tot de gegevens of de gegevensverwerkingsvoorzieningen, en opdat deze profielen desgevraagd onverwijld ter beschikking worden gesteld van de in artikel 51

bedoelde Europese Toezichthouder voor gegevensbescherming (personeelsprofielen);

(h) wordt gewaarborgd dat kan worden geverifieerd en vastgesteld aan welke instanties persoonsgegevens door middel van datatransmissieapparatuur mogen worden doorgezonden (controle op de overdracht);

(i) wordt gewaarborgd dat naderhand kan worden nagegaan en vastgesteld welke persoonsgegevens wanneer en door wie in een geautomatiseerd gegevensverwerkingssysteem zijn opgenomen (controle op de opneming);

(j) wordt voorkomen, in het bijzonder door middel van passende versleutelingstechnieken, dat bij de doorgifte van persoonsgegevens, alsmede bij het transport van gegevensdragers de gegevens onrechtmatig worden gelezen, gekopieerd, gewijzigd of gewist (controle op het transport);

(k) de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen wordt gemonitord, en de nodige organisatorische maatregelen voor de interne monitoring worden genomen om de naleving van deze verordening te waarborgen (interne audit).

2. Met het oog op de beveiliging van de verwerking en de uitwisseling van aanvullende informatie via de communicatie-infrastructuur neemt het Agentschap maatregelen die gelijkwaardig zijn aan die als bedoeld in lid 1.

Artikel 17
Vertrouwelijkheid - Agentschap

1. Onverminderd artikel 17 van het Statuut van de ambtenaren en de regeling welke van toepassing is op de andere personeelsleden van de Europese Unie, past het Agentschap adequate voorschriften inzake het beroepsgeheim of een gelijkwaardige geheimhoudingsplicht toe op iedere persoon die met SIS-gegevens moet werken, aan de hand van normen die vergelijkbaar zijn met die van artikel 11 van deze verordening. Deze geheimhoudingsplicht blijft gelden nadat de persoon zijn functie of dienstverband heeft beëindigd of zijn werkzaamheden heeft stopgezet.

2. Met het oog op de vertrouwelijkheid bij de uitwisseling van aanvullende informatie via de communicatie-infrastructuur neemt het Agentschap maatregelen die gelijkwaardig zijn aan die als bedoeld in lid 1.

Artikel 18
Bijhouden van logbestanden op centraal niveau

1. Het Agentschap draagt er zorg voor dat elke toegang tot en elke uitwisseling van persoonsgegevens in CS-SIS voor de in artikel 12, lid 1, genoemde doeleinden wordt geregistreerd in logbestanden.

2. De logbestanden bevatten met name het relaas van de signaleringen, de datum en het tijdstip van de gegevenstransmissie, het soort voor de bevraging gebruikte gegevens, een verwijzing naar het soort toegezonden gegevens, alsmede de naam van de bevoegde autoriteit die met de verwerking van de gegevens is belast.

3. Als voor de bevraging dactyloscopische gegevens of gezichtsopnamen worden gebruikt overeenkomstig de artikelen 22 en 28, bevatten de logbestanden met name het soort voor de bevraging gebruikte gegevens, een verwijzing naar het soort toegezonden gegevens, alsmede de naam van de bevoegde autoriteit en van de persoon die met de verwerking van de gegevens is belast.

4. De logbestanden worden alleen voor het in lid 1 genoemde doel gebruikt en worden ten vroegste één jaar en ten laatste drie jaar na het creëren ervan gewist. De logbestanden die het relaas van de signaleringen bevatten, worden één tot drie jaar na het wissen van de signaleringen gewist.

5. Logbestanden mogen langer worden bewaard indien zij nodig zijn in het kader van lopende monitoringprocedures.

6. De bevoegde nationale autoriteiten die zijn belast met het controleren van de rechtmatigheid van bevragingen, het monitoren van de rechtmatigheid van de gegevensverwerking, interne monitoring en het waarborgen van de goede werking van N.SIS en de gegevensintegriteit en -beveiliging hebben binnen de grenzen van hun bevoegdheden op verzoek toegang tot deze logbestanden met het oog op het vervullen van hun taken.

HOOFDSTUK IV

PUBLIEKSVOORLICHTING

Artikel 19
Voorlichtingscampagnes over het SIS

De Commissie organiseert in samenwerking met de nationale toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming geregeld campagnes om het publiek te informeren omtrent de doelstellingen van het SIS, de in het SIS opgeslagen gegevens, de autoriteiten die toegang hebben tot het SIS, en de rechten van de betrokkenen. De lidstaten ontwikkelen en implementeren in samenwerking met hun nationale toezichthoudende autoriteiten de nodige beleidsinitiatieven om hun burgers algemene voorlichting over het SIS te geven.

HOOFDSTUK V

SIGNALERINGEN VAN ONDERDANEN VAN DERDE LANDEN MET HET OOG OP WEIGERING VAN TOEGANG EN VERBLIJF

Artikel 20
Categorieën gegevens

1. Onverminderd artikel 8, lid 1, en de bepalingen van deze verordening met betrekking tot de opslag van extra gegevens, bevat het SIS alleen de door elke lidstaat verstrekte categorieën gegevens, als vereist voor de in artikel 24 genoemde doeleinden.

2. Voor gesignaleerde personen worden uitsluitend de onderstaande gegevens opgenomen:

   (a) achternaam/achternamen;

   (b) voornaam/voornamen;

   (c) naam/namen bij geboorte;

   (d) voorheen gebruikte namen en aliassen;

   (e) bijzondere, onveranderlijke objectieve fysieke kenmerken;

   (f) geboorteplaats;

   (g) geboortedatum;

   (h) geslacht;

   (i) nationaliteit(en);

   (j) de vermelding of de betrokken persoon gewapend, gewelddadig of ontsnapt is of is betrokken bij activiteiten die vallen onder de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van de Raad inzake terrorismebestrijding;

   (k) reden van signalering;

   (l) signalerende autoriteit;

   (m) vermelding van de beslissing die aan de signalering ten grondslag ligt;

   (n) de uit te voeren maatregel;

   (o) koppeling(en) met andere SIS-signaleringen in overeenstemming met artikel 38;

   (p) de vermelding of de betrokken persoon een familielid is van een EU-burger of van een andere persoon die rechten van vrij verkeer geniet als bedoeld in artikel 25;

(q) de vermelding of de beslissing tot weigering van toegang is gebaseerd op:

– eerdere veroordelingen als bedoeld in artikel 24, lid 2, onder a);

– ernstige veiligheidsdreigingen als bedoeld in artikel 24, lid 2, onder b);

– een inreisverbod als bedoeld in artikel 24, lid 3, of

– een beperkende maatregel als bedoeld in artikel 27;

(r) soort strafbaar feit (voor signaleringen op grond van artikel 24, lid 2);

(s) categorie van het identificatiedocument;

(t) land van afgifte van het identificatiedocument;

(u) nummer(s) van het identificatiedocument;

(v) datum van afgifte van het identificatiedocument;

(w) foto's en gezichtsopnamen;

(x) dactyloscopische gegevens;

(y) een kleurenkopie van het identificatiedocument.

3. De technische voorschriften voor het opnemen, bijwerken, wissen en doorzoeken van de in lid 2 bedoelde gegevens worden vastgesteld en ontwikkeld door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure.

4. De technische voorschriften voor het doorzoeken van de in lid 2 bedoelde gegevens worden vastgesteld en ontwikkeld overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure. Deze technische voorschriften worden ook gebruikt voor opzoekingen in CS-SIS, in nationale kopieën en in technische kopieën als bedoeld in artikel 36, en zijn gebaseerd op gemeenschappelijke normen die zijn vastgesteld en ontwikkeld door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure.

Artikel 21
Evenredigheid

1. Alvorens een persoon te signaleren of de geldigheidsduur van een signalering te verlengen, gaat een lidstaat na of het geval gepast, relevant en belangrijk genoeg is om opneming van een signalering in het SIS te rechtvaardigen.

2. Op grond van artikel 24, lid 2, worden onderdanen van derde landen onder alle omstandigheden door de lidstaten gesignaleerd, indien het betrokken strafbare feit

valt onder de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van de Raad inzake terrorismebestrijding[71].

Artikel 22
Specifieke voorschriften voor opneming van foto's, gezichtsopnamen en dactyloscopische gegevens

1. Gegevens als bedoeld in artikel 20, lid 2, onder w) en x), worden alleen in het SIS opgenomen nadat door middel van een kwaliteitscontrole is vastgesteld dat aan een minimumnorm voor gegevenskwaliteit is voldaan.

2. Er worden kwaliteitsnormen vastgesteld voor de opslag van de in lid 1 bedoelde gegevens. Deze normen worden nader uitgewerkt en bijgewerkt door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure.

Artikel 23
Vereisten voor de opneming van een signalering

1. Een signalering wordt niet opgenomen indien de in artikel 20, lid 2, onder a), g), k), m), n) en q), genoemde gegevens ontbreken. Wanneer een signalering is gebaseerd op een beslissing als bedoeld in artikel 24, lid 2, worden tevens de in artikel 20, lid 2, onder r), genoemde gegevens opgenomen.

2. Daarnaast worden, voor zover beschikbaar, alle andere in artikel 20, lid 2, genoemde gegevens opgenomen.

Artikel 24
Voorwaarden voor het uitvaardigen van signaleringen met het oog op weigering van toegang en verblijf

1. Gegevens over met het oog op weigering van toegang en verblijf gesignaleerde onderdanen van derde landen worden in het SIS opgenomen op grond van een nationale signalering ingevolge een beslissing die de bevoegde administratieve of gerechtelijke autoriteiten met inachtneming van de nationale wettelijke procedurevoorschriften hebben gegeven op basis van een individuele beoordeling. Het recht van beroep tegen deze beslissingen wordt uitgeoefend overeenkomstig het nationale recht.

2. Indien de in lid 1 bedoelde beslissing is gegeven omdat de aanwezigheid van de betrokken onderdaan van een derde land op het grondgebied van een lidstaat een bedreiging kan vormen voor de openbare orde of veiligheid of de nationale veiligheid, wordt een signalering opgenomen. Dit is in het bijzonder het geval bij:

   (a) een onderdaan van een derde land die in een lidstaat schuldig is bevonden aan een strafbaar feit waarvoor een vrijheidsstraf van ten minste één jaar geldt;

---

[71] Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding (PB L 164 van 22.6.2002, blz. 3).

(b) een onderdaan van een derde land ten aanzien van wie er gegronde redenen zijn om aan te nemen dat hij een ernstig strafbaar heeft gepleegd, of er duidelijke aanwijzingen zijn dat hij overweegt een dergelijk feit te plegen op het grondgebied van een lidstaat.

3. Indien de in lid 1 bedoelde beslissing is gegeven omdat een inreisverbod is uitgevaardigd overeenkomstig Richtlijn 2008/115/EG, wordt een signalering opgenomen. De signalerende lidstaat zorgt ervoor dat de signalering in het SIS van kracht wordt op het moment waarop de betrokken onderdaan van een derde land terugkeert naar het derde land. De bevestiging van de terugkeer wordt aan de signalerende lidstaat meegedeeld overeenkomstig artikel 6 van Verordening (EU) 2018/xxx [terugkeerverordening].

Artikel 25
Voorwaarden voor de opneming van signaleringen van onderdanen van derde landen die het recht van vrij verkeer binnen de Unie genieten

1. Een signalering van een onderdaan van een derde land die het recht van vrij verkeer binnen de Unie geniet in de zin van Richtlijn 2004/38/EG van het Europees Parlement en de Raad[72], wordt opgenomen overeenkomstig de maatregelen ter uitvoering van die richtlijn.

2. In geval van een treffer met een op grond van artikel 24 gesignaleerde onderdaan van een derde land die het recht van vrij verkeer binnen de Unie geniet, pleegt de uitvoerende lidstaat onmiddellijk overleg met de signalerende lidstaat via het uitwisselen van aanvullende informatie, teneinde onverwijld te besluiten welke maatregel moet worden uitgevoerd.

Artikel 26
Overlegprocedure

1. Een lidstaat die overweegt een verblijfstitel of andere machtiging tot verblijf af te geven aan een onderdaan van een derde land die door een andere lidstaat is gesignaleerd met het oog op weigering van toegang en verblijf, pleegt eerst door middel van de uitwisseling van aanvullende informatie overleg met de signalerende lidstaat en houdt rekening met de belangen van die lidstaat. De signalerende lidstaat geeft binnen zeven dagen een definitief antwoord. Indien de lidstaat die overweegt een verblijfstitel of andere machtiging tot verblijf af te geven, daadwerkelijk tot afgifte beslist, wordt de signalering met het oog op weigering van toegang en verblijf gewist.

