VERORDENING (EU) 2018/1861 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 28 november 2018

betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van de Overeenkomst ter uitvoering van het Akkoord van Schengen en tot wijziging en 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 ([1]),

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. 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 Unie, door ondersteuning te bieden bij de operationele samenwerking tussen nationale bevoegde autoriteiten, met name grenswachters, de politie, douaneautoriteiten, immigratieautoriteiten, en autoriteiten die verantwoordelijk zijn voor het voorkomen, opsporen, onderzoeken of vervolgen van strafbare of tenuitvoerleggen van strafrechtelijke sancties.

(2) SIS is aanvankelijk ingesteld op grond 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 ([2]) (de overeenkomst ter uitvoering van het Schengenakkoord). De ontwikkeling van de tweede generatie van SIS (SIS II) was toevertrouwd aan de Commissie krachtens Verordening (EG) nr. 2424/2001 van de Raad ([3]) en Besluit 2001/886/JBZ van de Raad ([4]). SIS II is later ingesteld bij Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad ([5]) en Besluit 2007/533/JBZ van de Raad ([6]). SIS II heeft het bij de overeenkomst ter uitvoering van het Schengenakkoord ingestelde SIS vervangen.

(3) Drie jaar na de ingebruikneming van SIS II heeft de Commissie het systeem geëvalueerd overeenkomstig Verordening (EG) nr. 1987/2006 en van Besluit 2007/533/JBZ. De Commissie diende op 21 december 2016 bij het Europees Parlement en de Raad een verslag in over de evaluatie van het Schengeninformatiesysteem van de tweede generatie (SIS II) 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, en een bijbehorend werkdocument van de diensten van de Commissie. De aanbevelingen die in die documenten worden gedaan, moeten, waar passend, tot uiting komen in deze verordening.

(4) Deze verordening vormt de rechtsgrondslag voor SIS met betrekking tot aangelegenheden die vallen onder het toepassingsgebied van het derde deel, titel V, hoofdstuk 2, van het Verdrag betreffende de werking van de Europese Unie (VWEU). Verordening (EG) 2018/1862 van het Europees Parlement en de Raad ([7]) vormt de rechtsgrondslag voor SIS met betrekking tot aangelegenheden die vallen onder het toepassingsgebied van het derde deel, titel V, hoofdstukken 4 en 5, VWEU.

([1]) Standpunt van het Europees Parlement van 24 oktober 2018 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 19 november 2018.

([2]) PB L 239 van 22.9.2000, blz. 19.

([3]) Verordening (EG) nr. 2424/2001 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. 4).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) Verordening (EU) 2018/1862 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken en tot wijziging en intrekking van Verordening 2007/533/JBZ, en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad, en Besluit 2010/261/EU van de Commissie (zie bladzijde 56 van dit Publicatieblad).

(5) Het feit dat afzonderlijke instrumenten zijn vastgesteld als rechtsgrondslag voor SIS, doet geen afbreuk aan het beginsel dat SIS één integraal informatiesysteem vormt, dat als zodanig moet functioneren. Het dient één netwerk van nationale bureaus, Sirene-bureaus genaamd, te omvatten voor de uitwisseling van aanvullende informatie. Een aantal bepalingen van die instrumenten dient bijgevolg identiek te zijn.

(6) Het is noodzakelijk de doelstellingen, bepaalde elementen van de technische architectuur en de financiering van SIS te specificeren, voorschriften betreffende het volledige werkingstraject en het gebruik van het systeem vast te stellen, en de verantwoordelijkheden te definiëren. Het is ook noodzakelijk de categorieën in het systeem in te voeren gegevens, de doeleinden van de invoering en de verwerking van de gegevens en de criteria voor hun invoering te bepalen. Tevens zijn voorschriften vereist inzake het wissen van signaleringen, de autoriteiten die toegang hebben tot de gegevens, het gebruik van biometrische gegevens en het nader vaststellen van voorschriften inzake gegevensbescherming en -verwerking.

(7) Signaleringen in SIS bevatten uitsluitend informatie die nodig is om een persoon te identificeren en voor de te ondernemen actie. Daarom moeten lidstaten waar nodig aanvullende informatie in verband met signaleringen uitwisselen.

(8) SIS omvat een centraal systeem (het centrale SIS) en nationale systemen. De nationale systemen kunnen een volledige of gedeeltelijke kopie van de SIS-databank bevatten en door twee of meer lidstaten worden gedeeld. Aangezien SIS in Europa het belangrijkste instrument is voor de uitwisseling van informatie met het oog op het waarborgen van de veiligheid en een doeltreffend grensbeheer, moet het systeem zowel op centraal als op nationaal niveau ononderbroken operationeel zijn. Op de beschikbaarheid van SIS moet op centraal niveau en op het niveau van de lidstaten van dichtbij toegezien worden en elk incident inzake onbeschikbaarheid voor eindgebruikers moet worden geregistreerd en op nationaal en Unieniveau aan de belanghebbenden worden gemeld. Elke lidstaat dient een back-up voor zijn nationaal systeem op te zetten. Tevens moeten de lidstaten een ononderbroken verbinding met het centrale SIS garanderen door te voorzien in twee identieke, fysiek en geografisch gescheiden aansluitingspunten. Het centrale SIS en de communicatie-infrastructuur moeten zodanig worden beheerd dat hun werking 24 uur per dag en zeven dagen per week verzekerd is. Om die reden moet het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht („eu-LISA"), dat is opgericht bij Verordening (EU) 2018/1726 van het Europees Parlement en de Raad ([1]) technische oplossingen toepassen ter ondersteuning van de ononderbroken beschikbaarheid van SIS, onderworpen aan een onafhankelijke effectbeoordeling en kosten-batenanalyse.

(9) Er moet een handboek worden bijgehouden met gedetailleerde voorschriften voor de uitwisseling van aanvullende informatie over de in de signalering gevraagde te ondernemen actie („het Sirene-handboek"). De Sirene-bureaus moeten zorgen voor de snelle en doeltreffende uitwisseling van dergelijke informatie.

(10) Met het oog op de efficiënte uitwisseling van aanvullende informatie, met inbegrip van de in signaleringen gespecificeerde te ondernemen actie, 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.

(11) De lidstaten dienen ervoor te zorgen dat het personeel van hun Sirene-bureau de taalkundige vaardigheden en kennis van het relevante recht en de procedurele voorschriften heeft, die nodig zijn om hun taken uit te voeren.

(12) Om volledig gebruik te kunnen maken van de functies van SIS, moeten de lidstaten ervoor zorgen dat de eindgebruikers en het personeel van de Sirene-bureaus regelmatig worden bijgeschoold, onder meer over gegevensbeveiliging, gegevensbescherming, en gegevenskwaliteit. De Sirene-bureaus moeten worden betrokken bij de ontwikkeling van opleidingsprogramma's. De Sirene-bureaus moeten, voor zover mogelijk, ook ten minste eenmaal per jaar een uitwisseling van medewerkers met andere Sirene-bureaus organiseren. De lidstaten worden aangemoedigd passende maatregelen te nemen om te voorkomen dat door personeelsverloop vaardigheden en ervaring verloren gaan.

(13) Het operationele beheer van de centrale componenten van SIS wordt uitgevoerd door eu-LISA Om eu-LISA in staat te stellen de financiële en personele middelen in te zetten die nodig zijn voor een alomvattend operationeel beheer van het centrale SIS en de communicatie-infrastructuur, moeten in deze verordening de taken van het Agentschap nauwkeurig worden omschreven, met name wat de technische aspecten van de uitwisseling van aanvullende informatie betreft.

(14) Onverminderd de verantwoordelijkheid van de lidstaten voor de nauwkeurigheid van de in SIS ingevoerde gegevens, en de rol van de Sirene-bureaus als kwaliteitscoördinatoren, dient eu-LISA de verantwoordelijkheid te krijgen om de gegevenskwaliteit te verbeteren door een centraal instrument voor het toezicht op de gegevenskwaliteit in te voeren, en om op gezette tijden verslag uit te brengen aan de Commissie en de lidstaten. De Commissie

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

dient aan het Europees Parlement en de Raad verslag uit te brengen over eventuele problemen met de gegevenskwaliteit. Om de kwaliteit van de gegevens in SIS verder te verhogen, moet eu-LISA ook opleidingen over het gebruik van SIS aanbieden aan nationale opleidingsinstanties en, voor zover mogelijk, aan de Sirene-bureaus en aan eindgebruikers.

(15) Om beter te kunnen toezien op het gebruik van SIS en om trends inzake migratiedruk en grensbeheer te analyseren, moet eu-LISA in staat zijn om, zonder gevaar voor de integriteit van de gegevens, een geavanceerde voorziening te ontwikkelen voor statistische rapportage aan de lidstaten, het Europees Parlement, de Raad, de Commissie, Europol en het Europees Grens- en kustwachtagentschap. Hiertoe moet een centraal register worden opgezet. In dat register bewaarde of van dat register verkregen statistieken, mogen geen persoonsgegevens bevatten. De lidstaten dienen in het kader van samenwerking tussen toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming onder deze verordening statistieken mee te delen over de uitoefening van het recht op toegang tot gegevens, rectificatie van onjuiste gegevens en wissing van onrechtmatig opgeslagen gegevens.

(16) Nieuwe gegevenscategorieën dienen aan SIS te worden toegevoegd, zodat de eindgebruikers met kennis van zaken en zonder tijdverlies een beslissing 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, indien dergelijke informatie beschikbaar is, een verwijzing naar het persoonlijke identificatiedocument van de betrokken persoon of het nummer van dat document bevatten en een kopie van dat document, indien mogelijk in kleur.

(17) De bevoegde autoriteiten moeten, waar dat strikt noodzakelijk is, specifieke informatie in SIS kunnen invoeren over eventuele specifieke, onveranderlijke objectieve fysieke kenmerken van een persoon, zoals tatoeages, merktekens of littekens.

(18) Indien beschikbaar, moet bij het creëren van een signalering alle betrokken informatie en met name de voornaam van de betrokken persoon worden ingevoerd, zodat het risico van valse hits tot een minimum wordt beperkt en onnodige handelingen worden vermeden.

(19) Voor een doorzoeking gebruikte gegevens mogen niet in SIS worden opgeslagen, tenzij het gaat om logbestanden om de rechtmatigheid van de doorzoeking te verifiëren, toezicht op de rechtmatigheid van de gegevensverwerking te monitoren, intern toezicht, de goede werking van de nationale systemen alsmede de integriteit en beveiliging van de gegevens te waarborgen.

(20) SIS moet de verwerking van biometrische gegevens mogelijk maken om de betrouwbare identificatie van de desbetreffende personen te vergemakkelijken. Elke invoering van foto's, gezichtsopnamen of dactyloscopische gegevens in SIS en elk gebruik van dergelijke gegevens moet worden beperkt tot dat wat nodig is om de nagestreefde doelstellingen te verwezenlijken, moet op grond van het Unierecht toegestaan zijn, moet de grondrechten in acht nemen, met inbegrip van het belang van het kind, en moet in overeenstemming zijn met het Unierecht inzake gegevensbescherming, met inbegrip van de in deze verordening vastgestelde relevante gegevensbeschermingsbepalingen. In dit verband moet SIS tevens de verwerking mogelijk maken van gegevens van personen wier identiteit onrechtmatig is aangenomen, om problemen als gevolg van een verkeerde identificatie te voorkomen, met passende waarborgen, met instemming van de betrokken persoon voor iedere gegevenscategorie, in het bijzonder voor handpalmafdrukken, en met een strikte beperking van de doeleinden waarvoor dergelijke persoonsgegevens rechtmatig kunnen worden verwerkt.

(21) De lidstaten moeten het voor eindgebruikers technisch mogelijk maken om telkens wanneer zij een nationale politie- of immigratiedatabank mogen doorzoeken, zij tevens een parallelle doorzoeking in SIS uitvoeren overeenkomstig de beginselen van artikel 4 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad ([1]) en artikel 5 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([2]). Dit moet ervoor zorgen dat 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.

(22) Er moet worden vastgesteld onder welke voorwaarden dactyloscopische gegevens, foto's en gezichtsopnamen mogen worden gebruikt voor identificatie- en verificatiedoeleinden. Gezichtsopnamen en foto's voor identificatiedoeleinden dienen in eerste instantie uitsluitend te worden gebruikt bij reguliere grensdoorlaatposten. Dergelijk gebruik dient af te hangen van een verslag van de Commissie waarin de beschikbaarheid, betrouwbaarheid en paraatheid van de technologie wordt bevestigd.

([1]) 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).

([2]) 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).

(23) Het doorzoeken van dactyloscopische gegevens in SIS aan de hand van op een plaats delict aangetroffen volledige of onvolledige reeksen vingerafdrukken of handpalmafdrukken 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, en mits een doorzoeking tegelijk in de relevante nationale vingerafdrukdatabanken wordt uitgevoerd. Bijzondere aandacht moet worden besteed aan het vaststellen van kwaliteitsnormen voor de opslag van biometrische gegevens.

(24) Indien de identiteit van een persoon niet met behulp van andere middelen kan worden vastgesteld, moeten dactyloscopische gegevens worden gebruikt om te proberen de identiteit vast te stellen. Het moet in alle gevallen toegestaan zijn een persoon te identificeren door middel van dactyloscopische gegevens.

(25) Het moet voor de lidstaten mogelijk zijn signaleringen in SIS te linken. Het linken van twee of meer signaleringen mag geen gevolgen hebben voor de te ondernemen actie, de toetsingstermijn voor signaleringen of het recht op toegang tot de signaleringen.