2. Een lidstaat die overweegt een signalering met het oog op weigering van toegang en verblijf op te nemen voor een onderdaan van een derde land die in het bezit is van een door een andere lidstaat afgegeven geldige verblijfstitel of andere machtiging tot verblijf, pleegt eerst door middel van de uitwisseling van aanvullende informatie overleg met de lidstaat die de verblijfstitel heeft afgegeven, en houdt rekening met de belangen van die lidstaat. De lidstaat die de titel heeft afgegeven, geeft binnen zeven dagen een definitief antwoord. Indien de lidstaat die de titel heeft afgegeven, beslist

[72] PB L 158 van 30.4.2004, blz. 77.

deze te handhaven, wordt de signalering met het oog op weigering van toegang en verblijf niet opgenomen.

3. In geval van een treffer met een onderdaan van een derde land die met het oog op weigering van toegang en verblijf is gesignaleerd en in het bezit is van een geldige verblijfstitel of andere machtiging tot verblijf, pleegt de uitvoerende lidstaat onmiddellijk door middel van de uitwisseling van aanvullende informatie overleg met de lidstaat die de verblijftitel heeft afgegeven en met de signalerende lidstaat, teneinde onverwijld te besluiten welke maatregel moet worden uitgevoerd. Indien wordt besloten de verblijfstitel te handhaven, wordt de signalering gewist.

4. De lidstaten verstrekken jaarlijks statistieken aan het Agentschap over het overleg dat overeenkomstig de leden 1, 2 en 3 is gepleegd.

Artikel 27

Voorwaarden voor het uitvaardigen van signaleringen van onderdanen van derde landen ten aanzien van wie een beperkende maatregel is genomen

1. Onderdanen van derde landen ten aanzien van wie overeenkomstig een wetsbesluit van de Raad een beperkende maatregel is genomen om de toegang tot of de doorreis via het grondgebied van de lidstaten te beletten, met inbegrip van maatregelen ter uitvoering van een door de Veiligheidsraad van de Verenigde Naties ingesteld reisverbod, worden in het SIS gesignaleerd met het oog op weigering van toegang en verblijf, voor zover aan de eisen inzake de kwaliteit van de gegevens is voldaan.

2. Bij de aanneming van de desbetreffende maatregel overeenkomstig artikel 29 van het Verdrag betreffende de Europese Unie wordt bepaald welke lidstaat verantwoordelijk is voor het opnemen, bijwerken en wissen van deze signaleringen namens de andere lidstaten. De procedure voor het aanwijzen van de verantwoordelijke lidstaat wordt vastgesteld en ontwikkeld door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure.

HOOFDSTUK VI

BEVRAGING AAN DE HAND VAN BIOMETRISCHE GEGEVENS

Artikel 28

Specifieke voorschriften voor verificaties of bevragingen met foto's, gezichtsopnamen en dactyloscopische gegevens

1. In het SIS opgeslagen foto's, gezichtsopnamen en dactyloscopische gegevens worden opgevraagd om de identiteit van een persoon die naar aanleiding van een alfanumerieke bevraging van het SIS is gelokaliseerd, te verifiëren.

2. Ook dactyloscopische gegevens mogen worden gebruikt om een persoon te identificeren. In het SIS opgeslagen dactyloscopische gegevens worden voor identificatiedoeleinden gebruikt indien de identiteit van de persoon niet met behulp van andere middelen kan worden vastgesteld.

3. In het SIS opgeslagen dactyloscopische gegevens in verband met signaleringen op grond van artikel 24 kunnen tevens worden doorzocht aan de hand van volledige of onvolledige reeksen vingerafdrukken of handpalmafdrukken die zijn aangetroffen op de plaats van het delict dat wordt onderzocht, mits met een hoge mate van waarschijnlijkheid kan worden vastgesteld dat de afdrukken die van de dader zijn en mits de bevoegde autoriteiten niet in staat zijn om de identiteit van de persoon met behulp van andere nationale, Europese of internationale databanken vast te stellen.

4. Zodra dit technisch haalbaar is en mits voor de identificatie een hoge mate van betrouwbaarheid kan worden gewaarborgd, mogen foto's en gezichtsopnamen worden gebruikt om een persoon te identificeren. Identificatie op basis van foto's en gezichtsopnamen is uitsluitend toegestaan bij reguliere grensdoorlaatposten met zelfbedieningssystemen en automatische grenstoezichtsystemen.

HOOFDSTUK VII

RECHT OP TOEGANG TOT SIGNALERINGEN EN BEWARING VAN SIGNALERINGEN

Artikel 29
Autoriteiten met recht op toegang tot signaleringen

1. De toegang tot de in het SIS opgenomen gegevens en het recht om deze gegevens direct in het SIS of in een kopie van SIS-gegevens te bevragen, komt uitsluitend toe aan de autoriteiten die verantwoordelijk zijn voor het identificeren van onderdanen van derde landen ten behoeve van:

   (a) het grenstoezicht, overeenkomstig Verordening (EU) 2016/399 van het Europees Parlement en de Raad van 9 maart 2016 betreffende een Uniecode voor de overschrijding van de grenzen door personen (Schengengrenscode);

   (b) politie- en douanecontroles die in de betrokken lidstaat worden uitgevoerd, en de coördinatie daarvan door de daartoe aangewezen autoriteiten;

   (c) andere rechtshandhavingsactiviteiten die worden uitgevoerd met het oog op het voorkomen, opsporen en onderzoeken van strafbare feiten in de betrokken lidstaat;

   (d) het onderzoeken van de voorwaarden en het nemen van beslissingen in verband met de toegang tot en het verblijf van onderdanen van derde landen op het grondgebied van de lidstaten, onder meer inzake verblijfstitels en visa voor verblijf van langere duur, en in verband met de terugkeer van onderdanen van derde landen;

   (e) het onderzoeken van visumaanvragen en het nemen van beslissingen in verband met deze aanvragen, inclusief inzake nietigverklaring, intrekking of

verlenging van visa, overeenkomstig Verordening (EU) nr. 810/2009 van het Europees Parlement en de Raad[73].

2. Voor de toepassing van artikel 24, leden 2 en 3, en artikel 27 hebben ook de nationale gerechtelijke autoriteiten, met inbegrip van de autoriteiten die belast zijn met de instelling van strafvervolging en van gerechtelijke onderzoeken voorafgaand aan tenlastelegging, alsook hun coördinerende instanties, met het oog op de uitvoering van hun in de nationale wetgeving vastgestelde taken, recht op toegang tot de in het SIS opgenomen gegevens en tot directe bevraging daarvan.

3. Ook de in lid 1, onder d), bedoelde autoriteiten hebben recht op toegang tot en bevraging van gegevens over persoonsdocumenten die zijn opgenomen overeenkomstig artikel 38, lid 2, onder j) en k), van Verordening (EU) 2018/xxx [politiële samenwerking en justitiële samenwerking in strafzaken]. Het toegangsrecht van deze autoriteiten wordt uitgeoefend overeenkomstig de wetgeving van de onderscheiden lidstaten.

4. De in dit artikel bedoelde autoriteiten worden opgenomen in de in artikel 36, lid 8, bedoelde lijst.

Artikel 30
Toegang van Europol tot SIS-gegevens

1. Het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) heeft binnen de grenzen van zijn mandaat recht op toegang tot en bevraging van in het SIS opgenomen gegevens.

2. Indien Europol bij een bevraging een signalering in het SIS aantreft, stelt Europol de signalerende lidstaat daarvan in kennis via de kanalen als bedoeld in Verordening (EU) 2016/794.

3. Door bevraging van het SIS verkregen informatie wordt alleen gebruikt indien de betrokken lidstaat daarmee instemt. Indien de betrokken lidstaat het gebruik van dergelijke informatie toestaat, wordt deze door Europol behandeld overeenkomstig Verordening (EU) 2016/794. Europol deelt die informatie alleen mee aan andere landen en organen indien de betrokken lidstaat daarmee instemt.

4. Europol kan de betrokken lidstaat om nadere informatie verzoeken overeenkomstig Verordening (EU) 2016/794.

5. Europol is ertoe gehouden:

(a) onverminderd de leden 3, 4 en 6, geen delen van het SIS te verbinden met een computersysteem voor gegevensverzameling en -verwerking dat door of bij Europol wordt gebruikt, geen in het SIS opgenomen gegevens waartoe Europol toegang heeft, over te dragen naar een dergelijk systeem, en geen delen van het SIS te downloaden of anderszins te kopiëren;

---

[73] Verordening (EG) nr. 810/2009 van het Europees Parlement en de Raad van 13 juli 2009 tot vaststelling van een gemeenschappelijke visumcode (Visumcode) (PB L 243 van 15.9.2009, blz. 1).

(b) de toegang tot in het SIS opgenomen gegevens te beperken tot specifiek daartoe gemachtigd personeel van Europol;

(c) maatregelen als bedoeld in de artikelen 10 en 11 te nemen en toe te passen;

(d) de Europese Toezichthouder voor gegevensbescherming in de gelegenheid te stellen de activiteiten te evalueren die Europol verricht op grond van zijn recht op toegang tot en bevraging van in het SIS opgenomen gegevens.

6. Het kopiëren van gegevens is uitsluitend toegestaan voor technische doeleinden, voor zover dit noodzakelijk is voor een directe bevraging door naar behoren gemachtigd Europol-personeel. De bepalingen van deze verordening zijn van toepassing op dergelijke kopieën. De technische kopie wordt gebruikt om SIS-gegevens op te slaan terwijl deze worden doorzocht. Zodra de gegevens zijn doorzocht, worden zij gewist. Dergelijk gebruik wordt niet beschouwd als illegaal downloaden of kopiëren van SIS-gegevens. Europol kopieert geen signaleringsgegevens of extra gegevens die door de lidstaten zijn verstrekt of uit CS-SIS afkomstig zijn, in andere Europol-systemen.

7. In lid 6 bedoelde kopieën die leiden tot de aanleg van offline gegevensbanken, worden maximaal 48 uur bewaard. Deze duur kan in noodsituaties worden verlengd, totdat de noodsituatie is beëindigd. Europol meldt dergelijke verlengingen aan de Europese Toezichthouder voor gegevensbescherming.

8. Europol mag aanvullende informatie inzake SIS-signaleringen ontvangen en verwerken, op voorwaarde dat de in de leden 2 tot en met 7 bedoelde voorschriften inzake gegevensverwerking naar behoren worden toegepast.

9. Om de rechtmatigheid van de gegevensverwerking te verifiëren, interne monitoring uit te voeren en een adequate beveiliging en integriteit van de gegevens te waarborgen, houdt Europol logbestanden bij van elke toegang tot en bevraging van het SIS. Deze logbestanden en documentatie worden niet beschouwd als illegale downloads of kopieën van een deel van het SIS.

Artikel 31

Toegang tot SIS-gegevens voor de Europese grens- en kustwachtteams, de teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken, en leden van de ondersteuningsteams voor migratiebeheer

1. Overeenkomstig artikel 40, lid 8, van Verordening (EU) 2016/1624 hebben de leden van de Europese grens- en kustwachtteams, van teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken en van de ondersteuningsteams voor migratiebeheer, binnen de grenzen van hun mandaat, recht op toegang tot en bevraging van in het SIS ingevoerde gegevens.

2. De in lid 1 bedoelde toegang tot en bevraging van in het SIS ingevoerde gegevens door leden van de Europese grens- en kustwachtteams, van teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken en van de ondersteuningsteams voor migratiebeheer verloopt via de in artikel 32, lid 2, bedoelde technische interface die wordt opgezet en onderhouden door het Europees Grens- en kustwachtagentschap.

3. Indien een lid van een Europees grens- en kustwachtteam, van een team van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken of van een ondersteuningsteam voor migratiebeheer bij een bevraging een signalering in het SIS aantreft, wordt de signalerende lidstaat daarvan in kennis gesteld. Overeenkomstig artikel 40 van Verordening (EU) 2016/1624 wordt door de teamleden uitsluitend op een SIS-signalering gereageerd op instructie van en, als algemene regel, in aanwezigheid van grenswachters of bij met terugkeer verband houdende taken betrokken personeel van de ontvangende lidstaat waar zij actief zijn. De ontvangende lidstaat mag de teamleden toestaan namens hem op te treden.

4. Elke toegang en bevraging door een lid van een Europese grens- en kustwachtteam, van een team van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken of van een ondersteuningsteam voor migratiebeheer wordt overeenkomstig artikel 12 in een logbestand vastgelegd en elk gebruik dat dit lid maakt van de gegevens waartoe hij toegang heeft gekregen, wordt geregistreerd.

5. De toegang tot in het SIS opgenomen gegevens wordt beperkt tot een specifiek lid van een Europese grens- en kustwachtteam, van een team van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken of van een ondersteuningsteam voor migratiebeheer, en wordt niet uitgebreid tot andere teamleden.

6. Ter waarborging van de beveiliging en de vertrouwelijkheid worden de maatregelen als bedoeld in de artikelen 10 en 11 vastgesteld.

Artikel 32

Toegang tot SIS-gegevens voor het Europees Grens- en kustwachtagentschap

1. Het Europees Grens- en kustwachtagentschap heeft, met het oog op het opstellen van analyses van de dreigingen die de werking of de veiligheid van de buitengrenzen kunnen aantasten, recht op toegang tot en bevraging van in het SIS opgenomen gegevens, overeenkomstig de artikelen 24 en 27.

2. Voor de toepassing van artikel 31, lid 2, en lid 1 van dit artikel wordt door het Europees Grens- en kustwachtagentschap een technische interface opgezet en onderhouden die een rechtstreekse verbinding met het centrale SIS mogelijk maakt.

3. Indien het Europees Grens- en kustwachtagentschap bij een bevraging een signalering in het SIS aantreft, stelt het de signalerende lidstaat daarvan in kennis.

4. Het Europees Grens- en kustwachtagentschap heeft voor het vervullen van de taken waarmee het op grond van de verordening tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS) is belast, recht op toegang tot en verificatie van in het SIS opgenomen gegevens, overeenkomstig de artikelen 24 en 27.

5. Indien het Europees Grens- en kustwachtagentschap bij een verificatie overeenkomstig lid 2 een signalering in het SIS aantreft, is de procedure als bedoeld in artikel 22 van de verordening tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS) van toepassing.

6. Niets in dit artikel wordt zodanig uitgelegd dat afbreuk wordt gedaan aan de bepalingen van Verordening (EU) 2016/1624 die betrekking hebben op gegevensbescherming en de aansprakelijkheid voor onrechtmatige of incorrecte verwerking van deze gegevens door het Europees Grens- en kustwachtagentschap.

7. Elke toegang en bevraging door het Europees Grens- en kustwachtagentschap wordt overeenkomstig artikel 12 in een logbestand vastgelegd en elk gebruik dat dit agentschap maakt van de gegevens waartoe het toegang heeft, wordt geregistreerd.

8. Het is niet toegestaan om delen van het SIS te verbinden met een computersysteem voor gegevensverzameling en -verwerking dat door of bij het Europees Grens- en kustwachtagentschap wordt gebruikt, en evenmin om in het SIS opgeslagen gegevens waartoe het Europees Grens- en kustwachtagentschap toegang heeft, over te dragen naar een dergelijk systeem, tenzij zulks noodzakelijk is voor het uitvoeren van de taken op grond van de verordening tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS). Er mag geen deel van het SIS worden gedownload. Het registreren van de toegang en de bevraging in logbestanden wordt niet beschouwd als illegaal downloaden of kopiëren van SIS-gegevens.

9. Ter waarborging van de beveiliging en de vertrouwelijkheid worden de maatregelen als bedoeld in de artikelen 10 en 11 vastgesteld.

Artikel 33
Reikwijdte van de toegang

Eindgebruikers, met inbegrip van Europol en het Europees Grens- en kustwachtagentschap, krijgen slechts toegang tot de gegevens die zij voor het vervullen van hun taken nodig hebben.

Artikel 34
Bewaartermijn voor signaleringen

1. De in het SIS overeenkomstig deze verordening opgenomen signaleringen worden niet langer bewaard dan nodig is voor het met de opneming nagestreefde doel.

2. Uiterlijk vijf jaar na de opneming van een signalering in het SIS toetst de signalerende lidstaat de noodzaak van verdere bewaring.

3. In voorkomend geval stelt elke lidstaat overeenkomstig zijn nationale recht kortere toetsingstermijnen vast.

4. Wanneer het personeel in een Sirene-bureau dat verantwoordelijk is voor de coördinatie en de verificatie van de kwaliteit van de gegevens, constateert dat een signalering van een persoon haar doel heeft bereikt en uit het SIS moet worden gewist, stelt het de autoriteit die de signalering heeft opgenomen daarvan in kennis. Uiterlijk 30 kalenderdagen na ontvangst van deze kennisgeving meldt de autoriteit dat de signalering is of zal worden gewist, of motiveert zij waarom de signalering wordt bewaard. Indien de autoriteit binnen de termijn van 30 kalenderdagen niet in die zin reageert, wordt de signalering gewist door het personeel van het Sirene-bureau. Wanneer zich herhaaldelijk dergelijke kwesties voordoen, melden de Sirene-bureaus dat aan hun nationale toezichthoudende autoriteit.

5. Vóór het verstrijken van de toetsingstermijn kan de signalerende lidstaat, op grond van een grondige individuele beoordeling die wordt geregistreerd, besluiten de signalering langer te bewaren indien dit vereist is voor het met de signalering nagestreefde doel. In dat geval is lid 2 tevens van toepassing op de verlenging. Elke verlenging van een signalering wordt doorgegeven aan CS-SIS.

6. Na afloop van de in lid 2 bedoelde toetsingstermijn worden signaleringen automatisch gewist, behalve wanneer de signalerende lidstaat de verlenging van de signalering aan CS-SIS heeft doorgegeven, overeenkomstig lid 5. CS-SIS stelt de lidstaten vier maanden op voorhand automatisch in kennis van de geplande wissing van de gegevens uit het systeem.

7. De lidstaten houden statistieken bij van het aantal signaleringen waarvan de bewaartermijn overeenkomstig lid 5 is verlengd.

Artikel 35
Wissen van signaleringen

1. Signaleringen met het oog op weigering van toegang en verblijf uit hoofde van artikel 24 worden gewist wanneer de beslissing die eraan ten grondslag lag, is ingetrokken door de bevoegde autoriteit, in voorkomend geval na de in artikel 26 bedoelde overlegprocedure.

2. Signaleringen van onderdanen van derde landen ten aanzien van wie een in artikel 27 bedoelde beperkende maatregel is genomen, worden gewist wanneer de maatregel tot uitvoering van het reisverbod is beëindigd, geschorst of nietig verklaard.

3. Signaleringen van personen die het burgerschap hebben verkregen van een staat waarvan de onderdanen het recht van vrij verkeer binnen de Unie genieten, worden gewist zodra de signalerende lidstaat er, eventueel via de in artikel 38 bedoelde weg, kennis van krijgt dat de betrokkene het burgerschap heeft verkregen.

HOOFDSTUK VIII

ALGEMENE VOORSCHRIFTEN INZAKE GEGEVENSVERWERKING

Artikel 36
Verwerking van SIS-gegevens

1. De lidstaten mogen de in artikel 20 bedoelde gegevens verwerken met het oog op de weigering van toegang tot en verblijf op hun grondgebied.

2. Gegevens mogen uitsluitend voor technische doeleinden worden gekopieerd, voor zover dit noodzakelijk is voor een directe bevraging door de in artikel 29 bedoelde autoriteiten. De bepalingen van deze verordening zijn van toepassing op dergelijke kopieën. Lidstaten kopiëren geen signaleringsgegevens of extra gegevens die door een andere lidstaat zijn ingevoerd, uit hun N.SIS of uit CS-SIS naar andere nationale gegevensbestanden.

3. De in lid 2 bedoelde technische kopieën die leiden tot de aanleg van offline gegevensbanken, worden maximaal 48 uur bewaard. Deze duur kan in noodsituaties worden verlengd, totdat de noodsituatie is beëindigd.

Ongeacht de eerste alinea, zijn technische kopieën die leiden tot de aanleg van offline gegevensbanken voor gebruik door voor de visumverlening bevoegde autoriteiten, niet toegestaan, tenzij het gaat om kopieën die uitsluitend worden gebruikt in noodsituaties als gevolg van het feit dat het netwerk gedurende meer dan 24 uren niet beschikbaar is.

De lidstaten houden een actuele inventaris van deze kopieën bij, stellen deze inventaris ter beschikking van hun nationale toezichthoudende autoriteit, en zorgen ervoor dat de bepalingen van deze verordening, met name artikel 10, op deze kopieën worden toegepast.

4. Toegang tot gegevens is slechts toegestaan binnen de grenzen van de bevoegdheden van de in artikel 29 bedoelde nationale autoriteiten, en is voorbehouden aan daartoe gemachtigde personeelsleden.

5. In het SIS opgenomen informatie kan slechts worden verwerkt voor andere doelstellingen dan die welke met de opneming ervan in het SIS werden beoogd, indien er een verband bestaat met een specifieke zaak en de verwerking noodzakelijk is ter voorkoming van een ernstige en onmiddellijke dreiging voor de openbare orde en veiligheid, om ernstige redenen die verband houden met de nationale veiligheid, dan wel ter voorkoming van een ernstig strafbaar feit. Daartoe wordt vooraf de toestemming van de signalerende lidstaat gevraagd.

6. Gegevens over persoonsdocumenten die in het kader van artikel 38, lid 2, onder j) en k), van Verordening (EU) 2018/xxx zijn opgenomen, kunnen door de in artikel 29, lid 1, onder d), van deze verordening bedoelde autoriteiten worden gebruikt in overeenstemming met het recht van de onderscheiden lidstaten.

7. Elk gebruik van gegevens dat in strijd is met de leden 1 tot en met 6, wordt naar het nationale recht van de onderscheiden lidstaten aangemerkt als oneigenlijk gebruik.

8. Iedere lidstaat verstrekt het Agentschap een lijst van zijn bevoegde autoriteiten die op grond van deze verordening gemachtigd zijn tot directe bevraging van in het SIS opgenomen gegevens, alsmede alle wijzigingen van die lijst. In de lijst wordt voor elke autoriteit vermeld welke gegevens zij voor welke doeleinden mag bevragen. Het Agentschap zorgt voor de jaarlijkse bekendmaking van deze lijst in het *Publicatieblad van de Europese Unie*.

9. Voor zover het recht van de Unie niet in bijzondere bepalingen voorziet, is het recht van de onderscheiden lidstaten van toepassing op de in hun N.SIS opgenomen gegevens.

Artikel 37
SIS-gegevens en nationale bestanden

1. Artikel 36, lid 2, laat het recht van een lidstaat onverlet om in zijn nationale bestanden SIS-gegevens te bewaren in verband waarmee op zijn grondgebied een maatregel is genomen. Deze gegevens worden maximaal drie jaar in de nationale

bestanden bewaard, tenzij in specifieke bepalingen van nationaal recht een langere bewaartermijn is vastgesteld.

2. Artikel 36, lid 2, laat het recht van een lidstaat onverlet om in zijn nationale bestanden gegevens te bewaren die deel uitmaken van een specifieke signalering die door deze lidstaat in het SIS is opgenomen.

Artikel 38
Informatie bij niet-uitvoering van een signalering

Wanneer een gevraagde maatregel niet kan worden uitgevoerd, stelt de aangezochte lidstaat de signalerende lidstaat daarvan onmiddellijk in kennis.

Artikel 39
Kwaliteit van de in het SIS verwerkte gegevens

1. Een signalerende lidstaat is verantwoordelijk voor de juistheid en actualiteit van de gegevens, alsmede voor de rechtmatige opneming van de gegevens in het SIS.

2. Alleen de signalerende lidstaat is bevoegd de door hem ingevoerde gegevens te wijzigen, aan te vullen, te corrigeren, bij te werken of te wissen.

3. Wanneer een andere dan de signalerende lidstaat aanwijzingen heeft dat een gegeven in een signalering onjuist is of onrechtmatig is opgenomen, deelt hij dit zo spoedig mogelijk, maar niet later dan tien dagen nadat hij kennis heeft genomen van de aanwijzingen, mee aan de signalerende lidstaat door middel van de uitwisseling van aanvullende informatie. De signalerende lidstaat toetst de mededeling en corrigeert of wist zo nodig het betrokken gegeven onverwijld.