(26) Er kan een hoger niveau van doeltreffendheid, harmonisatie en samenhang worden bereikt door te eisen dat alle inreisverboden die de nationale bevoegde autoriteiten overeenkomstig Richtlijn 2008/115/EG van het Europees Parlement en de Raad [1] hebben uitgevaardigd, in SIS worden ingevoerd, en door gemeenschappelijke regels vast te stellen voor het invoeren van een signalering met het oog op weigering van toegang en verblijf 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 betrokken onderdaan van het derde land het Schengengebied verlaat, volledig samenvalt met het tijdstip waarop de signalering in SIS wordt geactiveerd. Op die manier moet worden gewaarborgd dat de inreisverboden bij de doorlaatposten aan de buitengrenzen worden uitgevoerd en afdoende wordt voorkomen dat de betrokken personen het Schengengebied terug binnenkomen.

(27) Personen ten aanzien van wie een beslissing is genomen tot weigering van toegang en verblijf moeten het recht hebben tegen die beslissing in beroep te gaan. Indien het een beslissing inzake terugkeer is, moet het recht van beroep voldoen aan Richtlijn 2008/115/EG.

(28) Bij deze verordening moeten bindende regels worden vastgesteld voor raadpleging tussen en kennisgeving aan nationale autoriteiten wanneer een onderdaan van een derde land in het bezit is of kan komen van een in een bepaalde lidstaat afgegeven geldige verblijfsvergunning of geldig visum voor verblijf van langere duur, en een andere lidstaat voornemens is ten aanzien van die onderdaan van een derde land een signalering met het oog op weigering van toegang en verblijf in te voeren, of zulks reeds heeft gedaan. Dergelijke situaties leiden tot grote onzekerheid bij grenswachters en politie- en immigratieautoriteiten. Daarom dient te worden gezorgd voor een bindende termijn voor spoedig overleg waarbinnen een definitief resultaat moet worden bereikt, teneinde ervoor te zorgen dat de onderdanen van derde landen die het recht hebben rechtmatig op het grondgebied van de lidstaten te verblijven, dat grondgebied zonder problemen kunnen binnenkomen en dat diegenen die geen recht hebben binnen te komen de toegang wordt verhinderd.

(29) Indien naar aanleiding van een raadpleging tussen de lidstaten een signalering in SIS wordt gewist, moet de signalerende lidstaat de mogelijkheid hebben de betrokken onderdaan van een derde land op zijn nationale signaleringslijst te handhaven.

(30) Deze verordening laat de toepassing van Richtlijn 2004/38/EG van het Europees Parlement en de Raad onverlet [2].

(31) Signaleringen mogen niet langer in SIS worden bewaard dan nodig is voor de met de signaleringen nagestreefde specifieke doeleinden. Uiterlijk drie jaar na de invoering van een signalering in SIS dient de signalerende lidstaat de noodzaak van verdere bewaring te toetsen. Indien echter bij de nationale beslissing die aan de basis ligt van de signalering een langere geldigheidsperiode dan drie jaar is bepaald, wordt de signalering uiterlijk binnen vijf jaar opnieuw getoetst. Besluiten om signaleringen van personen te bewaren, dienen gebaseerd te zijn op een uitvoerige individuele beoordeling. De lidstaten moeten signaleringen van personen binnen de voorgeschreven toetsingstermijnen toetsen en statistieken bijhouden van het aantal signaleringen van personen waarvan de bewaartermijn is verlengd.

(32) Voor de invoering van een signalering in SIS en de verlenging van de geldigheidsduur van een signalering in SIS moet een evenredigheidsvereiste in acht worden genomen, dat onderzoek inhoudt of een concreet geval gepast, relevant en belangrijk genoeg is om invoering van een signalering in SIS te rechtvaardigen. Waar het terroristische misdrijven betreft, moet het geval gepast, relevant en belangrijk genoeg worden bevonden om een signalering in SIS te rechtvaardigen. Om redenen van openbare en nationale veiligheid mag het de lidstaten bij uitzondering worden toegestaan om geen signalering in SIS in te voeren, wanneer te verwachten valt dat een dergelijke invoering officiële of justitiële onderzoeken, opsporingsonderzoeken of procedures zou belemmeren.

---

[1] 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).

[2] 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, tot wijziging van Verordening (EEG) nr. 1612/68 en tot intrekking van Richtlijnen 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG en 93/96/EEG (PB L 158 van 30.4.2004, blz. 77).

(33) De integriteit van SIS-gegevens is van essentieel belang. Daarom moeten voldoende waarborgen worden geboden ten aanzien van de beveiliging van de data gedurende het volledige verwerkingstraject, zowel op centraal als op nationaal niveau. De instanties die betrokken zijn bij de gegevensverwerking, moeten zich houden aan de beveiligingsvereisten van deze verordening en een uniforme procedure voor het melden van incidenten volgen. Hun personeel moet de juiste opleiding hebben gekregen en moet op de hoogte zijn gebracht van alle ter zake doende strafbare feiten en sancties.

(34) De ingevolge deze verordening in SIS verwerkte gegevens en de desbetreffende uitgewisselde aanvullende informatie mogen niet worden doorgegeven aan of ter beschikking gesteld van derde landen of internationale organisaties.

(35) 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, en over de terugkeer van illegaal verblijvende onderdanen van derde landen, dient aan die autoriteiten toegang tot SIS te worden verleend in het kader van deze verordening.

(36) Onverminderd meer specifieke in deze verordening vastgelegde regels betreffende de verwerking van persoonsgegevens, is Verordening (EU) 2016/679 van toepassing op de verwerking van persoonsgegevens door de lidstaten uit hoofde van deze verordening, tenzij de verwerking wordt verricht door de nationale bevoegde autoriteiten met het oog op het voorkomen, onderzoeken of opsporen van terroristische misdrijven of andere ernstige strafbare feiten.

(37) Onverminderd meer specifieke in deze verordening vastgelegde regels, zijn de nationale wettelijke en bestuursrechtelijke bepalingen die op grond van Richtlijn (EU) 2016/680 zijn vastgesteld, van toepassing op de verwerking van persoonsgegevens uit hoofde van deze verordening door de nationale bevoegde autoriteiten met het oog op het voorkomen, opsporen, onderzoeken of vervolgen van terroristische misdrijven of andere ernstige strafbare feiten, of de tenuitvoerlegging van strafrechtelijke sancties. De toegang tot in SIS ingevoerde gegevens en het recht van bevoegde nationale autoriteiten die verantwoordelijk zijn voor het voorkomen, opsporen, onderzoeken of vervolgen van terroristische misdrijven of andere ernstige strafbare feiten, of voor de tenuitvoerlegging van strafrechtelijke sancties, om deze gegevens te doorzoeken, moet onderworpen zijn aan alle toepasselijke bepalingen van deze verordening en die van Richtlijn (EU) 2016/680, zoals omgezet in het nationale recht, en met name aan het toezicht door de in Richtlijn (EU) 2016/680 bedoelde toezichthoudende autoriteiten.

(38) Wanneer de instellingen en organen van de Unie bij het uitvoeren van hun taken in het kader van deze verordening persoonsgegevens verwerken, is Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([1]) van toepassing.

(39) Wanneer Europol in het kader van deze verordening persoonsgegevens verwerkt, is Verordening (EU) 2016/794 van het Europees Parlement en de Raad ([2]) van toepassing.

(40) Wanneer zij SIS gebruiken, moeten de bevoegde autoriteiten ervoor zorgen dat de waardigheid en de integriteit van de persoon wiens gegevens worden verwerkt, worden geëerbiedigd. De verwerking van persoonsgegevens voor de toepassing van deze verordening mag niet leiden tot discriminatie van personen op grond van, onder meer, geslacht, ras of etnische afstamming, godsdienst of overtuiging, handicap, leeftijd of seksuele geaardheid.

(41) Wat de vertrouwelijkheid betreft, moeten ambtenaren en andere personeelsleden die werkzaamheden in verband met SIS verrichten, zich houden aan de relevante bepalingen van het Statuut van de ambtenaren van de Europese Unie en de regeling welke van toepassing is op andere personeelsleden van de Unie, zoals vastgesteld bij Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad ([3]) („het Statuut").

(42) De lidstaten en eu-LISA 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 aan te pakken.

(43) De in Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680 bedoelde nationale onafhankelijke toezichthoudende autoriteiten („toezichthoudende autoriteiten") moeten erop toezien dat de lidstaten de persoonsgegevens in het kader van deze verordening rechtmatig verwerken, met inbegrip van de uitwisseling van aanvullende informatie. De toezichthoudende autoriteiten moeten voldoende middelen krijgen voor het vervullen van deze taak. Er moeten bepalingen worden vastgesteld inzake de rechten van betrokkenen op inzage, rectificatie en wissing van hun in SIS opgeslagen persoonsgegevens, alsmede inzake de rechtsmiddelen voor de nationale gerechten en de wederzijdse erkenning van rechterlijke beslissingen in dat verband. Het is tevens passend van de lidstaten te verlangen dat zij hieromtrent jaarlijkse statistieken verstrekken.

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

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

([3]) PB L 56 van 4.3.1968, blz. 1.

(44) De toezichthoudende autoriteiten moeten erop toezien dat ten minste om de vier jaar een audit van de gegevensverwerking in de nationale systemen van hun lidstaten wordt uitgevoerd overeenkomstig internationale auditnormen. De audit moet worden uitgevoerd door de toezichthoudende autoriteiten of moet door de 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 toezichthoudende autoriteiten, die derhalve zelf de auditor dienen te instrueren, en een duidelijk omschreven doel, reikwijdte en methode voor de audit moeten vaststellen alsmede met betrekking tot de audit en de eindresultaten richtsnoeren moeten uitvaardigen en toezicht moeten uitoefenen.

(45) De Europese Toezichthouder voor gegevensbescherming dient toezicht uit te oefenen op de werkzaamheden van de instellingen en organen van de Unie in verband met de verwerking van persoonsgegevens krachtens deze verordening. De Europese Toezichthouder voor gegevensbescherming en de toezichthoudende autoriteiten dienen samen te werken bij het toezicht op SIS.

(46) De Europese Toezichthouder voor gegevensbescherming moet voldoende middelen krijgen om de taken te vervullen die hem krachtens deze verordening zijn toevertrouwd, met inbegrip van ondersteuning door deskundigen op het gebied van biometrische gegevens.

(47) Verordening (EU) 2016/794 bepaalt dat Europol ondersteuning en versterking moet bieden voor het optreden van de nationale bevoegde autoriteiten en hun onderlinge samenwerking bij de bestrijding van terrorisme en andere vormen van ernstige criminaliteit, en in dat verband analyses en dreigingsevaluaties dient te verstrekken. Om het werk van Europol, met name in het kader van het Europees Centrum tegen migrantensmokkel, te vergemakkelijken, dient Europol toegang te krijgen tot in deze verordening bepaalde signaleringscategorieën.

(48) Om de kloof op het gebied van informatiedeling over terrorisme en met name over buitenlandse terroristische strijders — in welk geval het monitoren van bewegingen van essentieel belang is — te overbruggen, worden de lidstaten aangemoedigd informatie over met terrorisme verband houdende activiteiten te delen met Europol. Deze informatiedeling moet worden uitgevoerd door met Europol aanvullende informatie over de betrokken signaleringen uit te wisselen. Europol dient daartoe te voorzien in een verbinding met de communicatie-infrastructuur.

(49) Met het oog op een optimaal gebruik van 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 nageleefd overeenkomstig deze verordening en Verordening (EU) 2016/794. Wanneer bij doorzoeking van SIS door Europol blijkt dat een lidstaat een signalering heeft ingevoerd, mag Europol de gevraagde actie niet uitvoeren. Europol dient in zulke gevallen via de uitwisseling van aanvullende informatie met het betrokken Sirene-bureau de betrokken lidstaat op de hoogte te brengen, zodat die lidstaat het vervolg van de zaak op zich kan nemen.

(50) Bij Verordening (EU) 2016/1624 van het Europees Parlement en de Raad [1] is voor de uitvoering van die verordening bepaald dat de ontvangende lidstaat de leden van de door het Europees Grens- en kustwachtagentschap ingezette teams als bedoeld in artikel 2, punt 8, van die verordening, toestemming moet verlenen om databanken van de Unie 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 relevante agentschappen van de Unie, meer bepaald het Europees Ondersteuningsbureau voor asielzaken en Europol, kunnen aan de ondersteuningsteams voor migratiebeheer deskundigen toevoegen die geen personeelslid van deze agentschappen van de Unie zijn. De inzet van de teams als bedoeld in artikel 2, punten 8 en 9, van die verordening, 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 teams als bedoeld in artikel 2, punten 8 en 9, van die verordening hebben voor de uitvoering van hun taken toegang nodig tot SIS via een technische interface van het Europees Grens- en kustwachtagentschap die wordt aangesloten op het centrale SIS. Wanneer bij doorzoeking van SIS door de teams bedoeld in artikel 2, punten 8 en 9, van Verordening (EU) 2016/1624 of door de teamleden blijkt dat een lidstaat een signalering heeft ingevoerd, voert het betrokken team- of personeelslid de gevraagde actie alleen uit indien de ontvangende lidstaat daartoe toestemming heeft verleend. In zulke gevallen moet de ontvangende lidstaat op de hoogte worden gebracht opdat deze de zaak kan opvolgen. De ontvangende lidstaat dient de signalerende lidstaat van de hit op de hoogte te brengen via de uitwisseling van aanvullende informatie.