4. Wanneer de lidstaten twee maanden nadat de aanwijzingen aan het licht zijn gekomen, nog geen overeenstemming hebben bereikt overeenkomstig lid 3, legt de niet-signalerende lidstaat de zaak voor aan de betrokken nationale toezichthoudende autoriteiten, die een besluit ter zake nemen.

5. De lidstaten wisselen aanvullende informatie uit, indien een klacht wordt ingediend door een persoon die stelt niet diegene te zijn die door middel van een signalering wordt opgespoord. Indien na controle blijkt dat het inderdaad twee verschillende personen betreft, wordt de klager ingelicht over de in artikel 42 bedoelde maatregelen.

6. Een lidstaat die een signalering opneemt met betrekking tot een persoon die reeds in het SIS is gesignaleerd, treft met de eerste signalerende lidstaat een regeling omtrent de opneming van de signalering. De regeling komt tot stand op basis van de uitwisseling van aanvullende informatie.

Artikel 40
Veiligheidsincidenten

1. Elke gebeurtenis die gevolgen heeft of kan hebben voor de veiligheid van het SIS en het SIS schade of verlies kan toebrengen, wordt beschouwd als een veiligheidsincident, met name wanneer toegang tot gegevens kan zijn verkregen of

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

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

3. De lidstaten melden veiligheidsincidenten aan de Commissie, het Agentschap en de Europese Toezichthouder voor gegevensbescherming. Het Agentschap meldt veiligheidsincidenten aan de Commissie en de Europese Toezichthouder voor gegevensbescherming.

4. Informatie over een veiligheidsincident dat gevolgen heeft of kan hebben voor de werking van het SIS in een lidstaat of bij het Agentschap, of voor de beschikbaarheid, de integriteit en de vertrouwelijkheid van de gegevens die door andere lidstaten zijn opgenomen of toegezonden, wordt verstrekt aan de lidstaten en gerapporteerd in overeenstemming met het door het Agentschap voorgelegde incidentenbeheerplan.

Artikel 41
Onderscheid tussen personen met vergelijkbare kenmerken

Indien bij de opneming van een nieuwe signalering blijkt dat in het SIS reeds een persoon met dezelfde identiteitsbeschrijving gesignaleerd is, is de volgende procedure van toepassing:

(a) het Sirene-bureau neemt contact op met de verzoekende autoriteit om zich ervan te vergewissen of de signalering dezelfde persoon betreft;

(b) indien uit de kruiscontrole blijkt dat de in de nieuwe signalering bedoelde persoon en de reeds in het SIS gesignaleerde persoon inderdaad dezelfde persoon zijn, volgt het Sirene-bureau de in artikel 39, lid 6, bedoelde procedure voor opneming van meervoudige signaleringen. Indien uit de controle blijkt dat het om twee verschillende personen gaat, bekrachtigt het Sirene-bureau het verzoek om opneming van de nieuwe signalering en voegt het de nodige elementen toe om verkeerde identificatie te voorkomen.

Artikel 42
Extra gegevens om gevallen van misbruik van identiteit te behandelen

1. Wanneer de daadwerkelijk met de signalering beoogde persoon kan worden verward met een persoon wiens identiteit is misbruikt, voegt de signalerende lidstaat in de signalering gegevens betreffende de laatstbedoelde persoon toe, voor zover deze uitdrukkelijk daarmee instemt, om nadelige gevolgen van verkeerde identificatie te voorkomen.

2. De gegevens betreffende een persoon wiens identiteit is misbruikt, worden uitsluitend gebruikt om:

(a) de bevoegde autoriteit in staat te stellen de persoon wiens identiteit is misbruikt, te onderscheiden van de daadwerkelijk met de signalering beoogde persoon;

(b) de persoon wiens identiteit is misbruikt, in staat te stellen zijn identiteit te bewijzen en aan te tonen dat zijn identiteit is misbruikt.

3. Voor de toepassing van dit artikel mogen slechts de volgende persoonsgegevens in het SIS worden opgenomen en verwerkt:

(a) achternaam/achternamen;

(b) voornaam/voornamen;

(c) naam/namen bij geboorte;

(d) voorheen gebruikte namen, en aliassen, zo mogelijk afzonderlijk;

(e) bijzondere, onveranderlijke objectieve fysieke kenmerken;

(f) geboorteplaats;

(g) geboortedatum;

(h) geslacht;

(i) gezichtsopnamen;

(j) vingerafdrukken;

(k) nationaliteit(en);

(l) categorie van het identiteitsdocument;

(m) land van afgifte van het identiteitsdocument;

(n) nummer(s) van het identiteitsdocument;

(o) datum van afgifte van het identiteitsdocument;

(p) adres van het slachtoffer;

(q) naam van de vader van het slachtoffer;

(r) naam van de moeder van het slachtoffer.

4. De technische voorschriften voor het opnemen en verder verwerken van de in lid 3 bedoelde gegevens worden door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure vastgesteld en ontwikkeld.

5. De in lid 3 bedoelde gegevens worden gewist op hetzelfde moment als de overeenkomstige signalering, of eerder indien de betrokken persoon daarom verzoekt.

6. Alleen de autoriteiten met toegangsrecht tot de overeenkomstige signalering hebben toegang tot de in lid 3 bedoelde gegevens. Zij hebben uitsluitend toegang ter voorkoming van verkeerde identificatie.

Artikel 43
Koppelingen tussen signaleringen

1. Een lidstaat kan de door hem in het SIS opgenomen signaleringen koppelen. Door een dergelijke koppeling worden twee of meer signaleringen met elkaar in verbinding gebracht.

2. De koppeling heeft geen gevolgen voor de in de gekoppelde signaleringen gevraagde specifieke maatregel of voor de bewaartermijn van de gekoppelde signaleringen.

3. De koppeling heeft geen gevolgen voor de in deze verordening vastgestelde toegangsrechten. Autoriteiten die geen toegangsrecht hebben tot bepaalde categorieën signaleringen, hebben geen inzage in koppelingen naar signaleringen waartoe zij geen toegang hebben.

4. Een lidstaat koppelt signaleringen wanneer daartoe een duidelijke operationele noodzaak bestaat.

5. Wanneer een lidstaat een door een andere lidstaat aangebrachte koppeling tussen signaleringen in strijd acht met zijn nationale recht of internationale verplichtingen, kan hij de nodige maatregelen nemen om ervoor te zorgen dat de koppeling niet toegankelijk is vanaf zijn grondgebied of voor de eigen, buiten zijn grondgebied gevestigde autoriteiten.

6. De technische voorschriften voor het koppelen van signaleringen worden vastgesteld en ontwikkeld overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure.

Artikel 44
Doel en bewaartermijn van aanvullende informatie

1. Ter ondersteuning van de uitwisseling van aanvullende informatie houden de lidstaten in het Sirene-bureau verwijzingen naar de aan signaleringen ten grondslag liggende beslissingen bij.

2. Persoonsgegevens die het Sirene-bureau naar aanleiding van de informatie-uitwisseling in bestanden heeft opgeslagen, worden niet langer bewaard dan nodig is om het doel te bereiken waarvoor zij werden verstrekt. Zij worden in ieder geval gewist uiterlijk één jaar nadat de betrokken signalering uit het SIS is gewist.

3. Lid 2 laat het recht van een lidstaat onverlet om in nationale bestanden gegevens te bewaren over een specifieke signalering die hij heeft uitgevaardigd, of over een signalering in verband waarmee op zijn grondgebied een maatregel is uitgevoerd. De periode gedurende welke dergelijke gegevens in die bestanden mogen worden bewaard, wordt geregeld door het nationale recht.

Artikel 45
Doorgifte van persoonsgegevens aan derden

De overeenkomstig deze verordening in het SIS verwerkte gegevens en de desbetreffende aanvullende informatie worden niet doorgegeven aan of ter beschikking gesteld van derde landen of internationale organisaties.

HOOFDSTUK IX

GEGEVENSBESCHERMING

Artikel 46
Toepasselijke wetgeving

1. Wanneer het Agentschap in het kader van deze verordening persoonsgegevens verwerkt, is Verordening (EG) nr. 45/2001 van toepassing.

2. Wanneer de in artikel 29 van deze verordening bedoelde autoriteiten in het kader van deze verordening persoonsgegevens verwerken, is Verordening (EU) 2016/679 van toepassing, tenzij de nationale bepalingen tot omzetting van Richtlijn (EU) 2016/680 van toepassing zijn.

3. De nationale bepalingen tot omzetting van Richtlijn (EU) 2016/680 zijn van toepassing op de verwerking van gegevens door bevoegde nationale autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van bedreigingen van de openbare veiligheid.

Artikel 47
Recht op inzage in gegevens, rectificatie van onjuiste gegevens en wissing van onrechtmatig opgeslagen gegevens

1. Het recht van betrokkenen op inzage in hen betreffende, in het SIS opgenomen gegevens en op rectificatie en wissing van deze gegevens wordt uitgeoefend overeenkomstig het recht van de lidstaat bij welke zij een beroep op dit recht doen.

2. Voor zover het nationale recht in die mogelijkheid voorziet, beslist de nationale toezichthoudende autoriteit of, en zo ja, met welke middelen informatie wordt meegedeeld.

3. Een andere dan de signalerende lidstaat mag slechts informatie over dergelijke gegevens meedelen indien hij de signalerende lidstaat vooraf de gelegenheid heeft geboden dienaangaande een standpunt te bepalen. Dit geschiedt door middel van de uitwisseling van aanvullende informatie.

4. De lidstaten besluiten overeenkomstig hun nationale recht geen of slechts gedeeltelijke informatie aan de betrokkene mee te delen, voor zover en zolang die volledige of gedeeltelijke beperking in een democratische samenleving, met inachtneming van de grondrechten en legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

   (a) belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen;

(b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

(c) de openbare veiligheid te beschermen;

(d) de nationale veiligheid te beschermen;

(e) de rechten en vrijheden van anderen te beschermen.

5. De betrokkene wordt zo spoedig mogelijk op de hoogte gesteld, en in elk geval binnen 60 dagen vanaf de datum waarop hij om inzage heeft verzocht, of binnen een kortere termijn indien het nationale recht in die mogelijkheid voorziet.

6. De betrokkene wordt zo spoedig mogelijk op de hoogte gesteld van het gevolg dat wordt gegeven aan de uitoefening van zijn recht op rectificatie of wissing van gegevens, en in elk geval binnen drie maanden vanaf de datum waarop hij om rectificatie of wissing heeft verzocht, of binnen een kortere termijn indien het nationale recht in die mogelijkheid voorziet.

Artikel 48
Recht op informatie

1. Aan overeenkomstig deze verordening gesignaleerde onderdanen van derde landen wordt overeenkomstig de artikelen 10 en 11 van Richtlijn 95/46/EG informatie verstrekt. Deze informatie wordt schriftelijk verstrekt en gaat vergezeld van een afschrift van of verwijzing naar de aan de in artikel 24, lid 1, bedoelde nationale beslissing die aan de signalering ten grondslag ligt.

2. Deze informatie wordt echter niet verstrekt:

(a) indien

i) de persoonsgegevens niet bij de betrokken onderdaan van een derde land zijn verkregen,

en

ii) de verstrekking van de informatie onmogelijk blijkt of onevenredig veel moeite zou kosten;

(b) indien de betrokken onderdaan van een derde land reeds over deze informatie beschikt;

(c) indien het nationale recht voorziet in een beperking van het recht op informatie, met name ter vrijwaring van de nationale veiligheid, de landsverdediging, de openbare veiligheid, dan wel met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten.

Artikel 49
Rechtsmiddelen

1. Eenieder heeft het recht om naar aanleiding van een hem betreffende signalering bij de naar het recht van elke lidstaat bevoegde rechter of instantie beroep in te stellen met het oog op inzage, rectificatie, wissing of schadevergoeding in verband met de signalering.

2. De lidstaten verbinden zich ertoe onherroepelijke beslissingen van de in lid 1 van dit artikel bedoelde rechter of instantie wederzijds ten uitvoer te leggen, onverminderd het bepaalde in artikel 53.

3. Met het oog op een samenhangend overzicht van de toegepaste rechtsmiddelen wordt de nationale toezichthoudende autoriteiten verzocht een standaard statistisch systeem te ontwikkelen om jaarlijks verslag uit te brengen over:

   (a) het aantal inzageverzoeken van betrokkenen dat bij de verwerkingsverantwoordelijke is ingediend, en het aantal gevallen waarin inzage in de gegevens is gegeven;

   (b) het aantal inzageverzoeken van betrokkenen dat bij de nationale toezichthoudende autoriteit is ingediend, en het aantal gevallen waarin inzage in de gegevens is gegeven;

   (c) het aantal verzoeken om rectificatie van onjuiste gegevens en wissing van onrechtmatig opgeslagen gegevens dat bij de verwerkingsverantwoordelijke is ingediend, en het aantal gevallen waarin de gegevens zijn gerectificeerd of gewist;

   (d) het aantal verzoeken om rectificatie van onjuiste gegevens en wissing van onrechtmatig opgeslagen gegevens dat bij de nationale toezichthoudende autoriteit is ingediend;

   (e) het aantal bij de rechter aanhangig gemaakte zaken;

   (f) het aantal zaken waarin de rechter de verzoeker in het gelijk heeft gesteld met betrekking tot een aspect van de zaak;

   (g) opmerkingen over zaken waarin ten aanzien van een door de signalerende lidstaat gecreëerde signalering een definitieve beslissing door een rechter of instantie van andere lidstaten is vastgesteld die wederzijds is erkend.

   De verslagen van de nationale toezichthoudende autoriteiten worden doorgestuurd naar het in artikel 52 bedoelde samenwerkingsmechanisme.

Artikel 50
Toezicht op N.SIS

1. De lidstaten zien erop toe dat hun aangewezen nationale toezichthoudende autoriteiten waaraan de bevoegdheden als bedoeld in hoofdstuk VI van Richtlijn (EU) 2016/680 of hoofdstuk VI van Verordening (EU) 2016/679 zijn toegekend, de rechtmatigheid van de verwerking van SIS-persoonsgegevens op hun grondgebied,

de doorgifte van SIS-gegevens vanuit dat grondgebied en de uitwisseling en verdere verwerking van aanvullende informatie op onafhankelijke wijze monitoren.

2. De nationale toezichthoudende autoriteiten zien erop toe dat ten minste om de vier jaar een audit van de gegevensverwerking in N.SIS wordt uitgevoerd overeenkomstig internationale auditnormen. De audit wordt uitgevoerd door de nationale toezichthoudende autoriteiten of wordt door de nationale toezichthoudende autoriteiten rechtstreeks uitbesteed aan een onafhankelijke auditor op het gebied van gegevensbescherming. De onafhankelijke auditor blijft te allen tijde onder de controle en de verantwoordelijkheid van de nationale toezichthoudende autoriteiten staan.

3. De lidstaten zien erop toe dat de nationale toezichthoudende autoriteiten over voldoende middelen beschikken om hun taken uit hoofde van deze verordening te kunnen vervullen.

Artikel 51
Toezicht op het Agentschap

1. De Europese Toezichthouder voor gegevensbescherming ziet erop toe dat de activiteiten van het Agentschap op het gebied van de verwerking van persoonsgegevens in overeenstemming zijn met deze verordening. De taken en bevoegdheden als bedoeld in de artikelen 46 en 47 van Verordening (EG) nr. 45/2001 zijn van overeenkomstige toepassing.

2. De Europese Toezichthouder voor gegevensbescherming ziet erop toe dat ten minste om de vier jaar een audit van de activiteiten van het Agentschap op het gebied van de verwerking van persoonsgegevens wordt uitgevoerd overeenkomstig internationale auditnormen. Het auditrapport wordt toegezonden aan het Europees Parlement, de Raad, het Agentschap, de Commissie en de nationale toezichthoudende autoriteiten. Voordat het rapport wordt aangenomen, wordt het Agentschap in de gelegenheid gesteld opmerkingen te maken.

Artikel 52
Samenwerking tussen de nationale toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming

1. De nationale toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming werken actief samen en zorgen voor een gecoördineerd toezicht op het SIS, binnen de grenzen van hun respectieve bevoegdheden en verantwoordelijkheden.

2. Zij wisselen, binnen de grenzen van hun respectieve bevoegdheden, relevante informatie uit, staan elkaar bij in de uitvoering van audits en inspecties, behandelen problemen met de uitlegging of toepassing van deze verordening en andere toepasselijke rechtshandelingen van de Unie, behandelen problemen met de uitoefening van het onafhankelijke toezicht of bij de uitoefening van de rechten van de betrokkenen, formuleren geharmoniseerde voorstellen voor gemeenschappelijke oplossingen voor problemen, en vestigen de aandacht op gegevensbeschermingsrechten wanneer dat nodig is.

3. Voor de in lid 2 neergelegde doeleinden komen de nationale toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming ten minste tweemaal per jaar bijeen in het kader van het Europees Comité voor gegevensbescherming dat is ingesteld bij Verordening (EU) 2016/679. De kosten en logistieke ondersteuning van deze bijeenkomsten zijn voor rekening van het bij Verordening (EU) 2016/679 ingestelde comité. Tijdens de eerste bijeenkomst wordt een reglement van orde vastgesteld. Indien nodig worden in onderling overleg andere werkmethoden vastgesteld.

4. Om de twee jaar zendt het bij Verordening (EU) 2016/679 ingestelde comité een gezamenlijk activiteitenverslag over het gecoördineerde toezicht toe aan het Europees Parlement, de Raad en de Commissie.

HOOFDSTUK X

AANSPRAKELIJKHEID

Artikel 53
Aansprakelijkheid

1. Elke lidstaat is aansprakelijk voor schade die door het gebruik van N.SIS aan een persoon is toegebracht. Dit geldt tevens wanneer de schade is toegebracht door de signalerende lidstaat doordat deze feitelijk onjuiste gegevens heeft aangeleverd of gegevens onrechtmatig heeft opgeslagen.

2. Wanneer de gedaagde lidstaat niet de signalerende lidstaat is, betaalt laatstgenoemde desgevraagd aan eerstgenoemde een vergoeding ter hoogte van de uitgekeerde schadevergoeding, tenzij de om vergoeding verzoekende lidstaat de gegevens in strijd met deze verordening heeft gebruikt.

3. Een lidstaat die zijn verplichtingen uit hoofde van deze verordening niet is nagekomen en daardoor schade aan het SIS heeft toegebracht, is aansprakelijk voor die schade, tenzij en voor zover het Agentschap of één of meer andere aan het SIS deelnemende lidstaten hebben nagelaten redelijke stappen te ondernemen om het ontstaan van de schade te voorkomen of de omvang ervan zo veel mogelijk te beperken.

HOOFDSTUK XI

SLOTBEPALINGEN

Artikel 54
Monitoring en statistieken

1. Het Agentschap zorgt ervoor dat er procedures voorhanden zijn om de resultaten, de kosteneffectiviteit, de beveiliging en de kwaliteit van de dienstverlening van het SIS te toetsen aan de doelstellingen.

2. Met het oog op het technische onderhoud en de opstelling van verslagen en statistieken heeft het Agentschap toegang tot de daartoe vereiste informatie over de in het centrale SIS verrichte verwerkingen.

3. Het Agentschap stelt dagelijkse, maandelijkse en jaarlijkse algemene en naar lidstaat uitgesplitste statistieken op over het aantal records per signaleringscategorie, het aantal treffers per signaleringscategorie, het aantal keren dat het SIS is doorzocht en het aantal keren dat toegang tot het SIS is verkregen om een signalering in te voeren, bij te werken of te wissen, inclusief statistieken over de in artikel 26 bedoelde overlegprocedure. De opgestelde statistieken bevatten geen persoonsgegevens. Het statistische jaarverslag wordt openbaar gemaakt.

4. De lidstaten, Europol en het Europees Grens- en kustwachtagentschap verstrekken het Agentschap en de Commissie de informatie die nodig is om de in de leden 7 en 8 bedoelde verslagen op te stellen.

5. Het Agentschap verstrekt alle statistische verslagen die het opstelt aan de lidstaten, de Commissie, Europol en het Europees Grens- en kustwachtagentschap. Om de tenuitvoerlegging van rechtshandelingen van de Unie te monitoren, kan de Commissie het Agentschap vragen om, op gezette tijden of ad hoc, aanvullende gerichte statistische verslagen te verstrekken over de prestaties of het gebruik van de SIS- en Sirene-communicatie.

6. Voor de toepassing van de leden 3, 4 en 5 van dit artikel en artikel 15, lid 5, wordt door het Agentschap op zijn technische locaties een centraal register opgezet, geïmplementeerd en gehost, met daarin de in lid 3 van dit artikel en in artikel 15, lid 5, bedoelde gegevens, aan de hand waarvan geen personen kunnen worden geïdentificeerd en aan de hand waarvan de Commissie en de in lid 5 bedoelde agentschappen verslagen en statistieken op maat kunnen verkrijgen. Het Agentschap verleent de lidstaten, de Commissie, Europol en het Europees Grens- en kustwachtagentschap uitsluitend voor het opstellen van verslagen en statistieken toegang tot het centrale register, door middel van beveiligde toegang via de communicatie-infrastructuur, toegangscontrole en specifieke gebruikersprofielen.

   Uitvoerige bepalingen voor de werking van het centrale register en de voorschriften voor gegevensbescherming en -beveiliging die voor het register gelden, worden door middel van uitvoeringsmaatregelen overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure vastgesteld en ontwikkeld.

7. Twee jaar na de ingebruikneming van het SIS, en vervolgens om de twee jaar, legt het Agentschap aan het Europees Parlement en de Raad een verslag voor over de technische werking van het centrale SIS en de communicatie-infrastructuur, alsmede over de beveiliging ervan, en over de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten.

8. Drie jaar na de ingebruikneming van het SIS, en vervolgens om de vier jaar, stelt de Commissie een algemene evaluatie op van het centrale SIS en van de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten. In deze algemene evaluatie worden de bereikte resultaten getoetst aan de doelstellingen, wordt nagegaan of de uitgangspunten nog gelden, worden de toepassing van deze verordening ten aanzien van het centrale SIS en de beveiliging van het centrale SIS beoordeeld en wordt bekeken welke gevolgen een en ander heeft voor toekomstige werkzaamheden. De Commissie legt deze evaluatie voor aan het Europees Parlement en de Raad.

Artikel 55
Comitéprocedure

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

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

Artikel 56

Wijzigingen van Verordening (EU) nr. 515/2014

Verordening (EU) nr. 515/2014[74] wordt als volgt gewijzigd:

In artikel 6 wordt het volgende lid 6 toegevoegd:

"6. Tijdens de ontwikkelingsfase ontvangen de lidstaten naast hun basistoewijzing een extra toewijzing van 36,8 miljoen EUR in de vorm van een forfaitair bedrag dat zij volledig gebruiken om de nationale SIS-systemen snel en doeltreffend af te stemmen op de implementatie van het centrale SIS, zoals voorgeschreven in Verordening (EU) 2018/…[*] en Verordening (EU) 2018/…[**].

[*] Verordening betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken (PB …).

[**] Verordening (EU) 2018/... betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles (PB …).".

---

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

Artikel 57
Intrekking

Verordening (EG) nr. 1987/2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II).

Besluit 2010/261/EU van de Commissie van 4 mei 2010 betreffende het beveiligingsplan voor het centrale SIS II en de communicatie-infrastructuur[75].

Artikel 25 van de Schengenuitvoeringsovereenkomst[76].

Artikel 58
Inwerkingtreding en toepasselijkheid

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

2. Zij is van toepassing met ingang van de datum die door de Commissie wordt vastgesteld nadat:

   (a) de vereiste uitvoeringsmaatregelen zijn aangenomen;

   (b) de lidstaten aan de Commissie hebben meegedeeld dat de nodige technische en juridische maatregelen zijn genomen om SIS-gegevens te verwerken en aanvullende informatie uit te wisselen op grond van deze verordening;

   (c) het Agentschap aan de Commissie heeft meegedeeld dat tests van CS-SIS en de interactie tussen CS-SIS en N.SIS zijn afgerond.

3. Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat overeenkomstig het Verdrag betreffende de werking van de Europese Unie.

Gedaan te Brussel,

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

[75] Besluit 2010/261/EU van de Commissie van 4 mei 2010 betreffende het beveiligingsplan voor het centrale SIS II en de communicatie-infrastructuur (PB L 112 van 5.5.2010, blz. 31).

[76] PB L 239 van 22.9.2000, blz. 19.