(51) Bepaalde aspecten van SIS kunnen vanwege hun technische, gedetailleerde en aan verandering onderhevige aard, niet uitputtend worden geregeld in deze verordening. Het gaat dan bijvoorbeeld over technische voorschriften inzake het invoeren, bijwerken, wissen en doorzoeken van gegevens, gegevenskwaliteit, regels inzake biometrische

[1] 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).

gegevens, en regels inzake verenigbaarheid en prioriteit van signaleringen, inzake het linken van signaleringen, en inzake 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.

(52) Teneinde eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad ([1]). Voor de vaststelling van uitvoeringshandelingen in het kader van deze verordening en in het kader van Verordening (EU) 2018/1862 dient dezelfde procedure te worden gevolgd.

(53) Met het oog op transparantie moet eu-LISA twee jaar nadat na aanvang van de werkzaamheden van SIS ingevolge deze verordening, een verslag opstellen over de technische werking van het centrale SIS en de communicatie-infrastructuur, met inbegrip van de beveiliging daarvan, alsmede over de bilaterale en multilaterale uitwisseling van aanvullende informatie. Om de vier jaar moet de Commissie een algehele evaluatie uitbrengen.

(54) Teneinde een soepele werking van SIS te verzekeren, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 VWEU handelingen vast te stellen met betrekking tot het bepalen van de omstandigheden waarin foto's en gezichtsopnamen mogen worden gebruikt voor de identificatie van personen anders dan bij reguliere grensdoorlaatposten. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen geschieden in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven ([2]). Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(55) Aangezien de doelstellingen van deze verordening, namelijk de instelling en regulering van een informatiesysteem van de Unie en de uitwisseling van aanvullende informatie, niet voldoende door de lidstaten kunnen worden verwezenlijkt maar door de aard ervan beter op het niveau van de Unie kunnen worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie (VEU) neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze doelstellingen te verwezenlijken.

(56) 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. Met name eerbiedigt deze verordening volledig de bescherming van persoonsgegevens zoals vastgelegd in artikel 8 van het Handvest van de grondrechten van de Europese Unie en is zij daarnaast gericht op het waarborgen van een veilige omgeving voor iedereen die op het grondgebied van de Unie verblijft, en op de bescherming van irreguliere migranten tegen uitbuiting en mensenhandel. Wanneer het om kinderen gaat, komt het belang van het kind op de eerste plaats.

(57) De geraamde kosten voor het opwaarderen van de nationale systemen en de uitvoering van de bij deze verordening voorziene nieuwe functies zijn lager dan het saldo van de kredietlijn die in Verordening (EU) nr. 515/2014 van het Europees Parlement en de Raad ([3]) is uitgetrokken voor slimme grenzen. Derhalve dient het bedrag dat is bestemd voor de ontwikkeling van IT-systemen ter beheersing van de migratiestromen langs de buitengrenzen, overeenkomstig Verordening (EU) nr. 515/2014, aan de lidstaten en eu-LISA te worden toegekend. Er moet worden toegezien op de financiële kosten voor het opwaarderen van SIS en de uitvoering van deze verordening. Indien de geraamde kosten hoger uitvallen, dient ter ondersteuning van de lidstaten financiering van de Unie beschikbaar te worden gesteld overeenkomstig het toepasselijke meerjarig financieel kader.

(58) Overeenkomstig de artikelen 1 en 2 van Protocol nr. 22 betreffende de positie van Denemarken, gehecht aan het VEU en het VWEU, neemt Denemarken niet deel aan de vaststelling van deze verordening, die derhalve niet bindend is voor, noch van toepassing is in deze lidstaat. Aangezien deze verordening voortbouwt op het Schengenacquis, beslist Denemarken overeenkomstig artikel 4 van het bovengenoemde protocol binnen een termijn van zes maanden nadat de Raad heeft beslist over deze verordening of het deze in zijn nationale wetgeving zal omzetten.

([1]) 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).

([2]) PB L 123 van 12.5.2016, blz. 1.

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

(59) Deze verordening vormt een ontwikkeling van de bepalingen van het Schengenacquis waaraan het Verenigd Koninkrijk niet deelneemt, overeenkomstig Besluit 2000/365/EG van de Raad ([1]); het Verenigd Koninkrijk neemt derhalve niet deel aan de vaststelling van deze verordening en deze is bijgevolg niet bindend voor, noch van toepassing op deze lidstaat.

(60) Deze verordening houdt een ontwikkeling in van de bepalingen van het Schengenacquis waaraan Ierland niet deelneemt, overeenkomstig Besluit 2002/192/EG van de Raad ([2]); Ierland neemt derhalve niet deel aan de vaststelling van deze verordening en deze is niet bindend voor, noch van toepassing op deze lidstaat.

(61) Wat IJsland en Noorwegen betreft, vormt deze verordening een ontwikkeling van de bepalingen van het Schengenacquis in de zin van de Overeenkomst tussen de Raad van de Europese Unie en 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 ([3]), die vallen onder het gebied bedoeld in artikel 1, punt G, van Besluit 1999/437/EG van de Raad ([4]).

(62) Wat Zwitserland betreft, vormt deze verordening een ontwikkeling van de bepalingen van het Schengenacquis in de zin 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 ([5]) die vallen onder het gebied bedoeld in artikel 1, punt G, van Besluit 1999/437/EG, in samenhang met artikel 3 van Besluit 2008/146/EG van de Raad ([6]).

(63) Wat Liechtenstein betreft, vormt deze verordening een ontwikkeling 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 ([7]) die vallen onder het gebied bedoeld in artikel 1, punt G, van Besluit 1999/437/EG juncto artikel 3 van Besluit 2011/350/EU van de Raad ([8]).

(64) Wat Bulgarije en Roemenië betreft, vormt deze verordening een handeling die op het Schengenacquis voortbouwt of anderszins daaraan is gerelateerd in de zin van artikel 4, lid 2, van de Toetredingsakte van 2005, en dient zij te worden gelezen in samenhang met respectievelijk Besluiten 2010/365/EU ([9]) en (EU) 2018/934 ([10]) van de Raad.

(65) Wat Kroatië betreft, vormt deze verordening een handeling die voortbouwt op het Schengenacquis of anderszins daaraan is gerelateerd in de zin van artikel 4, lid 2, van de Toetredingsakte van 2011 en dient zij te worden gelezen in samenhang met Besluit (EU) 2017/733 van de Raad ([11]).

(66) Wat Cyprus betreft, vormt deze verordening een handeling die voortbouwt op het Schengenacquis of anderszins daaraan is gerelateerd in de zin van artikel 3, lid 2, van de Toetredingsakte van 2003.

(67) Bij deze verordening wordt aan SIS een reeks verbeteringen aangebracht die een doeltreffender SIS, een sterkere gegevensbescherming en een uitgebreider recht op toegang zullen opleveren. Sommige van die verbeteringen vereisen geen complexe technische ontwikkelingen, terwijl voor andere technische wijzigingen van uiteenlopende omvang nodig zijn. Om verbeteringen van het systeem zo spoedig mogelijk beschikbaar te maken voor eindgebruikers, worden bij deze verordening gefaseerd wijzigingen van Verordening (EG) nr. 1987/2006 ingevoerd. Een

---

([1]) 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 (PB L 131 van 1.6.2000, blz. 43).

([2]) 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 (PB L 64 van 7.3.2002, blz. 20).

([3]) PB L 176 van 10.7.1999, blz. 36.

([4]) Besluit 1999/437/EG van de Raad van 17 mei 1999 inzake bepaalde toepassingsbepalingen van de door de Raad van de Europese Unie, de Republiek IJsland en het Koninkrijk Noorwegen gesloten overeenkomst inzake de wijze waarop deze twee staten worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengen-acquis (PB L 176 van 10.7.1999, blz. 31).

([5]) PB L 53 van 27.2.2008, blz. 52.

([6]) Besluit 2008/146/EG van de Raad van 28 januari 2008 betreffende de sluiting namens de Europese Gemeenschap 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 53 van 27.2.2008, blz. 1).

([7]) PB L 160 van 18.6.2011, blz. 21.

([8]) 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).

([9]) Besluit 2010/365/EU 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).

([10]) Besluit (EU) 2018/934 van de Raad van 25 juni 2018 betreffende de inwerkingstelling van de resterende bepalingen van het Schengenacquis die betrekking hebben op het Schengeninformatiesysteem in de Republiek Bulgarije en in Roemenië (PB L 165 van 2.7.2018, blz. 37).

([11]) Besluit (EU) 2017/733 van de Raad van 25 april 2017 betreffende de toepassing van de bepalingen van het Schengenacquis met betrekking tot het Schengeninformatiesysteem in de Republiek Kroatië (PB L 108 van 26.4.2017, blz. 31).

aantal verbeteringen van het systeem moet onmiddellijk na de inwerkingtreding van deze verordening van toepassing zijn, terwijl andere een of twee jaar na de inwerkingtreding van toepassing moeten zijn. Deze verordening moet in al haar onderdelen binnen drie jaar na de inwerkingtreding ervan van toepassing zijn. Om vertragingen bij de toepassing ervan te vermijden moet de gefaseerde uitvoering van deze verordening nauwlettend in het oog worden gehouden.

(68) Verordening (EG) nr. 1987/2006 moet met ingang van de datum van volledige toepassing van deze verordening worden ingetrokken.

(69) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 28, lid 2, van Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad [1], en heeft op 3 mei 2017 advies uitgebracht,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Algemene doelstelling van SIS

SIS heeft tot doel met behulp van de via dit systeem gecommuniceerde 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 toepassing te garanderen van de bepalingen van het derde deel, titel V, hoofdstuk 2, VWEU inzake het verkeer van personen op het grondgebied van de lidstaten.

Artikel 2

Onderwerp

1. Bij deze verordening worden de voorwaarden en procedures vastgesteld voor het invoeren en verwerken in SIS van signaleringen in verband met onderdanen van derde landen 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. Bij deze verordening worden ook bepalingen vastgesteld betreffende de technische architectuur van SIS, betreffende de verantwoordelijkheden van de lidstaten en van het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA), betreffende gegevensverwerking, betreffende de rechten van de betrokken personen en betreffende aansprakelijkheid.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1. „signalering": een in SIS ingevoerde reeks gegevens aan de hand waarvan de bevoegde autoriteiten een persoon kunnen identificeren met het oog op het uitvoeren van een specifieke actie;
2. „aanvullende informatie": andere informatie dan de in SIS opgeslagen signaleringsgegevens, die gerelateerd is aan signaleringen in SIS en die via de Sirene-bureaus moet worden uitgewisseld:
   a) om de lidstaten in staat te stellen elkaar te raadplegen of elkaar inlichtingen te verstrekken bij de invoering van een signalering;
   b) bij een hit zodat de passende actie kan worden ondernomen;
   c) indien de gevraagde actie niet kan worden uitgevoerd;
   d) inzake de kwaliteit van de SIS-gegevens;
   e) inzake de verenigbaarheid en de prioriteit van signaleringen;
   f) inzake toegangsrechten;
3. „extra gegevens": de in SIS opgeslagen en aan signaleringen in SIS gerelateerde gegevens die onmiddellijk ter beschikking van de bevoegde autoriteiten moeten staan wanneer personen over wie gegevens in SIS zijn ingevoerd, worden gelokaliseerd als gevolg van een doorzoeking van SIS;

[1] 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).

4. „onderdaan van een derde land": eenieder die geen burger van de Unie in de zin van artikel 20, lid 1, VWEU is, met uitzondering van begunstigden van rechten van vrij verkeer die gelijkwaardig zijn aan die van burgers van de Unie uit hoofde van overeenkomsten tussen de Unie of de Unie en haar lidstaten, enerzijds, en derde landen, anderzijds;

5. „persoonsgegevens": persoonsgegevens als gedefinieerd in artikel 4, punt 1, van Verordening (EU) 2016/679;

6. „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, registreren in logbestanden, ordenen, structureren, opslaan, veranderen of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzenden, verspreiden of op andere wijze ter beschikking stellen, in overeenstemming brengen of combineren, beperken van de verwerking, wissen of vernietigen van gegevens;

7. „match": de opeenvolging van de volgende stappen:

   a) een eindgebruiker voert een doorzoeking uit in SIS;

   b) uit die doorzoeking blijkt dat een andere lidstaat een signalering in SIS heeft ingevoerd, alsmede

   c) gegevens betreffende de signalering in SIS komen overeen met de gegevens van de doorzoeking;

8. „hit": een match die voldoet aan de volgende criteria:

   a) hij is bevestigd door:

      i) de eindgebruiker, of

      ii) de bevoegde autoriteit overeenkomstig de nationale procedures, indien de betrokken match gebaseerd was op de vergelijking van biometrische gegevens,

      en

   b) er wordt om verdere acties verzocht;

9. „signalerende lidstaat": de lidstaat die de signalering in SIS heeft ingevoerd;

10. „verlenende lidstaat": de lidstaat die overweegt een verblijfsvergunning of een visum voor verblijf van langere duur te verlenen of te verlengen, of verleend of verlengd heeft, en die bij de raadplegingsprocedure met een andere lidstaat betrokken is;

11. „uitvoerende lidstaat": de lidstaat die de gevraagde actie naar aanleiding van een hit uitvoert of heeft uitgevoerd;

12. „eindgebruiker": een personeelslid van een bevoegde autoriteit dat gemachtigd is CS-SIS, N.SIS of een technische kopie daarvan rechtstreeks te doorzoeken;

13. „biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke of fysiologische kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, met name foto's, gezichtsopnamen en dactyloscopische gegevens;

14. „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;

15. „gezichtsopname": een digitale afbeelding van het gezicht met toereikende resolutie en kwaliteit voor gebruik bij geautomatiseerde biometrische matching;

16. „terugkeer": terugkeer als omschreven in artikel 3, punt 3, van Richtlijn 2008/115/EG;

17. „inreisverbod": een inreisverbod als omschreven in artikel 3, punt 6, van Richtlijn 2008/115/EG;

18. „terroristische misdrijven": strafbare feiten naar nationaal recht bedoeld in de artikelen 3 tot en met 14 van Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad ([1]), of, voor de niet door die richtlijn gebonden lidstaten, strafbare feiten die daaraan gelijkwaardig zijn;

19. „verblijfsvergunning": een verblijfsvergunning als omschreven in artikel 2, punt 16, van Verordening (EU) 2016/399 van het Europees Parlement en de Raad ([2]);

20. „visum voor een verblijf van langere duur": een visum als omschreven in artikel 18, lid 1, van de overeenkomst ter uitvoering van het Akkoord van Schengen;

21. „gevaar voor de volksgezondheid": een gevaar voor de volksgezondheid als gedefinieerd in artikel 2, punt 21, van Verordening (EU) 2016/399.