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur

1.3. Aard van het voorstel/initiatief

1.4. Doelstelling(en)

1.5. Motivering van het voorstel/initiatief

1.6. Duur en financiële gevolgen

1.7. Beheersvorm(en)

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesysteem

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

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

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

3.2.2. Geraamde gevolgen voor de beleidskredieten

3.2.3. Geraamde gevolgen voor de administratieve kredieten

3.2.4. Verenigbaarheid met het huidig meerjarig financieel kader

3.2.5. Bijdragen van derden

3.3. Geraamde gevolgen voor de ontvangsten

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van Verordening (EU) nr. 515/2014 en tot intrekking van Verordening (EG) nr. 1987/2006.

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur[77]

Beleidsterrein: Migratie en Binnenlandse zaken (titel 18)

1.3. Aard van het voorstel/initiatief

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

☐ Het voorstel/initiatief betreft **een nieuwe actie na een proefproject/een voorbereidende actie**[78]

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

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

1.4. Doelstelling(en)

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

Doelstelling — "Naar een nieuw migratiebeleid"

De Commissie heeft herhaaldelijk gewezen op de noodzaak de rechtsgrondslag van het SIS te herzien om het hoofd te kunnen bieden aan nieuwe uitdagingen op het gebied van veiligheid en migratie. In de "Europese migratieagenda"[79] stelt de Commissie in dit verband dat een efficiënter beheer van onze grenzen ook inhoudt dat beter gebruik wordt gemaakt van de mogelijkheden die IT-systemen en -technologieën bieden. In de "Europese veiligheidsagenda"[80] kondigt de Commissie haar voornemen aan om het SIS in 2015-2016 te evalueren en na te gaan welke mogelijkheden er zijn om de lidstaten te helpen bij de tenuitvoerlegging van een op nationaal niveau opgelegd reisverbod. In het "EU-actieplan tegen migrantensmokkel"[81] geeft de Commissie aan te overwegen de autoriteiten van de

---

77 ABM: activity-based management; ABB: activity-based budgeting.
78 In de zin van artikel 54, lid 2, onder a) of b), van het Financieel Reglement.
79 COM(2015) 240 final.
80 COM(2015) 185 final.
81 COM(2015) 285 final.

lidstaten ertoe te verplichten alle inreisverboden in het SIS te registreren, zodat deze in de hele EU kunnen worden gehandhaafd. Voorts kondigt de Commissie in het actieplan aan te zullen onderzoeken of het mogelijk en evenredig is om de terugkeerbesluiten van de lidstaten in het SIS te registreren, zodat kan worden nagegaan of een andere lidstaat ten aanzien van een aangehouden irreguliere migrant een terugkeerbesluit heeft uitgevaardigd. Ten slotte benadrukt de Commissie in de mededeling over "slimmere en betere informatiesystemen voor grenzen en veiligheid"[82] dat zij mogelijke aanvullende functies van het SIS onderzoekt met het oog op het indienen van voorstellen tot herziening van de rechtsgrondslag van het systeem.

Als gevolg van de algemene evaluatie van het systeem en volledig in overeenstemming met de meerjarendoelstellingen van de Commissie als opgenomen in bovengenoemde mededelingen en het strategisch plan 2016-2020 van DG Migratie en Binnenlandse Zaken[83] wordt met dit voorstel beoogd de structuur, de werking en het gebruik van het Schengeninformatiesysteem op het gebied van grenscontroles te hervormen.

1.4.2. Specifieke doelstelling(en) en betrokken ABM/ABB-activiteit(en)

Specifieke doelstelling nr.

Managementplan 2017 van DG Migratie en Binnenlandse Zaken — Specifieke doelstelling nr. 1.2:

Doeltreffend grensbeheer – levens redden en de EU-buitengrenzen beveiligen

Betrokken ABM/ABB-activiteit(en)

Hoofdstuk 18 02 — Interne veiligheid

82 COM(2016) 205 final.

83 Ares(2016)2231546 – 12.5.2016.

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

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

Het beleid beoogt met name:

1) bij te dragen aan een hoog niveau van veiligheid in de ruimte van vrijheid, veiligheid en recht van de EU;

2) de doeltreffendheid en efficiëntie van het grenstoezicht te versterken.

In de algemene evaluatie van het SIS, die DG HOME in 2015-2016 heeft uitgevoerd, wordt aanbevolen technische verbeteringen in het systeem aan te brengen en de nationale procedures om weigeringen met het oog op toegang en verblijf te beheren, te harmoniseren. Zo is in de bestaande SIS II-verordening alleen maar de mogelijkheid, maar niet de verplichting, opgenomen om signaleringen met het oog op weigering van toegang en verblijf in het systeem in te voeren. Sommige lidstaten voeren systematisch alle inreisverboden in het SIS in, terwijl andere dat niet doen. Het huidige voorstel zal bijdragen tot het bereiken van een hoger niveau van harmonisatie op dit gebied door de verplichting op te leggen om alle inreisverboden volgens bepaalde gemeenschappelijke regels in het SIS in te voeren en de achterliggende reden voor de signalering op te geven.

Voorts worden maatregelen voorgesteld die tegemoetkomen aan operationele en technische behoeften van de eindgebruikers. Met name zullen grenswachters dankzij de nieuwe datavelden voor bestaande signaleringen over alle noodzakelijke gegevens beschikken om hun taken doeltreffend uit te voeren. Omdat het uitvallen van het systeem de uitvoering van het buitengrenstoezicht danig kan verstoren, wordt in het voorstel bijzondere nadruk gelegd op het belang van de ononderbroken beschikbaarheid van het SIS – wat een uitermate positief effect zal hebben op de doeltreffendheid van het grenstoezicht.

Eenmaal aangenomen en ten uitvoer gelegd zal het voorstel ook de bedrijfscontinuïteit bevorderen, aangezien de lidstaten over een volledige of gedeeltelijke nationale kopie en een back-up daarvan moeten beschikken en het systeem dus volledig functioneel en operationeel zal blijven voor de functionarissen op het terrein.

1.4.4. Resultaat- en effectindicatoren

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

Tijdens de upgrade van het systeem

Na de goedkeuring van het ontwerpvoorstel en de vaststelling van de technische specificaties zal het SIS worden geüpgraded om de nationale procedures voor het gebruik van het systeem beter te stroomlijnen, om de reikwijdte van het systeem uit te breiden door eindgebruikers meer informatie aan te reiken zodat de functionarissen die de controles verrichten, beter geïnformeerd zijn, om technische wijzigingen voor een betere beveiliging aan te brengen en om de administratieve belasting te helpen reduceren. eu-LISA wordt belast met de coördinatie van het projectbeheer voor het upgraden van het systeem. eu-LISA zal een projectbeheerstructuur en een tijdschema

met ijkpunten voor de tenuitvoerlegging van de voorgestelde wijzigingen voorleggen aan de hand waarvan de Commissie de uitvoering van het voorstel van dichtbij kan monitoren.

Specifieke doelstelling — ingebruikneming van de geactualiseerde functies van het SIS in 2020.

Indicator — succesvolle afsluiting van aan de invoering van het herziene systeem voorafgaande omvattende tests.

Na de inbedrijfstelling van het systeem

eu-LISA zal er na de inbedrijfstelling voor zorgen dat er procedures voorhanden zijn om de resultaten, de kosteneffectiviteit, de beveiliging en de kwaliteit van de dienstverlening van het SIS te toetsen aan de doelstellingen. Twee jaar na de inbedrijfstelling van het SIS, en vervolgens om de twee jaar, moet eu-LISA aan het Europees Parlement en de Raad een verslag voorleggen over de technische werking van het centrale SIS en de communicatie-infrastructuur, alsmede over de beveiliging ervan, en over de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten. Voorts moet eu-LISA dagelijkse, maandelijkse en jaarlijkse algemene en naar lidstaat uitgesplitste statistieken opstellen over het aantal records per signaleringscategorie, het aantal treffers per signaleringscategorie, het aantal keren dat het SIS is doorzocht en het aantal keren dat toegang tot het SIS is verkregen om een signalering in te voeren, bij te werken of te wissen.

Drie jaar na de inbedrijfstelling van het SIS, en vervolgens om de vier jaar, stelt de Commissie een algemene evaluatie op van het centrale SIS en van de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten. In deze algemene evaluatie worden de bereikte resultaten getoetst aan de doelstellingen en wordt nagegaan of de uitgangspunten nog gelden, worden de toepassing van deze verordening ten aanzien van het centrale SIS en de beveiliging van het centrale SIS beoordeeld en wordt bekeken welke gevolgen een en ander heeft voor toekomstige werkzaamheden. De Commissie legt deze evaluatie voor aan het Europees Parlement en de Raad.

1.5. Motivering van het voorstel/initiatief

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

1. Bijdragen tot de handhaving van een hoog niveau van veiligheid in de ruimte van vrijheid, veiligheid en recht van de EU

2. De strijd tegen internationale criminaliteit, terrorisme en andere veiligheidsdreigingen intensiveren

3. Het toepassingsgebied van het SIS uitbreiden door elementen toe te voegen in signaleringen met het oog op weigering van toegang en verblijf

4. De doeltreffendheid van het grenstoezicht verbeteren

5. De efficiëntie van het werk van de grenswachters en de immigratiediensten verbeteren

6. De doeltreffendheid en de harmonisatie van de nationale procedures vergroten en de uitvoerbaarheid van inreisverboden waarborgen in het hele Schengengebied

7. Bijdragen tot de bestrijding van irreguliere migratie

1.5.2. Toegevoegde waarde van de deelname van de EU

Het SIS is de belangrijkste veiligheidsgerelateerde databank in Europa. Door het wegvallen van het toezicht aan de binnengrenzen heeft de doeltreffende bestrijding van criminaliteit en terrorisme een Europese dimensie gekregen. Tegen die achtergrond is het SIS een onontbeerlijk instrument voor de ondersteuning van het buitengrenstoezicht en van de controles op irreguliere migranten die op het nationale grondgebied worden aangetroffen. Dit voorstel heeft tot doel technische verbeteringen aan te brengen om de doelmatigheid en de doeltreffendheid van het systeem te versterken en het gebruik ervan in de deelnemende lidstaten te harmoniseren. Omdat deze doelstellingen een grensoverschrijdende dimensie hebben en omdat het waarborgen van een doeltreffende uitwisseling van informatie ter bestrijding van steeds weer andersoortige dreigingen met bepaalde uitdagingen gepaard gaat, is de EU het beste geplaatst om oplossingen aan te dragen. De doelstellingen – verbetering van de doeltreffendheid en het geharmoniseerde gebruik van het SIS, verhoging van het volume, de kwaliteit en de snelheid van de informatie-uitwisseling via een gecentraliseerd, grootschalig informatiesysteem dat wordt beheerd door een regelgevend agentschap (eu-LISA) – zijn van dien aard dat ze niet door de lidstaten alleen kunnen worden bereikt en een optreden op EU-niveau vereisen. Als deze problemen niet worden aangepakt en het SIS blijft functioneren volgens de huidige regels, gaat men voorbij aan de mogelijkheden die bij de evaluatie van het systeem en het gebruik ervan door de lidstaten naar voren komen om de doeltreffendheid en de toegevoegde EU-waarde van het SIS te optimaliseren.

Alleen al in 2015 hebben de nationale autoriteiten het SIS bijna 2,9 miljard keer bevraagd en meer dan 1,8 miljoen aanvullende informatie-elementen uitgewisseld – een duidelijk bewijs van de cruciale bijdrage van het systeem aan het buitengrenstoezicht. Deze intensieve informatie-uitwisseling tussen de lidstaten zou er niet gekomen zijn met gedecentraliseerde oplossingen, noch zouden dezelfde resultaten zijn bereikt met een nationale aanpak. Het SIS is bovendien het meest doeltreffende instrument voor informatie-uitwisseling met het oog op terrorismebestrijding gebleken en levert een toegevoegde EU-waarde, door de nationale veiligheidsdiensten in staat te stellen op een snelle, vertrouwelijke en efficiënte manier samen te werken. De nieuwe voorstellen zullen de informatie-uitwisseling en de samenwerking tussen de grenstoezichtautoriteiten van de EU-lidstaten verder vergemakkelijken. Als een duidelijk bewijs voor de toegevoegde waarde van een aanpak op EU-niveau zullen Europol en de Europese grens- en kustwacht bovendien volledige toegang krijgen tot het systeem.

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

De belangrijkste lessen die kunnen worden getrokken uit de ontwikkeling van het Schengeninformatiesysteem van de tweede generatie:

1. De ontwikkelingsfase mag pas van start gaan nadat de technische en operationele vereisten volledig zijn gedefinieerd en nadat de achterliggende rechtsinstrumenten,

met een omschrijving van het doel, het toepassingsgebied, de functies en de technische details, definitief zijn vastgesteld.