([1]) Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad (PB L 88 van 31.3.2017, blz. 6).

([2]) 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) (PB L 77 van 23.3.2016, blz. 1).

Artikel 4

Technische architectuur en werkwijze van SIS

1. SIS bestaat uit:

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

i) een technisch ondersteunende voorziening („CS-SIS") die een databank (de „SIS-databank"), met inbegrip van een CS-SIS-back-up, bevat;

ii) 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, en minstens één nationale of gedeelde N.SIS-back-up, en

c) een communicatie-infrastructuur tussen CS-SIS, CS-SIS-back-up en de 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.

Een N.SIS als bedoeld onder b), kan een gegevensbestand bevatten (een „nationale kopie") met een volledige of gedeeltelijke kopie van de SIS-databank. Twee of meer lidstaten kunnen in een van hun N.SIS een gedeelde kopie onderbrengen die door die lidstaten gezamenlijk kan worden gebruikt. Een dergelijke gedeelde kopie wordt beschouwd als de nationale kopie van elk van de deelnemende lidstaten.

Een gedeelde N.SIS-back-up als bedoeld onder b), kan gezamenlijk door twee of meer lidstaten worden gebruikt. In dergelijke gevallen wordt de gedeelde back-up beschouwd als de N.SIS-back-up van elk van die deelnemende lidstaten. Het N.SIS en de back-up daarvan kunnen tegelijkertijd worden gebruikt om een ononderbroken beschikbaarheid voor de eindgebruikers te waarborgen.

Lidstaten die voornemens zijn een gedeelde kopie of een gedeelde N.SIS-back-up op te zetten die gezamenlijk kan worden gebruikt, komen hun respectieve verantwoordelijkheden schriftelijk overeen. Zij melden hun regeling aan de Commissie.

De communicatie-infrastructuur ondersteunt en draagt bij tot het waarborgen van de ononderbroken beschikbaarheid van SIS. Zij omvat redundante en afzonderlijke paden voor de verbindingen tussen CS-SIS en de CS-SIS-back-up en ook redundante en afzonderlijke paden voor de verbindingen tussen ieder nationaal SIS-netwerktoegangspunt, en CS-SIS en de CS-SIS-back-up.

2. SIS-gegevens worden door de lidstaten ingevoerd, bijgewerkt, gewist en doorzocht via hun eigen N.SIS. De lidstaten die een gedeeltelijke of volledige nationale kopie of een gedeeltelijke of volledige gedeelde kopie gebruiken, maken die kopie beschikbaar om op het grondgebied van elk van die lidstaten geautomatiseerde doorzoeking mogelijk te maken. De gedeeltelijke nationale of gedeelde kopie bevat ten minste de gegevens als bedoeld in artikel 20, lid 2, onder a) tot en met v). De N.SIS-gegevensbestanden van andere lidstaten kunnen niet worden doorzocht, behalve in het geval van gedeelde kopieën.

3. CS-SIS zorgt voor technische toezichts- en beheersfuncties en heeft een CS-SIS-back-up die alle functies van de hoofd-CS-SIS kan overnemen wanneer dit uitvalt. CS-SIS en de CS-SIS-back-up bevinden zich op de twee technische locaties van eu-LISA.

4. eu-LISA voert technische oplossingen door om de ononderbroken beschikbaarheid van SIS te versterken, hetzij door de gelijktijdige werking van de CS-SIS en de back-up van de CS-SIS, mits de back-up van de CS-SIS kan blijven zorgen voor de werking van SIS als de CS-SIS uitvalt, hetzij door verdubbeling van het systeem of de componenten ervan. Niettegenstaande de procedurele voorschriften in artikel 10 van Verordening (EU) 2018/1726 maakt eu-LISA uiterlijk op 28 december 2019 een studie van de opties voor technische oplossingen, met een onafhankelijke effectbeoordeling en kosten-batenanalyse.

5. Zo nodig kan eu-LISA in uitzonderlijke omstandigheden tijdelijk een extra kopie van de SIS-databank ontwikkelen.

6. CS-SIS levert de nodige diensten voor het invoeren en verwerken van SIS-gegevens, inclusief voor doorzoekingen van de SIS-databank. Voor de lidstaten die een nationale of gedeelde kopie gebruiken, verzorgt CS-SIS:

a) de online bijwerking van de nationale kopieën;

b) de synchronisatie van en de samenhang tussen de nationale kopieën en de SIS-databank, en

c) het proces van de initialisatie en het herstel van de nationale kopieën.

7. CS-SIS zorgt voor 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 Unie. Die kosten omvatten de werkzaamheden in verband met CS-SIS teneinde de levering van de in artikel 4, lid 6, bedoelde diensten te verzekeren.

2. Om de kosten van de uitvoering van deze verordening te dekken, wordt financiering toegewezen uit het totaalbedrag van 791 miljoen EUR waarbij in artikel 5, lid 5, onder b), van Verordening (EU) nr. 515/2014 is voorzien.

3. Van het in lid 2 bedoelde totaalbedrag en onverminderd verdere financiering voor dit doel uit andere bronnen van de algemene begroting van de Unie, wordt een bedrag van 31 098 000 EUR aan eu-LISA toegewezen. Dergelijke financiering wordt uitgevoerd in indirect beheer en draagt bij tot de verwezenlijking van de technische ontwikkelingen die krachtens deze verordening vereist zijn met betrekking tot het centrale SIS en de communicatie-infrastructuur, evenals daarmee verband houdende opleidingsactiviteiten.

4. Van het in lid 2 bedoelde totaalbedrag krijgen de lidstaten die deelnemen aan Verordening (EU) nr. 515/2014 een aanvullend algemeen bedrag van 36 810 000 EUR toegewezen dat in gelijke delen moet worden verdeeld via een vast bedrag dat bij hun basistoewijzing komt. Deze financiering wordt uitgevoerd in gedeeld beheer en is volledig bestemd voor de snelle en doeltreffende opwaardering van de betrokken nationale systemen, overeenkomstig de vereisten van deze verordening.

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

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 ervan op de NI-SIS.

Iedere lidstaat is verantwoordelijk voor het waarborgen van de ononderbroken beschikbaarheid van SIS-gegevens voor eindgebruikers.

Elke lidstaat geeft zijn signaleringen door via zijn N.SIS.

Artikel 7

N.SIS-instantie en Sirene-bureau

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

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

2. Elke lidstaat wijst een nationale autoriteit aan die 24 uur per dag, zeven dagen per week operationeel is en die ervoor zorgt dat alle aanvullende informatie overeenkomstig het Sirene-handboek wordt uitgewisseld en beschikbaar is (het Sirene-bureau). Elk Sirene-bureau fungeert als een centraal contactpunt voor zijn lidstaat voor de uitwisseling van aanvullende informatie in verband met signaleringen, en om het ondernemen van de gevraagde actie te vergemakkelijken wanneer signaleringen van personen in SIS zijn ingevoerd en die personen na een hit worden gelokaliseerd.

Elk Sirene-bureau heeft overeenkomstig het nationale recht gemakkelijke al dan niet rechtstreeks toegang tot alle relevante nationale informatie, met inbegrip van nationale databanken en alle informatie over de signaleringen van zijn lidstaat, en tot deskundigenadvies, om snel en binnen de in artikel 8 bepaalde tijdslimiet te kunnen reageren op verzoeken om aanvullende informatie.

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

3. De lidstaten voorzien eu-LISA van details van hun N.SIS-instantie en hun Sirene-bureau. eu-LISA maakt de lijst van de N.SIS-instanties en de Sirene-bureaus bekend, samen met de in artikel 41, 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 tijdige en doeltreffende uitwisseling van aanvullende informatie te waarborgen. Indien geen communicatie-infrastructuur voorhanden is, gebruiken de lidstaten andere afdoende beveiligde technische middelen voor de uitwisseling van aanvullende informatie. Een lijst met afdoende beveiligde technische middelen wordt ingevoerd in het Sirene-handboek.

2. Aanvullende informatie wordt alleen gebruikt voor het doel waarvoor zij is doorgegeven overeenkomstig artikel 49, tenzij vooraf toestemming voor een ander gebruik is verkregen van de signalerende lidstaat.

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

Uiterst dringende verzoeken om aanvullende informatie worden op de Sirene-formulieren met „URGENT" gemarkeerd met vermelding van de reden van de urgentie.

4. De Commissie stelt uitvoeringshandelingen vast met daarin nadere bepalingen over de taken van de Sirene-bureaus uit hoofde van deze verordening en de uitwisseling van aanvullende informatie in de vorm van een handboek, getiteld het „Sirene-handboek". Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 9

Naleving van technische en functionele vereisten

1. Bij het opzetten van zijn N.SIS conformeert elke lidstaat zich aan de gemeenschappelijke normen, protocollen en technische procedures die zijn vastgesteld om de verenigbaarheid van zijn N.SIS met het centrale SIS te waarborgen met het oog op een snelle en doeltreffende gegevensdoorgifte.

2. Indien een lidstaat een nationale kopie gebruikt, zorgt hij er met behulp van de door de CS-SIS geleverde diensten en de in artikel 4, lid 6, bedoelde automatische bijwerking voor dat de in de nationale kopie opgeslagen gegevens identiek en consistent zijn met de SIS-databank, en dat een doorzoeking die nationale kopie een resultaat oplevert dat gelijkwaardig is aan een doorzoeking van de SIS-databank.

3. De eindgebruikers ontvangen, met name, de gegevens die zij voor de uitvoering van hun taken nodig hebben en, indien nodig, alle beschikbare gegevens om de betrokkene te kunnen identificeren en om de gevraagde actie te kunnen ondernemen.

4. De lidstaten en eu-LISA voeren regelmatig tests uit om de technische conformiteit van de nationale kopieën bedoeld in lid 2 te controleren. Met de resultaten van die tests wordt rekening gehouden als onderdeel van het mechanisme dat is ingesteld bij Verordening (EU) nr. 1053/2013 van de Raad ([1]).

5. De Commissie stelt uitvoeringshandelingen vast om de in lid 1 van dit artikel bedoelde normen, protocollen en technische procedures vast te leggen en te ontwikkelen. Deze uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 10

Beveiliging — Lidstaten

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

a) de gegevens fysiek worden beschermd, onder meer met noodplannen voor de bescherming van vitale 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 de gegevensdragers);

([1]) Verordening (EU) nr. 1053/2013 van de Raad 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 het Uitvoerend Comité van 16 september 1998 tot oprichting van de Permanente Schengenbeoordelings- en toepassingscommissie (PB L 295 van 6.11.2013, blz. 27).

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 voorkomen dat gegevens onrechtmatig in SIS worden verwerkt en dat in SIS verwerkte gegevens onrechtmatig worden gewijzigd of gewist (controle op de invoering van gegevens);

g) wordt gewaarborgd dat degenen die bevoegd zijn een systeem voor automatische gegevensverwerking te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft door middel van persoonlijke en unieke gebruikersidentificatiemiddelen en geheime toegangsprocedures (controle op de toegang tot de gegevens);

h) wordt gewaarborgd dat alle autoriteiten met toegangsrecht tot 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 die profielen desgevraagd onverwijld ter beschikking worden gesteld van de toezichthoudende autoriteiten als bedoeld in artikel 55, lid 1 (personeelsprofielen);

i) wordt gewaarborgd, dat kan worden nagegaan en vastgesteld aan welke instanties persoonsgegevens door middel van datatransmissieapparatuur kunnen worden doorgegeven (controle op de doorgifte);

j) 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 opname);

k) 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);

l) wordt toegezien op de doeltreffendheid van de in dit lid bedoelde beveiligingsmaatregelen en de nodige organisatorische maatregelen worden genomen met betrekking tot het intern toezicht om de naleving van deze verordening te waarborgen (interne audit);

m) ervoor wordt gezorgd dat geïnstalleerde systemen in geval van storing opnieuw kunnen worden ingesteld naar normale werking (herstel), en

n) ervoor wordt gezorgd dat de functies van SIS correct worden uitgevoerd, dat fouten gesignaleerd worden (betrouwbaarheid) en dat in SIS opgeslagen persoonsgegevens niet door verkeerd functioneren van het systeem beschadigd kunnen worden (integriteit).

2. Voor de beveiliging van de verwerking en uitwisseling van aanvullende gegevens, waaronder de beveiliging van de kantoren van de Sirene-bureaus, 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 34 bedoelde autoriteiten nemen de lidstaten maatregelen die gelijkwaardig zijn aan die als bedoeld in lid 1 van dit artikel.

4. De in de leden 1, 2 en 3 beschreven maatregelen kunnen deel uitmaken van een algemene beveiligingsbenadering en -plan op nationaal niveau die meerdere IT-systemen omvatten. In dergelijke gevallen zijn de in dit artikel vastgelegde vereisten en hun toepasbaarheid op SIS in een dergelijk plan duidelijk identificeerbaar en worden erdoor gewaarborgd.

Artikel 11

Vertrouwelijkheid — Lidstaten

1. Elke lidstaat past, in overeenstemming met zijn nationaal 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.

2. Indien een lidstaat bij de uitvoering van taken in verband met SIS samenwerkt met een externe contractant, ziet het nauwlettend toe op de werkzaamheden van die contractant om de naleving van alle bepalingen van deze verordening te waarborgen, met name de bepalingen inzake beveiliging, vertrouwelijkheid en gegevensbescherming.

3. Het operationeel beheer van het N.SIS of van technische kopieën wordt niet toevertrouwd aan particuliere ondernemingen of particuliere organisaties.

Artikel 12

Bijhouden van logbestanden op nationaal niveau

1. De lidstaten zorgen ervoor dat elke toegang tot en uitwisseling van persoonsgegevens in CS-SIS in logbestanden in hun N.SIS wordt geregistreerd met het oog op controle op de rechtmatigheid van de doorzoeking, toezicht op de rechtmatigheid van de gegevensverwerking, intern toezicht, de goede werking van N.SIS, alsmede de integriteit en beveiliging van de gegevens. Dit vereiste is niet van toepassing op de automatische processen bedoeld in artikel 4, lid 6, onder a), b) en c).

2. De logbestanden bevatten met name signaleringsgeschiedenis, de datum en het tijdstip van de gegevensverwerking, de voor de doorzoeking gebruikte gegevens, een verwijzing naar de verwerkte gegevens, alsmede de persoonlijke en unieke gebruikersidentificatiemiddelen van de bevoegde autoriteit en van de persoon die de gegevens verwerkt.

3. Als voor de doorzoeking dactyloscopische gegevens of een gezichtsopname worden gebruikt overeenkomstig artikel 33, bevatten de logbestanden, in afwijking van lid 2 van dit artikel, het soort gegevens dat voor het uitvoeren van de doorzoeking wordt gebruikt, in plaats van de eigenlijke gegevens.

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

5. Logbestanden mogen langer dan de in lid 4 bedoelde perioden worden bewaard indien zij nodig zijn in het kader van lopende monitoringprocedures.

6. De nationale bevoegde autoriteiten die zijn belast met het controleren van de rechtmatigheid van doorzoekingen, met het toezicht op de rechtmatigheid van de gegevensverwerking, met intern toezicht 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 de logbestanden met het oog op het vervullen van hun taken.

Artikel 13

Intern toezicht

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 toezichthoudende autoriteit.

Artikel 14

Opleiding van het personeel

1. Alvorens te worden gemachtigd tot de verwerking van in SIS opgeslagen gegevens, en vervolgens op regelmatige basis, krijgt het personeel van de autoriteiten met toegangsrecht tot SIS een adequate opleiding over gegevensbeveiliging, grondrechten met inbegrip van gegevensbescherming, en de in het Sirene-handboek vastgelegde regels en procedures voor gegevensverwerking. Het personeel wordt op de hoogte gebracht van alle relevante bepalingen inzake strafbare feiten en sancties, inclusief degene die zijn vastgesteld in artikel 59.

2. De lidstaten beschikken over een nationaal opleidingsprogramma over SIS, dat opleidingen omvat voor zowel de eindgebruikers als het personeel van de Sirene-bureaus.

Dat opleidingsprogramma kan deel uitmaken van een algemeen opleidingsprogramma op nationaal niveau dat opleidingen op andere relevante gebieden omvat.

3. Gemeenschappelijke opleidingen worden ten minste eenmaal per jaar op Unieniveau georganiseerd om de samenwerking tussen de Sirene-bureaus te vergroten.

HOOFDSTUK III

VERANTWOORDELIJKHEDEN VAN EU-LISA

Artikel 15

Operationeel beheer

1. eu-LISA is verantwoordelijk voor het operationele beheer van het centrale SIS. eu-LISA 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. eu-LISA 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;

d) begrotingsuitvoeringstaken;

e) aanschaf en vernieuwing, en

f) contractuele aangelegenheden.

3. eu-LISA wordt tevens belast met de volgende taken met betrekking tot de Sirene-bureaus en de communicatie tussen de Sirene-bureaus:

a) de coördinatie, het beheer en de ondersteuning van testactiviteiten;

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

c) het beheer van de gevolgen van technische wijzigingen die een impact hebben op zowel SIS als de uitwisseling van aanvullende informatie tussen de Sirene-bureaus.

4. eu-LISA ontwikkelt en onderhoudt een mechanisme en procedures voor het uitvoeren van kwaliteitscontroles op de gegevens in CS-SIS. Het brengt daarover regelmatig verslag uit aan de lidstaten.

eu-LISA rapporteert regelmatig aan de Commissie welke kwesties zijn geconstateerd en welke lidstaten hierbij zijn betrokken.

De Commissie legt aan het Europees Parlement en de Raad regelmatig een verslag voor over aangetroffen problemen met de kwaliteit van de gegevens.

5. eu-LISA verricht ook taken met betrekking tot het aanbieden van opleiding in het technische gebruik van SIS en inzake maatregelen ter verbetering van de kwaliteit van SIS-gegevens.

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

7. De Commissie stelt een uitvoeringshandeling vast om de technische voorschriften van de communicatie-infrastructuur vast te leggen. Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 16

Beveiliging — eu-LISA

1. eu-LISA 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 vitale 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 de 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 voorkomen dat gegevens onrechtmatig in SIS worden verwerkt en dat in SIS verwerkte gegevens onrechtmatig worden gewijzigd of gewist (controle op de invoering van gegevens);

g) wordt gewaarborgd dat degenen die bevoegd zijn een systeem voor automatische gegevensverwerking te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft door middel van persoonlijke en unieke gebruikersidentificatiemiddelen en geheime toegangsprocedures (controle op de toegang tot de gegevens);

h) 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 gegevensverwerkingsfaciliteiten, en opdat die profielen desgevraagd onverwijld ter beschikking worden gesteld van de Europese Toezichthouder voor gegevensbescherming (personeelsprofielen);

i) wordt gewaarborgd, dat kan worden nagegaan en vastgesteld aan welke instanties persoonsgegevens door middel van datatransmissieapparatuur kunnen worden doorgegeven (controle op de doorgifte);

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

k) 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);

l) wordt toegezien op de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen en de nodige organisatorische maatregelen voor het intern toezicht worden genomen om de naleving van deze verordening te waarborgen (interne audit).

m) ervoor wordt gezorgd dat geïnstalleerde systemen in geval van storing opnieuw kunnen worden ingesteld naar normale werking (herstel);

n) ervoor wordt gezorgd dat de functies van SIS correct worden uitgevoerd, dat fouten gesignaleerd worden (betrouwbaarheid) en dat in SIS opgeslagen persoonsgegevens niet door verkeerd functioneren van het systeem beschadigd kunnen worden (integriteit), en

o) de beveiliging van zijn technische locaties wordt gewaarborgd.

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

Artikel 17

Vertrouwelijkheid — eu-LISA

1. Onverminderd artikel 17 van het Statuut, past eu-LISA adequate voorschriften inzake het beroepsgeheim of een gelijkwaardige geheimhoudingsplicht toe op iedere persoon die met SIS-gegevens moet werken, aan de hand van een norm die vergelijkbaar is met die van artikel 11 van deze verordening. Die 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 eu-LISA maatregelen die gelijkwaardig zijn aan die als bedoeld in lid 1.

3. Indien eu-LISA bij de uitvoering van taken in verband met SIS samenwerkt met een externe contractant, ziet het nauwlettend toe op de werkzaamheden van die contractant, om de naleving van alle bepalingen van deze verordening te waarborgen, met name de bepalingen inzake beveiliging, vertrouwelijkheid en gegevensbescherming.

4. Het operationeel beheer van CS-SIS wordt niet toevertrouwd aan particuliere ondernemingen of particuliere organisaties.

Artikel 18

Bijhouden van logbestanden op centraal niveau

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

2. De logbestanden bevatten met name de signaleringsgeschiedenis, de datum en het tijdstip van de gegevensverwerking, de voor de doorzoeking gebruikte gegevens, een verwijzing naar de verwerkte gegevens, alsmede de persoonlijke en unieke gebruikersidentificatiemiddelen van de bevoegde autoriteit die de gegevens verwerkt.

3. Als voor de doorzoeking dactyloscopische gegevens of gezichtsopnamen worden gebruikt overeenkomstig artikel 33, bevatten de logbestanden, in afwijking van lid 2 van dit artikel, het soort gegevens dat voor het uitvoeren van de doorzoeking wordt gebruikt, in plaats van de eigenlijke gegevens.

4. De logbestanden worden alleen voor het in lid 1 bedoelde doel gebruikt en worden drie jaar na het creëren ervan gewist. De logbestanden die de signaleringsgeschiedenis bevatten, worden drie jaar na het wissen van de signaleringen gewist.

5. Logbestanden mogen langer dan de in lid 4 bedoelde perioden worden bewaard indien zij nodig zijn in het kader van lopende monitoringprocedures.

6. Ter uitvoering van het intern toezicht en om een goede werking van CS-SIS en de integriteit en beveiliging van gegevens te garanderen, heeft eu-LISA, binnen de grenzen van zijn bevoegdheid, toegang tot die logbestanden.

De Europese Toezichthouder voor gegevensbescherming heeft op verzoek toegang tot die logbestanden, binnen de grenzen van zijn bevoegdheid, en met het oog op de vervulling van zijn taken.

HOOFDSTUK IV

PUBLIEKSVOORLICHTING

Artikel 19

SIS-voorlichtingscampagnes

Zodra deze verordening wordt toegepast, organiseert de Commissie in samenwerking met de nationale toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming een campagne om het publiek te informeren omtrent de doelstellingen van SIS, de in SIS opgeslagen gegevens, de autoriteiten die toegang hebben tot SIS, en de rechten van de betrokkenen. De Commissie herhaalt op gezette tijden dit soort campagnes, in samenwerking met de toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming. De Commissie onderhoudt een openbaar toegankelijke website met alle relevante informatie over SIS. De lidstaten ontwikkelen en implementeren in samenwerking met hun toezichthoudende autoriteiten de nodige beleidsinitiatieven om hun burgers en ingezetenen algemene voorlichting over SIS te geven.

HOOFDSTUK V

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

Artikel 20

Gegevenscategorieën

1. Onverminderd artikel 8, lid 1, en de bepalingen van deze verordening met betrekking tot de opslag van extra gegevens, bevat SIS alleen de door elke lidstaat verstrekte gegevenscategorieën, als vereist voor de in de artikelen 24 en 25 genoemde doeleinden.

2. Elke signalering in SIS die informatie over personen bevat, omvat uitsluitend de onderstaande gegevens:

a) achternamen;

b) voornamen;

c) namen bij de geboorte;

d) voorheen gebruikte namen en aliassen;

e) bijzondere, onveranderlijke objectieve fysieke kenmerken;

f) geboorteplaats;

g) geboortedatum;

h) geslacht;

i) alle huidige en voorgaande nationaliteiten;

j) de vermelding of de betrokkene:

   i) gewapend is;

   ii) gewelddadig is;

   iii) ondergedoken of ontsnapt is;

   iv) een risico op zelfdoding vertoont;

   v) een gevaar voor de volksgezondheid vormt, of

   vi) betrokken is bij een in de artikelen 3 tot en met 14 van Richtlijn (EU) 2017/541 bedoelde activiteit;

k) de reden van signalering;

l) de signalerende autoriteit;

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

n) de bij een hit te ondernemen actie;

o) links naar andere signaleringen ingevolge artikel 48;

p) of de betrokken persoon een familielid is van een burger van de Unie of van een andere persoon die een begunstigde is van de in artikel 26 bedoelde rechten van vrij verkeer geniet;

q) of de beslissing tot weigering van toegang en verblijf gebaseerd is op:

i) een eerdere veroordeling als bedoeld in artikel 24, lid 2, onder a);

ii) een ernstige veiligheidsdreiging als bedoeld in artikel 24, lid 2, onder b);

iii) het omzeilen van de Uniewetgeving of nationale wetgeving met betrekking tot binnenkomst en verblijf als bedoeld in artikel 24, lid 2, onder c);

iv) een inreisverbod als bedoeld in artikel 24, lid 1, onder b), of

v) een beperkende maatregel als bedoeld in artikel 25;

r) het soort strafbaar feit;

s) de categorie van de identificatiedocumenten;

t) het land van afgifte van de identificatiedocumenten;

u) het (de) nummer(s) van de identificatiedocumenten;

v) de datum van afgifte van de identificatiedocumenten;

w) foto's en gezichtsopnamen;

x) dactyloscopische gegevens;

y) een kopie van de identificatiedocumenten, indien mogelijk in kleur.