2. De Commissie blijft, net als voorheen, regelmatig overleg plegen met de belanghebbenden, met inbegrip van de gedelegeerden van het SISVIS-comité in het kader van de comitéprocedure. In dit comité hebben vertegenwoordigers van de lidstaten zitting die bevoegd zijn voor operationele Sirene-aangelegenheden (grensoverschrijdende samenwerking met betrekking tot het SIS) en technische aangelegenheden op het gebied van ontwikkeling en onderhoud van het SIS en de betrokken Sirene-applicatie. De in deze verordening voorgestelde wijzigingen zijn uit en te na en op transparante wijze besproken in het kader van speciaal daarvoor georganiseerde bijeenkomsten en workshops. Bovendien heeft de Commissie intern een horizontale stuurgroep opgezet, met vertegenwoordigers van het secretariaat-generaal en van de directoraten-generaal Migratie en Binnenlandse Zaken, Justitie en Consumenten, Personele middelen en veiligheid, en Informatica. Deze groep monitorde het evaluatieproces en gaf sturing waar dat nodig was.

3. Ook de bevindingen van drie door de Commissie uitbestede studies zijn in het voorstel verwerkt:

– Technische beoordeling van het SIS (Kurt Salmon) – deze beoordeling legt de vinger op de belangrijkste knelpunten in de werking van het SIS, brengt de behoeften voor de toekomst in kaart en wijst vooral op de noodzaak de bedrijfscontinuïteit te optimaliseren en de algehele architectuur af te stemmen op de vereiste capaciteitsuitbreiding.

– Effectbeoordeling van mogelijke verbeteringen van de SIS II-architectuur op het gebied van ICT (Kurt Salmon) – deze studie beoordeelt de huidige kosten voor de werking van het SIS op nationaal niveau en evalueert drie mogelijke technische scenario's om het systeem te verbeteren. Alle scenario's bevatten een reeks technische voorstellen die gericht zijn op verbeteringen in het centrale systeem en de algehele architectuur.

– Studie over de haalbaarheid en de gevolgen van het opzetten, in het kader van het Schengeninformatiesysteem, van een EU-breed systeem voor het uitwisselen van gegevens over en het monitoren van de naleving van terugkeerbesluiten (PwC) – deze studie beoordeelt de haalbaarheid en de technische en operationele gevolgen van de wijzigingsvoorstellen ten behoeve van een versterkt gebruik van het SIS om de terugkeer van irreguliere migranten te bevorderen en te voorkomen dat zij het Schengengebied opnieuw binnenkomen.

1.5.4. Verenigbaarheid en eventuele synergie met andere passende instrumenten

Met dit voorstel wordt uitvoering gegeven aan de acties genoemd in de mededeling van 6 april 2016 over "Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid"[84], waarin wordt gesteld dat de EU haar IT-systemen, gegevensarchitectuur en informatie-uitwisseling op het gebied van rechtshandhaving, terrorismebestrijding en grensbeheer moet versterken en verbeteren.

[84] COM(2016) 205 final.

Bovendien strookt het voorstel met een aantal beleidsmaatregelen van de Unie op het gebied van:

a) interne veiligheid, omdat het SIS bijdraagt tot het voorkomen van de binnenkomst van onderdanen van derde landen die een bedreiging vormen voor de veiligheid;

b) gegevensbescherming, in de zin dat dit voorstel borg staat voor de bescherming van het grondrecht op eerbiediging van het privéleven van personen van wie de persoonsgegevens in het SIS worden verwerkt.

Het voorstel is ook verenigbaar met de bestaande wetgeving van de Europese Unie, meer bepaald inzake:

a) een doeltreffend terugkeerbeleid van de EU, door het verbeteren en versterken van het EU-systeem om op te sporen en te voorkomen dat onderdanen van derde landen na hun terugkeer opnieuw het Schengengebied binnenkomen. Dit zou bijdragen tot een van de voornaamste doelstellingen van de Europese migratieagenda[85]: het ontmoedigen van irreguliere migratie naar de EU; b) **de Europese grens- en kustwacht**[86], door het personeel van het Agentschap dat risicoanalyses uitvoert, alsook de leden van de Europese grens- en kustwachtteams, van de teams van personeelsleden die betrokken zijn bij met terugkeer verband houdende taken en van de ondersteuningsteams voor migratiebeheer, binnen de grenzen van hun bevoegdheid, het recht te geven op toegang tot in het SIS opgenomen gegevens en op het doorzoeken van deze gegevens;

c) **het toezicht op de buitengrenzen**, in de zin dat deze verordening de lidstaten helpt om hun deel van de EU-buitengrenzen te controleren en om het vertrouwen in de doeltreffendheid van het EU-systeem voor grensbeheer te versterken;

d) Europol, door Europol, binnen de grenzen van zijn mandaat, aanvullende rechten te verlenen op toegang tot en bevraging van in het SIS opgenomen gegevens.

Het voorstel is ook verenigbaar met toekomstige wetgeving van de Europese Unie, meer bepaald inzake:

a) **het inreis-/uitreissysteem**[87], waarin een combinatie van vingerafdrukken en gezichtsopnamen wordt voorgesteld als biometrische identificatiemiddelen voor de toepassing van het inreis-uitreissysteem (EES) – een aanpak die in dit voorstel moet worden weerspiegeld;

---

85 COM(2015) 240 final.

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

87 Voorstel voor een verordening van het Europees Parlement en de Raad tot instelling van een inreis-uitreissysteem (EES) voor de registratie van inreis- en uitreisgegevens en van gegevens over weigering van toegang ten aanzien van onderdanen van derde landen die de buitengrenzen van de Europese Unie overschrijden en tot vaststelling van de voorwaarden voor toegang tot het EES voor rechtshandhavingsdoeleinden en tot wijziging van Verordening (EG) nr. 767/2008 en Verordening (EU) nr. 1077/2011 (COM(2016) 194 final).

b) het ETIAS-systeem, waarin een grondige veiligheidsbeoordeling, inclusief een controle in het SIS, wordt voorgesteld voor onderdanen van derde landen die naar de EU willen reizen en zijn vrijgesteld van de visumplicht.

1.6. Duur en financiële gevolgen

☐ Voorstel/initiatief met een **beperkte geldigheidsduur**

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

– ☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ

☑ Voorstel/initiatief met een **onbeperkte geldigheidsduur**

– Uitvoering met een opstartperiode vanaf 2018 tot en met 2020,

– gevolgd door een volledige uitvoering.

1.7. Beheersvorm(en)[88]

☑ **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:

– ☐ derde landen of de door hen aangewezen organen;

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

– ☐ de EIB en het Europees Investeringsfonds;

– ☑ de in de artikelen 208 en 209 van het Financieel Reglement bedoelde organen;

– ☐ publiekrechtelijke organen;

– ☐ privaatrechtelijke organen met een openbaredienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

– ☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;

– ☐ personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

– *Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".*

Opmerkingen

---

[88] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

De Commissie is verantwoordelijk voor het algemene beleidsbeheer en eu-LISA is verantwoordelijk voor de ontwikkeling, de werking en het onderhoud van het systeem.

Het SIS is één integraal informatiesysteem. Bijgevolg moeten de bedragen voor de uitgaven als genoemd in twee van de voorstellen (het onderhavige en het voorstel voor een verordening betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken) worden beschouwd als één bedrag, en niet als twee afzonderlijke bedragen. De informatie over de budgettaire gevolgen van de wijzigingen die nodig zijn voor de tenuitvoerlegging van beide voorstellen, is gebundeld in één financieel memorandum.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

De Commissie, de lidstaten en het Agentschap zullen het gebruik van het SIS op gezette tijden evalueren en monitoren om ervoor te zorgen dat het systeem doeltreffend en efficiënt blijft functioneren. Voor de uitvoering van de voorgestelde technische en operationele maatregelen zal de Commissie worden bijgestaan door het SISVIS-comité.

In artikel 54, leden 7 en 8, van het verordeningsvoorstel is bovendien een procedure voor regelmatige evaluatie en herziening vastgelegd.

eu-LISA moet om de twee jaar verslag uitbrengen aan het Europees Parlement en de Raad over de technische werking – inclusief beveiliging – van het SIS, de communicatie-infrastructuur ter ondersteuning van het SIS, en de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten.

Voorts dient de Commissie om de vier jaar een algemene evaluatie van het SIS en de uitwisseling van informatie tussen de lidstaten op te stellen, die zij moet voorleggen aan het Parlement en de Raad. In deze evaluatie wordt nagegaan:

a) hoe de bereikte resultaten zich verhouden tot de doelstellingen;

b) of de uitgangspunten voor het systeem nog gelden;

c) hoe de verordening wordt toegepast op het centrale systeem;

d) hoe het staat met de beveiliging van het centrale systeem;

e) welke de gevolgen zijn voor de toekomstige werking van het systeem.

eu-LISA krijgt nu ook tot taak dagelijkse, maandelijkse en jaarlijkse statistieken over het gebruik van het SIS in te dienen, wat ervoor zorgt dat niet alleen het systeem zelf continu wordt gemonitord, maar ook de mate waarin het voldoet aan de beoogde doelstellingen.

2.2 Beheers- en controlesysteem

2.2.1. Mogelijke risico's

De volgende risicofactoren zijn vastgesteld:

1. eu-LISA zal de ontwikkelingstaken in het kader van dit voorstel moeten combineren met werkzaamheden die al aan de gang zijn (de invoering van AFIS in het SIS) of nog op stapel staan (inreis-uitreissysteem, ETIAS, upgrade van Eurodac). Het beheren van deze combinatie kan problemen veroorzaken, die echter ten dele kunnen worden opgevangen door eu-LISA voldoende personeel en middelen ter beschikking te stellen en door het beheer in handen te laten van de MWO-contractant (Maintenance in Working Order).

2. Problemen voor de lidstaten

2.1 Deze problemen zijn vooral van financiële aard. Zo wordt voorgesteld om de ontwikkeling van een gedeeltelijke nationale kopie in elk N.SIS verplicht te stellen. Lidstaten die er nog geen hebben ontwikkeld, zullen hier dus in moeten investeren. Evenzo moet het Interface Control Document op nationaal niveau integraal ten uitvoer worden gelegd. Lidstaten die dit nog niet hebben gedaan, moeten hiervoor middelen uittrekken in de begroting van de betrokken ministeries. Dit risico kan deels worden opgevangen met EU-financiering, bijvoorbeeld uit het onderdeel "Grenzen" van het Fonds voor interne veiligheid (ISF).

2.2 Besprekingen met de lidstaten over het afstemmen van de nationale systemen op de centrale vereisten kunnen leiden tot vertragingen bij de ontwikkeling. Dit risico kan deels worden opgevangen door vroegtijdig een beroep te doen op de lidstaten zodat tijdig maatregelen kunnen worden genomen.

2.2.2. Informatie over het ingestelde systeem voor interne controle

eu-LISA is verantwoordelijk voor de centrale onderdelen van het SIS. Om het gebruik van het SIS voor het analyseren van trends op het gebied van migratiedruk, grensbeheer en strafbare feiten beter te monitoren, moet het Agentschap een geavanceerde capaciteit kunnen ontwikkelen voor statistische rapportage aan de lidstaten en de Commissie.

De rekeningen van het Agentschap worden ter goedkeuring voorgelegd aan de Rekenkamer en worden onderworpen aan de kwijtingsprocedure. De Interne Auditdienst van de Commissie zal de audits uitvoeren in samenwerking met de interne auditor van het Agentschap.

2.2.3. Raming van de kosten en baten van de controles en beoordeling van het verwachte foutenrisico

n.v.t.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen.

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

1. Met het oog op de bestrijding van fraude, corruptie en andere onwettige activiteiten is Verordening (EG) nr. 1073/1999 van toepassing.

2. Het Agentschap treedt toe tot het Interinstitutioneel Akkoord betreffende de interne onderzoeken verricht door het Europees Bureau voor fraudebestrijding (OLAF) en stelt onverwijld de dienovereenkomstige voorschriften vast, die op alle personeelsleden van het Agentschap van toepassing zijn.

3. In de financieringsbesluiten en de uitvoeringsovereenkomsten en -instrumenten die uit die besluiten voortvloeien, wordt uitdrukkelijk bepaald dat de Rekenkamer en OLAF, indien nodig, tot controle ter plaatse kunnen overgaan bij de begunstigden

van de middelen van het Agentschap en bij de tussenpersonen die deze middelen verdelen.