3. De Commissie stelt uitvoeringshandelingen vast om technische voorschriften vast te leggen en te ontwikkelen inzake het invoeren, bijwerken, wissen en doorzoeken van de in lid 2 van dit artikel bedoelde gegevens en inzake de in lid 4 van dit artikel bedoelde gemeenschappelijke normen. Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

4. Technische voorschriften worden ook gevolgd voor doorzoekingen in CS-SIS, in nationale of gedeelde kopieën en in uit hoofde van artikel 41, lid 2, gemaakte technische kopieën. Zij zijn gebaseerd op gemeenschappelijke normen.

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 een signalering in SIS te rechtvaardigen.

2. Wanneer het in artikel 24, lid 1, onder a), bedoelde besluit tot weigering van toegang en verblijf verband houdt met een terroristisch misdrijf, wordt de zaak beschouwd als gepast, relevant en belangrijk genoeg om een signalering in SIS te rechtvaardigen. Om redenen van openbare en nationale veiligheid kunnen lidstaten bij uitzondering geen signalering invoeren, wanneer te verwachten valt dat die signalering officiële of justitiële onderzoeken, opsporingsonderzoeken of procedures zal belemmeren.

Artikel 22

Vereisten voor de invoering van een signalering

1. De reeks gegevens die minimaal nodig is om een signalering in SIS in te voeren, bestaat uit de gegevens als bedoeld in artikel 20, lid 2, onder a), g), k), m), n) en q). De overige in dat lid bedoelde gegevens worden eveneens in SIS ingevoerd als deze beschikbaar zijn.

2. De in artikel 20, lid 2, onder e), van deze verordening bedoelde gegevens worden uitsluitend ingevoerd indien dat strikt noodzakelijk is ter identificatie van de betrokken onderdaan van een derde land. Wanneer dergelijke gegevens worden ingevoerd, zorgen de lidstaten ervoor dat artikel 9 van Verordening (EU) 2016/679 wordt nageleefd.

Artikel 23

Verenigbaarheid van signaleringen

1. Voordat een signalering wordt ingevoerd, controleert de lidstaat of voor de betrokken persoon reeds een signalering in SIS is ingevoerd. Daartoe wordt ook een controle met dactyloscopische gegevens verricht, indien deze beschikbaar zijn.

2. Voor eenzelfde persoon wordt per lidstaat in SIS slechts één signalering ingevoerd. Indien nodig kunnen andere lidstaten overeenkomstig lid 3 nieuwe signaleringen voor diezelfde persoon invoeren.

3. Een lidstaat die een nieuwe signalering wil invoeren met betrekking tot een persoon voor wie reeds een signalering in SIS is ingevoerd, controleert of de signaleringen niet onverenigbaar zijn. Indien ze niet onverenigbaar zijn, mag de lidstaat de nieuwe signalering invoeren. Indien de signaleringen onverenigbaar zijn, plegen de Sirene-bureaus van de betrokken lidstaten onderling overleg door het uitwisselen van aanvullende informatie, teneinde overeenstemming te bereiken. Regels inzake de verenigbaarheid van signaleringen worden vastgesteld in het Sirene-handboek. Van de regels inzake verenigbaarheid kan na overleg tussen de lidstaten worden afgeweken indien wezenlijke nationale belangen in het geding zijn.

4. Bij hits naar aanleiding van meervoudige signaleringen ten aanzien van dezelfde persoon, volgt de uitvoerende lidstaat de in het Sirene-handboek vastgelegde prioriteitsregels voor signaleringen.

Indien voor een persoon meervoudige signaleringen door verschillende lidstaten zijn ingevoerd, worden signaleringen met het oog op aanhouding die zijn ingevoerd overeenkomstig artikel 26 van Verordening (EU) 2018/1862, onverminderd artikel 25 van die Verordening, bij voorrang uitgevoerd.

Artikel 24

Voorwaarden voor de invoering van signaleringen met het oog op weigering van toegang en verblijf

1. De lidstaten voeren een signalering in met het oog op weigering van toegang en verblijf uit indien aan een van de volgende voorwaarden is voldaan:

a) de lidstaat is tot de slotsom gekomen dat op basis van een individuele evaluatie, waarbij de persoonlijke omstandigheden van de betrokken onderdaan van een derde land en de gevolgen van een weigering van toegang en verblijf zijn geëvalueerd, de aanwezigheid van die onderdaan van een derde land op zijn grondgebied een bedreiging vormt voor de openbare orde of veiligheid of de nationale veiligheid, en de lidstaat heeft dientengevolge een administratieve of gerechtelijke beslissing tot weigering van toegang en verblijf genomen en heeft daartoe overeenkomstig zijn nationaal recht een nationale signalering met het oog op weigering van toegang en verblijf ingevoerd, of

b) de lidstaat heeft overeenkomstig procedures met inachtneming van Richtlijn 2008/115/EG een inreisverbod ten aanzien van een onderdaan van een derde land uitgevaardigd.

2. De in lid 1, onder a), genoemde situaties doen zich voor wanneer:

a) een onderdaan van een derde land in een lidstaat veroordeeld is voor een strafbaar feit waarvoor een vrijheidsstraf van ten minste één jaar geldt;

b) er zijn gegronde redenen om aan te nemen dat een onderdaan van een derde land een ernstig strafbaar feit, onder meer een terroristisch misdrijf, heeft gepleegd of er zijn duidelijke aanwijzingen dat hij overweegt een dergelijk feit te plegen op het grondgebied van een lidstaat, of

c) een onderdaan van een derde land heeft het Unierecht of het nationale recht inzake binnenkomst in en verblijf op het grondgebied van de lidstaten omzeild of gepoogd deze te omzeilen.

3. De signalerende lidstaat zorgt ervoor dat de signalering in SIS van kracht wordt zodra de betrokken onderdaan van een derde land het grondgebied van de lidstaten heeft verlaten, of zo spoedig mogelijk indien de signalerende lidstaat over duidelijke aanwijzingen beschikt dat dit het geval is, teneinde die onderdaan van een derde land te beletten opnieuw binnen te komen.

4. Personen ten aanzien van wie een in lid 1 bedoelde beslissing tot weigering van toegang en verblijf is genomen, kunnen tegen die beslissing in beroep gaan. Dergelijk beroep wordt ingesteld overeenkomstig het Unierecht en nationaal recht, die moeten voorzien in een doeltreffende voorziening voor de rechter.

Artikel 25

Voorwaarden voor de invoering 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 rechtshandeling 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 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. De signaleringen worden ingevoerd, geactualiseerd en gewist door de bevoegde autoriteit van de lidstaat die het voorzitterschap van de Raad van de Europese Unie bekleedde wanneer de maatregel is genomen. Indien die lidstaat geen toegang heeft tot SIS of tot overeenkomstig deze verordening ingevoerde signaleringen, wordt die verantwoordelijkheid genomen door de lidstaat die het volgende voorzitterschap bekleedt en die toegang heeft tot SIS, met inbegrip van overeenkomstig deze verordening ingevoerde signaleringen.

De lidstaten voorzien in de nodige procedures voor het invoeren, bijwerken en wissen van deze signaleringen.

Artikel 26

Voorwaarden voor de invoering van signaleringen van onderdanen van derde landen die begunstigden zijn van het recht van vrij verkeer binnen de Unie

1. Een signalering ten aanzien van een onderdaan van een derde land die een begunstigde is van het recht van vrij verkeer binnen de Unie overeenkomstig Richtlijn 2004/38/EG of een overeenkomst tussen de Unie of de Unie en haar lidstaten enerzijds, en een derde land anderzijds, voldoet aan de tot omzetting van die richtlijn of overeenkomst vastgestelde voorschriften.

2. In geval van een hit naar aanleiding van een signalering die overeenkomstig artikel 24 is ingevoerd met betrekking tot een onderdaan van een derde land die een begunstigde is het recht van vrij verkeer binnen de Unie, pleegt de uitvoerende lidstaat onmiddellijk overleg met de signalerende lidstaat via het uitwisselen van aanvullende informatie, teneinde onverwijld te besluiten welke actie moet worden ondernomen.

Artikel 27

Raadpleging voorafgaand aan het verlenen of verlengen van een verblijfsvergunning of een visum voor verblijf van langere duur

Indien een lidstaat verlening of verlenging overweegt van een verblijfsvergunning of een visum voor verblijf van langere duur van een onderdaan van een derde land voor wie een andere lidstaat een signalering met het oog op weigering van toegang en verblijf heeft ingevoerd, raadplegen de betrokken lidstaten elkaar via de uitwisseling van aanvullende informatie, volgens de onderstaande regels:

a) voorafgaand aan de verlening of verlenging van de verblijfsvergunning of het visum voor verblijf van langere duur raadpleegt de verlenende lidstaat de signalerende lidstaat;

b) de signalerende lidstaat beantwoordt het raadplegingsverzoek binnen tien kalenderdagen;

c) bij gebreke van een antwoord binnen de onder b) genoemde termijn, wordt de signalerende lidstaat geacht geen bezwaar te hebben tegen de verlening of verlenging van de verblijfsvergunning of het visum voor verblijf van langere duur;

d) bij het nemen van de betrokken beslissing houdt de verlenende lidstaat rekening met de motivering van de beslissing van de signalerende lidstaat en neemt hij, overeenkomstig het nationaal recht, elk gevaar voor de openbare orde of de openbare veiligheid dat de aanwezigheid van de betrokken onderdaan van een derde land op het grondgebied van een lidstaat kan vormen, in overweging;

e) de verlenende lidstaat stelt de signalerende lidstaat van zijn beslissing in kennis, en

f) indien de verlenende lidstaat de signalerende lidstaat ervan in kennis stelt dat hij voornemens is of besloten heeft de verblijfstitel of het visum voor verblijf van langere duur te verlenen of te verlengen, of dat hij daartoe heeft besloten, wist de signalerende lidstaat de signalering met het oog op weigering van toegang en verblijf.

De uiteindelijke beslissing tot het al dan niet verlenen van een verblijfsvergunning of een visum voor verblijf van langere duur aan een onderdaan van een derde land berust bij de verlenende lidstaat.

Artikel 28

Raadpleging voorafgaand aan de invoering van een signalering met het oog op weigering van toegang en verblijf

Indien een lidstaat een beslissing als bedoeld in artikel 24, lid 1, heeft genomen, en overweegt een signalering met het oog op weigering van toegang en verblijf in te voeren ten aanzien van een onderdaan van een derde land die houder is van een door een andere lidstaat verleende geldige verblijfsvergunning of geldig visum voor verblijf van langere duur, raadplegen de betrokken lidstaten elkaar door aanvullende informatie uit te wisselen, volgens de onderstaande regels:

a) de lidstaat die de in artikel 24, lid 1, bedoelde beslissing heeft genomen, stelt de verlenende lidstaat van die beslissing in kennis;

b) de uit hoofde van de onder a) van dit artikel uitgewisselde informatie omvat voldoende details over de motivering van de in artikel 24, lid 1, bedoelde beslissing;

c) op basis van de informatie van de lidstaat die de in artikel 24, lid 1, bedoelde beslissing heeft genomen, overweegt de verlenende lidstaat of er redenen zijn om de verblijfsvergunning of het visum voor verblijf van langere duur in te trekken;

d) bij het nemen van de betrokken beslissing houdt de verlenende lidstaat rekening met de motivering van de lidstaat die de in artikel 24, lid 1, bedoelde beslissing heeft genomen, en neemt hij, overeenkomstig het nationaal recht, elk gevaar voor de openbare orde of de openbare veiligheid dat de aanwezigheid van de betrokken onderdaan van een derde land op het grondgebied van een lidstaat kan vormen, in overweging;

e) binnen 14 kalenderdagen na ontvangst van het verzoek om raadpleging stelt de verlenende lidstaat de lidstaat die de in artikel 24, lid 1, bedoelde beslissing heeft genomen in kennis van zijn beslissing, of, indien het voor de verlenende lidstaat onmogelijk was om binnen die termijn een beslissing te nemen, van zijn met redenen omkleed verzoek om de termijn van zijn antwoord bij uitzondering met maximaal twaalf bijkomende kalenderdagen te verlengen.

f) indien de verlenende lidstaat de lidstaat die de in artikel 24, lid 1, bedoelde beslissing heeft genomen ervan in kennis stelt dat hij de verblijfsvergunning of het visum voor verblijf van langere duur handhaaft, voert de lidstaat die de beslissing heeft genomen, de signalering inzake terugkeer niet in.