Overeenkomstig deze bepaling heeft de raad van bestuur van het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht op 28 juni 2012 een besluit vastgesteld over de voorwaarden voor interne onderzoeken in verband met het voorkomen van fraude, corruptie en elke andere onwettige activiteit waardoor de financiële belangen van de Unie worden geschaad.

De strategie voor fraudepreventie en -opsporing van DG HOME zal van toepassing zijn.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

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

- Bestaande begrotingsonderdelen

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen.

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgaven	Bijdrage			
	[Rubriek 3 – Veiligheid en burgerschap	GK/NGK[89].	van EVA-landen[90]	van kandidaat-lidstaten[91]	van derde landen	in de zin van artikel 21, lid 2, onder b), van het Financieel Reglement.
	18.0208 – Schengeninformatiesysteem	Gespl.	NEE	NEE	JA	NEE
	18.020101 – Steun voor grensbeheer en een gemeenschappelijk visumbeleid om legitiem reizen te vergemakkelijken	Gespl.	NEE	NEE	JA	NEE
	18.0207 – Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA)	Gespl.	NEE	NEE	JA	NEE

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

90 EVA: Europese Vrijhandelsassociatie.

91 Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaat-lidstaten van de Westelijke Balkan.

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

Rubriek van het meerjarig financieel kader	3	Veiligheid en burgerschap

DG HOME			Jaar **2018**	Jaar **2019**	Jaar **2020**	**TOTAAL**
•Beleidskredieten						
18.0208 – Schengeninformatiesysteem	Vastleggingen	(1)	6,234	1,854	1,854	**9,942**
	Betalingen	(2)	6,234	1,854	1,854	**9,942**
18.020101 (Grenzen & Visum)	Vastleggingen	(1)		18,405	18,405	**36,810**
	Betalingen	(2)		18,405	18,405	**36,810**
TOTAAL kredieten voor DG HOME	Vastleggingen	=1+1a +3	6,234	20,259	20,259	**46,752**
	Betalingen	=2+2a +3	6,234	20,259	20,259	**46,752**

in miljoenen euro's (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	3	Veiligheid en burgerschap

eu-LISA			Jaar **2018**	Jaar **2019**	Jaar **2020**	**TOTAAL**
•Beleidskredieten						
Titel 1: Personeelsuitgaven	Vastleggingen	(1)	0,210	0,210	0,210	**0,630**
	Betalingen	(2)	0,210	0,210	0,210	**0,630**
Titel 2: Infrastructuur- en operationele uitgaven	Vastleggingen	(1a)	0	0	0	**0**
	Betalingen	(2 a)	0	0	0	**0**
Titel 3: Operationele uitgaven	Vastleggingen	(1a)	12,893	2,051	1,982	**16,926**
	Betalingen	(2 a)	2,500	7,893	4,651	**15,044**
TOTAAL kredieten voor eu-LISA	Vastleggingen	=1+1a +3	13,103	2,261	2,192	**17,556**
	Betalingen	=2+2a +3	2,710	8,103	4,861	**15,674**

3.2.2. Geraamde gevolgen voor de beleidskredieten

•TOTAAL beleidskredieten	Vastleggingen	(4)								
	Betalingen	(5)								

•TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)								
TOTAAL kredieten onder RUBRIEK <….> van het meerjarig financieel kader	Vastleggingen	=4+ 6								
	Betalingen	=5+ 6								

Wanneer het voorstel/initiatief gevolgen heeft voor meerdere rubrieken

•TOTAAL beleidskredieten	Vastleggingen	(4)							
	Betalingen	(5)							
•TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)							
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 4 van het meerjarig financieel kader (referentiebedrag)	Vastleggingen	=4+ 6	19,337	22,520	22,451				**64,308**
	Betalingen	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3. Geraamde gevolgen voor de administratieve kredieten

Rubriek van het meerjarig financieel kader	**5**	"Administratieve uitgaven"

in miljoenen euro's (tot op drie decimalen)

		Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	... invullen: zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
DG: <…….>									
• Personele middelen									
• Andere administratieve uitgaven									
TOTAAL DG <…….>	Kredieten								

TOTAAL kredieten voor RUBRIEK 5 van het meerjarig financieel kader	(totaal vastleggingen = totaal betalingen)								

in miljoenen euro's (tot op drie decimalen)

		Jaar **N**[92]	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	... invullen: zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 5 van het meerjarig financieel kader	Vastleggingen								
	Betalingen								

[92] Het jaar N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen.

3.2.3.1. Geraamde gevolgen voor de beleidskredieten voor eu-LISA

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☑ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vermeld doelstellingen en outputs ⇩			Jaar **2018**		Jaar **2019**		Jaar **2020**		... invullen: zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)						**TOTAAL**			
	OUTPUTS																	
	Soort [93]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1 [94] Ontwikkeling centraal systeem																		
- Contractant			1	5.013														5.013
- Software			1	4,050														4,050
- Hardware			1	3,692														3,692
Subtotaal voor specifieke doelstelling nr. 1				12,755														12,755
SPECIFIEKE DOELSTELLING NR. 2 Onderhoud centraal systeem																		
- Contractant			1	0	1	0,365	1	0,365										0,730
Software			1	0	1	0,810	1	0,810										1,620
Hardware			1	0	1	0,738	1	0,738										1,476

[93] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[94] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

Subtotaal voor specifieke doelstelling nr. 2				1,913		1,913										3,826
SPECIFIEKE DOELSTELLING NR. 3 Vergaderingen/opleiding																
Opleidingsactiviteiten	1	0,138	1	0,138	1	0,069										0,345
Subtotaal voor specifieke doelstelling nr. 3		0,138		0,138		0,069										0,345
TOTALE KOSTEN		12,893		2,051		1,982										16,926

Vastleggingskredieten, in miljoenen euro's (tot op drie decimalen)

3.2.3.2. Geraamde gevolgen voor de kredieten van DG HOME

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☑ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vermeld doelstellingen en outputs ⇩			Jaar **2018**		Jaar **2019**		Jaar **2020**		... invullen: zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)						**TOTAAL**			
	OUTPUTS																	
	Soort [95]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1 [96]			1		1	1,221	1	1,221										2,442
SPECIFIEKE DOELSTELLING NR. 2			1		1	17,184	1	17,184										34,368
TOTALE KOSTEN						18,405		18,405										36,810

[95] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

[96] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

3.2.3.3. Geraamde gevolgen voor de personele middelen van eu-LISA - Samenvatting

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☑ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoenen euro's (tot op drie decimalen)

	Jaar **2018**	Jaar **2019**	Jaar **2020**	**TOTAAL**
Ambtenaren (AD)				
Ambtenaren (AST)				
Arbeidscontractanten	0,210	0,210	0,210	0,630
Tijdelijke functionarissen				
Gedetacheerde nationale deskundigen				
TOTAAL	**0,210**	**0,210**	**0,210**	**0,630**

Aanwerving is gepland voor januari 2018. Alle medewerkers moeten vanaf begin 2018 beschikbaar zijn, zodat tijdig met de ontwikkeling kan worden gestart en de nieuwe editie van het SIS in 2020 in gebruik kan worden genomen. De 3 nieuwe arbeidscontractanten zijn nodig voor de implementatie van het project en voor de operationele ondersteuning en het onderhoud na de ingebruikneming. De middelen zullen worden gebruikt voor:

- ondersteuning van de uitvoering van het project door de leden van het projectteam, door middel van: de vaststelling van vereisten en technische specificaties, samenwerking met en ondersteuning van de lidstaten tijdens de implementatie, actualisering van het Interface Control Document (ICD), follow-up van de contractuele leveringen, aanlevering van documentatie en updates, enz.;

- ondersteuning van overschakelingswerkzaamheden voor het operationeel maken van het systeem in samenwerking met de contractant (follow-up van softwarereleases, operationele procesupdates, opleiding (waaronder opleidingsactiviteiten in de lidstaten), enz.);

- ondersteuning van activiteiten op de langere termijn, vaststelling van specificaties, contractuele voorbereidingen voor eventuele re-engineering van het systeem (bijv. in verband met beeldherkenning) of voor het geval dat het contract inzake "Maintenance in Working Order" (MWO) voor het SIS II moet worden gewijzigd in verband met extra aanpassingen (technisch en budgettair);

- handhaving van de tweedelijnsondersteuning na de ingebruikneming, bij het lopende onderhoud en tijdens de werking.

De drie nieuwe posten (tijdelijke functionarissen in vte) vormen een aanvulling op de capaciteit van het interne team die eveneens zal worden ingezet voor het project, de contractuele en financiële follow-up en de operationele activiteiten. De inzet van tijdelijke functionarissen is passend voor de looptijd en de continuïteit van de contracten, zodat de bedrijfscontinuïteit is verzekerd en ook na de afronding van het project voor de operationele ondersteuning een beroep kan worden gedaan op reeds aanwezig gespecialiseerd personeel. Bovendien is voor de operationele ondersteuningsactiviteiten toegang tot de productieomgeving vereist, die niet kan worden verleend aan contractanten of extern personeel.

3.2.3.4. Geraamde personeelsbehoeften

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

– ☐ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in voltijdequivalenten

	Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	... invullen: zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
•Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)							
XX 01 01 01 (zetel en vertegenwoordigingen van de Commissie)							
XX 01 01 02 (delegaties)							
XX 01 05 01 (onderzoek door derden)							
10 01 05 01 (eigen onderzoek)							
•Extern personeel (in voltijdequivalenten VTE)[97]							
XX 01 02 01 (AC, END, INT van de "totale financiële middelen")							
XX 01 02 02 (AC, AL, END, INT en JED in de delegaties)							
XX 01 04 **jj** [98] - zetel							
XX 01 04 **jj** [98] - delegaties							
XX 01 05 02 (AC, END, INT – onderzoek door derden)							
10 01 05 02 (AC, END, SNE – eigen onderzoek)							
Ander begrotingsonderdeel (te vermelden)							
TOTAAL							

XX is het beleidsterrein of de begrotingstitel.

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.

97 AC= Agent Contractuel (arbeidscontractant); AL = Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT = Intérimaire (uitzendkracht); JED= Jeune Expert en Délégation (jonge deskundige in delegaties).

98 Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	
Extern personeel	

3.2.4. Verenigbaarheid met het huidig meerjarig financieel kader

– ☐ Het voorstel/initiatief is verenigbaar met het huidig meerjarig financieel kader.

– ☑ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarig financieel kader.

Gepland wordt de rest van de begroting die in het Fonds voor interne veiligheid is geoormerkt voor slimme grenzen, te herprogrammeren om de functies en wijzigingen die in de twee voorstellen zijn opgenomen, te implementeren. De ISF-grenzenverordening is het financiële instrument waarin het budget voor de tenuitvoerlegging van het slimmegrenzenpakket is opgenomen. In artikel 5 van die verordening is bepaald dat 791 miljoen EUR wordt aangewend door middel van een programma voor het opzetten van IT-systemen ter beheersing van de migratiestromen over de buitengrenzen onder de voorwaarden als bepaald in artikel 15. 480 miljoen EUR daarvan is gereserveerd voor de ontwikkeling van het inreis-uitreissysteem en 210 miljoen EUR voor de ontwikkeling van het Europees systeem voor reisinformatie en -autorisatie (ETIAS). De rest (100,828 miljoen EUR) zal gedeeltelijk worden gebruikt ter dekking van de kosten die gepaard gaan met de wijzigingen die in de twee voorstellen zijn opgenomen.

– ☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarig financieel kader.

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

3.2.5. Bijdragen van derden

– ☑ Het voorstel/initiatief voorziet niet in medefinanciering door derden.

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

Kredieten in miljoenen euro's (tot op drie decimalen)

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

3.3. Geraamde gevolgen voor de ontvangsten

– ☐ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

– ☑ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

– ☐ voor de eigen middelen

– ☑ voor de diverse ontvangsten

in miljoenen euro's (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief[99]						
		2018	2019	2020	2021	... invullen: zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
Artikel 6313 – Bijdrage van de geassocieerde Schengenlanden (CH, NO, LI, IS)		p.m.	p.m.	p.m.	p.m.			

Voor de diverse ontvangsten die worden "toegewezen", vermeld het (de) betrokken begrotingsonderde(e)l(en) voor uitgaven.

18.02.08 (Schengeninformatiesysteem), 18.02.07 (eu-LISA)

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

De begroting omvat een bijdrage van de landen die betrokken worden bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis.

[99] Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 25 % aan inningskosten.