Artikel 29

Raadpleging na invoering van een signalering met het oog op weigering van toegang en verblijf

Indien blijkt dat een lidstaat een signalering met het oog op weigering van toegang en verblijf heeft ingevoerd ten aanzien een onderdaan van een derde land die houder is van een door een andere lidstaat afgegeven geldige verblijfsvergunning of geldig visum voor verblijf van langere duur, raadplegen de betrokken lidstaten elkaar door aanvullende informatie uit te wisselen, volgens de onderstaande regels:

a) de signalerende lidstaat informeert de verlenende lidstaat over de signalering met het oog op weigering van toegang en verblijf;

b) de uit hoofde van de onder a) uitgewisselde informatie omvat voldoende details over de redenen van de signalering met het oog op weigering van toegang en verblijf;

c) op basis van de door de signalerende lidstaat verstrekte informatie overweegt de verlenende lidstaat of er redenen zijn om de verblijfsvergunning of het visum voor verblijf van langere duur in te trekken;

d) bij het nemen van zijn beslissing houdt de verlenende lidstaat rekening met de redenen van de beslissing van de signalerende lidstaat en neemt hij, overeenkomstig het nationaal recht, elk gevaar voor de openbare orde of de openbare veiligheid dat de aanwezigheid van de betrokken onderdaan van een derde land op het grondgebied van een lidstaat kan vormen, in overweging;

e) binnen 14 kalenderdagen na ontvangst van het verzoek om raadpleging stelt de verlenende lidstaat de signalerende lidstaat in kennis van zijn beslissing, of, indien het voor de verlenende lidstaat onmogelijk was om binnen die termijn een beslissing te nemen, van zijn met redenen omkleed verzoek om de termijn van zijn antwoord bij uitzondering met maximaal twaalf bijkomende kalenderdagen te verlengen.

f) indien de verlenende lidstaat de signalerende lidstaat ervan in kennis stelt dat hij de verblijfstitel of het visum voor verblijf van langere duur handhaaft, wist de signalerende lidstaat onmiddellijk de signalering met het oog op weigering van toegang en verblijf.

Artikel 30

Raadpleging in geval van een hit betreffende een onderdaan van een derde land die houder is van een geldige verblijfsvergunning of geldig visum voor verblijf van langere duur

Indien een lidstaat een hit vaststelt naar aanleiding van een door een lidstaat ingevoerde signalering met het oog op weigering van toegang en verblijf ten aanzien van een onderdaan van een derde land die houder is van een door een andere lidstaat afgegeven geldige verblijfsvergunning of geldig visum voor verblijf van langere duur, raadplegen de betrokken lidstaten elkaar door aanvullende informatie uit te wisselen, volgens de onderstaande regels:

a) de uitvoerende lidstaat stelt de signalerende lidstaat van de situatie in kennis;

b) de signalerende lidstaat leidt de procedure van artikel 29 in;

c) de signalerende lidstaat stelt de uitvoerende lidstaat in kennis van het resultaat na de raadpleging.

De beslissing over de toegang van de onderdaan van een derde land wordt door de uitvoerende lidstaat genomen overeenkomstig Verordening (EU) 2016/399.

Artikel 31

Statistieken over de uitwisseling van informatie

De lidstaten verstrekken eu-LISA jaarlijks statistieken over de uitwisseling van informatie die overeenkomstig de artikelen 27 tot en met 30 heeft plaatsgevonden en over de gevallen waarin de in die artikelen gestelde termijnen niet zijn gehaald.

HOOFDSTUK VI

DOORZOEKING AAN DE HAND VAN BIOMETRISCHE GEGEVENS

Artikel 32

Specifieke voorschriften voor invoering van foto's, gezichtsopnamen en dactyloscopische gegevens

1. Uitsluitend foto's, gezichtsopnamen en dactyloscopische gegevens, als bedoeld in artikel 20, lid 2, onder w) en x), die voldoen aan de minimumnormen inzake gegevenskwaliteit en de technische specificaties, worden in SIS ingevoerd. Voordat die gegevens worden ingevoerd, wordt een kwaliteitscontrole uitgevoerd om vast te stellen of aan de minimumnormen inzake gegevenskwaliteit en de technische specificaties is voldaan.

2. De in SIS ingevoerde dactyloscopische gegevens bestaan uit één tot tien platte vingerafdrukken of één tot tien gerolde vingerafdrukken. Zij kunnen ook maximaal twee handpalmafdrukken omvatten.

3. Voor de opslag van de in lid 1 van dit artikel bedoelde biometrische gegevens worden overeenkomstig lid 4 van dit artikel minimumnormen inzake gegevenskwaliteit en technische specificaties vastgesteld. Die minimumnormen inzake gegevenskwaliteit en technische specificaties bepalen het kwaliteitsniveau dat vereist is om de gegevens te kunnen gebruiken voor het vaststellen van de identiteit van een persoon overeenkomstig artikel 33, lid 1, en voor het identificeren van een persoon overeenkomstig artikel 33, leden 2, 3 en 4.

4. De Commissie stelt uitvoeringshandelingen vast om de in de leden 1 en 3 van dit artikel bedoelde minimumnormen inzake gegevenskwaliteit en technische specificaties vast te leggen. Deze uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 33

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

1. Indien foto's, gezichtsopnamen en dactyloscopische gegevens beschikbaar zijn in een signalering in SIS, worden dergelijke foto's, gezichtsopnamen en dactyloscopische gegevens gebruikt om de identiteit te bevestigen van een persoon die naar aanleiding van een alfanumerieke doorzoeking van SIS is gevonden.

2. Dactyloscopische gegevens kunnen in alle gevallen worden doorzocht om een persoon te identificeren. Dactyloscopische gegevens worden evenwel doorzocht voor identificatiedoeleinden indien de identiteit van de persoon niet met behulp van andere middelen kan worden vastgesteld. Dactyloscopische gegevens mogen altijd worden doorzocht om een persoon te identificeren. Daartoe omvat het centrale SIS een geautomatiseerd vingerafdrukidentificatiesysteem (AFIS).

3. Dactyloscopische gegevens in SIS in verband met overeenkomstig artikelen 24 en 25 ingevoerde signaleringen kunnen tevens worden doorzocht aan de hand van volledige of onvolledige reeksen vingerafdrukken of handpalmafdrukken die zijn aangetroffen op de plaats delict van ernstige strafbare feiten of terroristische misdrijven die worden onderzocht, mits met een hoge mate van waarschijnlijkheid kan worden vastgesteld dat die afdrukken van een dader van het strafbare feit zijn en op voorwaarde dat de doorzoeking tegelijkertijd in de relevante nationale vingerafdrukdatabanken van de lidstaat wordt uitgevoerd.

4. Zodra het technisch mogelijk is en mits voor de identificatie een hoge betrouwbaarheid kan worden gewaarborgd, mogen foto's en gezichtsopnamen worden gebruikt om een persoon te identificeren bij reguliere grensdoorlaatposten.

Voordat deze functie in SIS wordt ingevoerd, brengt de Commissie een verslag uit over de beschikbaarheid, de gereedheid, en de betrouwbaarheid van de vereiste technologie. Het Europees Parlement wordt over dit verslag geraadpleegd.

Na de start van het gebruik van de functionaliteit bij reguliere grensdoorlaatposten is de Commissie overeenkomstig artikel 61 bevoegd ter aanvulling van onderhavige verordening gedelegeerde handelingen vast te stellen over de bepaling van andere omstandigheden waarin foto's en gezichtsopnamen mogen worden gebruikt voor de identificatie van personen.

HOOFDSTUK VII

TOEGANGSRECHT EN TOETSING EN WISSING VAN SIGNALERINGEN

Artikel 34

Nationale bevoegde autoriteiten met recht op toegang tot gegevens in SIS

1. De bevoegde nationale autoriteiten die verantwoordelijk zijn voor de identificatie van onderdanen van derde landen hebben toegang tot de in SIS ingevoerde gegevens en hebben het recht om deze gegevens direct in SIS of in een kopie van de SIS-databank te bevragen ten behoeve van:

a) grenscontrole, overeenkomstig Verordening (EU) 2016/399;

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

c) het voorkomen, opsporen, onderzoeken of vervolgen van terroristische misdrijven of andere ernstige strafbare feiten, of voor de tenuitvoerlegging van strafrechtelijke sancties, in de betrokken lidstaat, mits Richtlijn (EU) 2016/680 van toepassing is;

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, met inbegrip van verblijfsvergunningen en visa voor verblijf van langere duur, en in verband met de terugkeer van onderdanen van derde landen, alsmede het verrichten van controles van onderdanen van derde landen die het grondgebied van de lidstaten illegaal zijn binnengekomen of er illegaal verblijven;

e) veiligheidscontroles van onderdanen van derde landen die internationale bescherming vragen, voor zover de autoriteiten die de controles verrichten geen „beslissingsautoriteiten" zijn zoals gedefinieerd in artikel 2, onder f), van Richtlijn 2013/32/EU van het Europees Parlement en de Raad ([1]), en in voorkomend geval het verstrekken van advies overeenkomstig Verordening (EG) nr. 377/2004 van de Raad ([2]);

f) het onderzoeken van visumaanvragen en het nemen van beslissingen in verband met deze aanvragen, alsmede inzake nietigverklaring, intrekking of verlenging van visa, overeenkomstig Verordening (EG) nr. 810/2009 van het Europees Parlement en de Raad ([3]).

2. De nationale bevoegde autoriteiten die verantwoordelijk zijn voor naturalisatie hebben overeenkomstig het nationale recht, met het oog op het onderzoek van een aanvraag tot naturalisatie, recht op toegang tot gegevens in SIS en hebben het recht tot rechtstreekse doorzoeking daarvan.

3. Voor de toepassing van de artikelen 24 en 25 hebben ook de nationale justitiële autoriteiten, met inbegrip van de autoriteiten die belast zijn met de instelling van strafvervolging en van justitiële onderzoeken voorafgaand aan het in staat van beschuldiging stellen van een persoon, alsook hun coördinerende instanties, met het oog op de uitvoering van hun bij nationaal recht vastgestelde taken, recht op toegang tot de gegevens in SIS en tot rechtstreekse doorzoeking daarvan.

4. Ook de in lid 1, onder f), van dit artikel bedoelde autoriteiten hebben recht op toegang tot en doorzoeking van gegevens over persoonsdocumenten die zijn ingevoerd overeenkomstig artikel 38, lid 2, onder k) en l), van Verordening (EU) 2018/1862.

5. De in dit artikel bedoelde bevoegde autoriteiten worden ingevoerd in de in artikel 41, lid 8, bedoelde lijst.

Artikel 35

Toegang van Europol tot gegevens in SIS

1. Het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol), ingesteld bij Verordening (EU) 2016/794, heeft, indien nodig voor de vervulling van zijn mandaat, recht op toegang tot en doorzoeking van in SIS ingevoerde gegevens. Europol kan ook aanvullende informatie uitwisselen en vragen overeenkomstig de bepalingen van het Sirene-handboek.

2. Indien Europol bij een doorzoeking een signalering in SIS aantreft, stelt Europol de signalerende lidstaat daarvan in kennis door de uitwisseling van aanvullende informatie door middel van de communicatie-infrastructuur en overeenkomstig het Sirene-handboek. Totdat Europol de functies voor de uitwisseling van aanvullende informatie kan gebruiken, stelt het de signalerende lidstaat in kennis via de in Verordening (EU) 2016/794 bepaalde kanalen.

3. Europol mag de hem door de lidstaten verstrekte aanvullende informatie verwerken die door de lidstaten is verstrekt voor vergelijking van die informatie met zijn databanken en voor operationele analyseprojecten, om connecties of andere relevante verbanden op te sporen en voor de in artikel 18, lid 2, onder a), b) en c), van Verordening (EU) 2016/794 bedoelde strategische, thematische of operationele analyses. De verwerking van aanvullende informatie door Europol voor de toepassing van dit artikel geschiedt overeenkomstig die verordening.

4. Door doorzoeking van SIS of door de verwerking van aanvullende informatie verkregen informatie wordt door Europol alleen gebruikt indien de signalerende lidstaat daarmee instemt. Indien de lidstaat het gebruik van dergelijke informatie toestaat, wordt deze door Europol behandeld overeenkomstig Verordening (EU) 2016/794. Europol deelt die informatie alleen mee aan derde landen en organen indien de signalerende lidstaat daarmee instemt, met volledige naleving van het Unierecht inzake gegevensbescherming.

([1]) Richtlijn 2013/32/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende gemeenschappelijke procedures voor de toekenning en intrekking van de internationale bescherming (PB L 180 van 29.6.2013, blz. 60).

([2]) Verordening (EG) nr. 377/2004 van de Raad van 19 februari 2004 betreffende de oprichting van een netwerk van immigratieverbindingsfunctionarissen (PB L 64 van 2.3.2004, blz. 1).

([3]) 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).

5. Europol is ertoe gehouden:

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

b) niettegenstaande artikel 31, lid 1, van Verordening (EU) 2016/794, uiterlijk een jaar nadat de betreffende signalering is gewist, aanvullende informatie die persoonsgegevens bevat te wissen. In afwijking daarvan kan Europol, indien het informatie in zijn databanken of operationele analyseprojecten heeft over een geval dat met de aanvullende informatie verband houdt, de aanvullende informatie bij wijze van uitzondering verder bewaren, voor zover dit nodig is om zijn taken uit te voeren. Europol informeert de signalerende en de uitvoerende lidstaat over de verdere opslag van die aanvullende informatie en rechtvaardigt die verdere opslag;

c) de toegang tot gegevens in SIS, met inbegrip van aanvullende informatie, te beperken tot specifiek daartoe gemachtigd personeel van Europol dat toegang tot dergelijke gegevens nodig heeft om zijn taken te kunnen uitoefenen;

d) maatregelen als bedoeld in de artikelen 10, 11 en 13, vast te stellen en toe te passen, om beveiliging, vertrouwelijkheid en intern toezicht te waarborgen;

e) ervoor te zorgen dat personeel dat gemachtigd is SIS-gegevens te verwerken een geschikte opleiding en informatie krijgt overeenkomstig artikel 14, lid 1, en

f) onverminderd Verordening (EU) 2016/794, de Europese Toezichthouder voor gegevensbescherming in de gelegenheid te stellen toezicht te houden op de activiteiten die Europol verricht in de uitoefening van zijn recht op toegang tot en doorzoeking van gegevens in SIS, en bij de uitwisseling en verwerking van aanvullende informatie, en dit alles te evalueren.

6. Europol kopieert alleen gegevens uit SIS voor technische doeleinden, indien dat noodzakelijk is voor een rechtstreekse doorzoeking door naar behoren gemachtigd Europol-personeel. Deze verordening is van toepassing op dergelijke kopieën. De technische kopie wordt enkel 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. Om de rechtmatigheid van de gegevensverwerking te verifiëren, intern toezicht uit te voeren en een adequate beveiliging en integriteit van de gegevens te waarborgen, houdt Europol overeenkomstig de bepalingen van artikel 12 logbestanden bij van elke toegang tot en doorzoeking van SIS. Deze logbestanden en documentatie worden niet beschouwd als illegale downloads of kopieën van een deel van SIS.

8. De lidstaten informeren Europol door aanvullende informatie uit te wisselen over hits bij signaleringen in verband met terroristische misdrijven. De lidstaten kunnen in uitzonderlijke gevallen Europol niet informeren indien dit lopende onderzoeken of de veiligheid van een persoon in gevaar zou brengen of tegen de wezenlijke belangen van de veiligheid van de signalerende lidstaat zou indruisen.

9. Lid 8 is van toepassing vanaf de datum waarop Europol aanvullende informatie overeenkomstig lid 1 kan ontvangen.

Artikel 36

Toegang tot gegevens in SIS 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

1. Overeenkomstig artikel 40, lid 8, van Verordening (EU) 2016/1624 hebben de in artikel 2, punten 8 en 9, van die verordening bedoelde teamleden, binnen de grenzen van hun mandaat en op voorwaarde dat zij gemachtigd zijn controles uit te voeren overeenkomstig artikel 34, lid 1, van deze verordening, en de nodige opleiding hebben genoten overeenkomstig artikel 14, lid 1, van deze verordening, recht op toegang tot gegevens in SIS en op doorzoeking van die gegevens voor zover dat noodzakelijk is voor de uitvoering van hun taak en voor zover vereist door het operationele plan voor een specifieke operatie. Toegang tot gegevens in SIS wordt niet verleend aan andere teamleden.

2. De in lid 1 bedoelde teamleden oefenen het recht op toegang tot gegevens in SIS en op doorzoeking van die gegevens uit overeenkomstig lid 1, via een technische interface. De technische interface wordt opgezet en onderhouden door het Europees Grens- en kustwachtagentschap en voorziet in een rechtstreekse verbinding met het centrale SIS.

3. Wanneer door een in lid 1 van dit artikel bedoeld teamlid bij een doorzoeking een signalering in 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 signalering in SIS 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. Om de rechtmatigheid van de gegevensverwerking te verifiëren, intern toezicht uit te oefenen en een adequate beveiliging en integriteit van de gegevens te waarborgen, houdt het Europees Grens- en kustwachtagentschap overeenkomstig de bepalingen van artikel 12 logbestanden bij van elke toegang tot en doorzoeking van SIS.

5. Het Europees Grens- en kustwachtagentschap stelt maatregelen als bedoeld in de artikelen 10, 11 en 13, vast en past deze toe om beveiliging, vertrouwelijkheid en intern toezicht te waarborgen en zorgt ervoor dat de teams als bedoeld in lid 1 van dit artikel die maatregelen toepassen.

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 van het Europees Grens- en kustwachtagentschap voor onrechtmatige of onjuiste verwerking van gegevens door haar.

7. Onverminderd lid 2 is het niet toegestaan delen van SIS te verbinden met een computersysteem voor gegevensverzameling en -verwerking dat door de in lid 1 bedoelde teams of door het Europees Grens- en kustwachtagentschap wordt gebruikt, noch om de gegevens in SIS waartoe die teams toegang hebben over te dragen naar een dergelijk systeem. Er mogen geen delen van SIS worden gedownload of gekopieerd. Het registreren van de toegang en de doorzoeking in logbestanden wordt niet beschouwd als illegaal downloaden of kopiëren van SIS-gegevens.

8. Het Europees Grens- en kustwachtagentschap geeft de Europese Toezichthouder voor gegevensbescherming toestemming om toezicht te houden op de activiteiten van de in dit artikel bedoelde teams bij het uitoefenen van hun recht op toegang tot gegevens in SIS en op doorzoeking van die gegevens, en om die activiteiten te evalueren. Dit laat de verdere bepalingen van Verordening (EU) 2018/1725 onverlet.

Artikel 37

Evaluatie van het gebruik van SIS door Europol en het Europees Grens- en kustwachtagentschap

1. De Commissie evalueert ten minste om de vijf jaar hoe SIS werkt en hoe Europol en de in artikel 36, lid 1, bedoelde teams SIS gebruiken.

2. Europol en het Europees Grens- en kustwachtagentschap zorgen ervoor dat aan de bevindingen van de evaluatie en de naar aanleiding daarvan opgestelde aanbevelingen een passend gevolg wordt gegeven.

3. Een verslag over de resultaten van en het vervolg op de evaluatie wordt naar het Europees Parlement en de Raad gestuurd.

Artikel 38

Reikwijdte van de toegang

Eindgebruikers, met inbegrip van Europol en de in artikel 2, punten 8 en 9 van Verordening (EU) 2016/1624 bedoelde teamleden, hebben slechts toegang tot de gegevens die zij voor het vervullen van hun taken nodig hebben.

Artikel 39

Toetsingstermijn voor signaleringen

1. Signaleringen worden niet langer bewaard dan nodig is voor het met de invoering nagestreefde doel.

2. Uiterlijk drie jaar na de invoering van een signalering in SIS toetst de signalerende lidstaat de noodzaak van verdere bewaring. Indien bij de nationale beslissing die aan de basis ligt van de signalering echter een langere geldigheidsperiode dan drie jaar is bepaald, wordt de signalering uiterlijk binnen vijf jaar opnieuw getoetst.

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

4. Vóór het verstrijken van de toetsingstermijn kan de signalerende lidstaat, op grond van een grondige individuele beoordeling die wordt geregistreerd, besluiten de signalering langer dan de toetsingstermijn te handhaven indien dit noodzakelijk blijkt voor en evenredig is aan het met de signalering nagestreefde doel. In dat geval is lid 2 tevens van toepassing op de verlenging. Iedere verlenging wordt doorgegeven aan CS-SIS.

5. Na afloop van de in lid 2 bedoelde toetsingstermijn worden signaleringen automatisch gewist, behalve wanneer de signalerende lidstaat overeenkomstig lid 4een verlenging aan CS-SIS heeft doorgegeven. CS-IS stelt de signalerende lidstaat vier maanden op voorhand automatisch in kennis van de geplande wissing van gegevens.

6. De lidstaten houden statistieken bij van het aantal signaleringen waarvan de bewaartermijnen overeenkomstig lid 4 van dit artikel zijn verlengd en zenden die statistieken op verzoek toe aan de in artikel 55 bedoelde toezichthoudende autoriteiten.

7. Zodra een Sirene-bureau constateert dat een signalering haar doel heeft bereikt en derhalve moet worden gewist, stelt het de autoriteit die de signalering heeft ingevoerd, daarvan onmiddellijk in kennis. Uiterlijk 15 kalenderdagen na ontvangst van die kennisgeving antwoordt de autoriteit dat de signalering is of zal worden gewist, of motiveert zij waarom de signalering wordt bewaard. Indien binnen de periode van 15 dagen niet wordt geantwoord, zorgt het Sirene-bureau ervoor dat de signalering wordt gewist. Indien het nationaal recht dit toestaat wordt de signalering gewist door het Sirene-bureau. Sirene-bureaus melden hun toezichthoudende autoriteit herhaaldelijke kwesties die zij tegenkomen wanneer zij uit hoofde van dit lid handelen.

Artikel 40

Wissing van signaleringen

1. Signaleringen met het oog op weigering van toegang en verblijf op grond van artikel 24 worden gewist:

a) wanneer de beslissing die eraan ten grondslag lag, door de bevoegde autoriteit is ingetrokken of nietig verklaard, of

b) in voorkomend geval ingevolge de in artikel 27 en artikel 29 bedoelde raadplegingsprocedure.

2. Signaleringen van onderdanen van derde landen ten aanzien van wie een beperkende maatregel is genomen om de toegang tot of de doorreis via het grondgebied van de lidstaten te beletten, worden gewist wanneer de beperkende maatregel is beëindigd, geschorst of nietig verklaard.

3. Signaleringen van personen die het burgerschap hebben verkregen van een lidstaat of een staat waarvan de onderdanen uit hoofde van het Unierecht begunstigden zijn van het recht van vrij verkeer, worden gewist zodra de signalerende lidstaat er, eventueel ingevolge artikel 44, kennis van krijgt dat de betrokken persoon het burgerschap heeft verkregen.

4. Signaleringen worden gewist na hun verstrijking overeenkomstig artikel 39.

HOOFDSTUK VIII

ALGEMENE VOORSCHRIFTEN INZAKE GEGEVENSVERWERKING

Artikel 41

Verwerking van SIS-gegevens

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

2. De gegevens mogen slechts voor technische doeleinden worden gekopieerd, indien dit voor rechtstreekse doorzoeking door de in artikel 34 bedoelde bevoegde autoriteiten noodzakelijk is. Deze verordening is van toepassing op dergelijke kopieën. Een lidstaat kopieert geen signaleringsgegevens of extra gegevens die door een andere lidstaat zijn ingevoerd, uit zijn N.SIS of uit de CS-SIS naar andere nationale gegevensbestanden.

3. De in lid 2 bedoelde technische kopieën die resulteren in de aanleg van offlinedatabanken, worden maximaal 48 uur bewaard.

Niettegenstaande de eerste alinea, zijn technische kopieën die resulteren in de aanleg van offline databanken 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 uur niet beschikbaar is.

De lidstaten houden een actuele inventaris van deze kopieën bij, stellen deze inventaris ter beschikking van hun toezichthoudende autoriteiten, en zorgen ervoor dat deze verordening, met name artikel 10, met betrekking deze kopieën wordt toegepast.

4. Toegang tot gegevens in SIS door in artikel 34 bedoelde nationale bevoegde autoriteiten is slechts toegestaan binnen de grenzen van hun bevoegdheden, en is uitsluitend voorbehouden aan daartoe gemachtigde personeelsleden.

5. SIS-gegevens kunnen slechts door de lidstaten worden verwerkt voor andere doelstellingen dan die waarvoor zij in SIS zijn ingevoerd, indien er een verband bestaat met een specifieke zaak en de verwerking noodzakelijk is ter voorkoming van een ernstige en onmiddellijke bedreiging 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. Uit hoofde van artikel 38, lid 2, onder k) en l), van Verordening (EU) 2018/1862 in SIS ingevoerde gegevens kunnen door de in artikel 34, lid 1, onder f), van deze verordening bedoelde bevoegde autoriteiten worden gebruikt in overeenstemming met het recht van de elke lidstaat.

7. Elk gebruik van SIS-gegevens dat in strijd is met de leden 1 tot en met 6 van dit artikel, wordt naar het nationale recht van elke lidstaat aangemerkt als oneigenlijk gebruik, en onderworpen aan sancties overeenkomstig artikel 59.

8. Iedere lidstaat verstrekt eu-LISA een lijst van zijn bevoegde autoriteiten die op grond van deze verordening gemachtigd zijn tot rechtstreekse doorzoeking van gegevens in SIS, alsmede alle wijzigingen van die lijst. In de lijst wordt voor elke autoriteit vermeld welke gegevens zij voor welke doeleinden mag bevragen. eu-LISA zorgt ervoor dat de lijst jaarlijks in het *Publicatieblad van de Europese Unie* wordt bekendgemaakt. eu-LISA houdt op zijn website een voortdurend bijgewerkte lijst bij waarin de wijzigingen zijn opgenomen die de lidstaten tussen de jaarlijkse bekendmakingen door opsturen.

9. Voor zover het recht van de Unie niet in bijzondere bepalingen voorziet, is het recht van elke lidstaat van toepassing op de gegevens in zijn N.SIS.

Artikel 42

SIS-gegevens en nationale bestanden

1. Artikel 41, lid 2, laat het recht van een lidstaat onverlet om in zijn nationale bestanden SIS-gegevens te bewaren in verband waarmee op zijn grondgebied actie is ondernomen. 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 41, 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 SIS is ingevoerd.

Artikel 43

Informatie bij niet-uitvoering van een signalering

Wanneer een gevraagde actie niet kan worden uitgevoerd, stelt de lidstaat waarvan actie is gevraagd de signalerende lidstaat daarvan onmiddellijk in kennis door de uitwisseling van aanvullende informatie.

Artikel 44

Kwaliteit van de gegevens in SIS

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

2. Wanneer een signalerende lidstaat relevante aanvullingen op of wijzigingen van gegevens zoals vermeld in artikel 20, lid 2, ontvangt, vult hij de signalering onverwijld aan of wijzigt deze.

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

4. Wanneer een andere dan de signalerende lidstaat beschikt over relevante aanvullingen op of wijzigingen van gegevens zoals vermeld in artikel 20, lid 2, stuurt hij die onverwijld door middel van de uitwisseling van aanvullende informatie door aan de signalerende lidstaat zodat deze de signalering kan vervolledigen of wijzigen. De gegevens worden alleen doorgestuurd als de identiteit van de onderdaan van het derde land is vastgesteld.

5. Wanneer een andere dan de signalerende lidstaat bewijs heeft dat een gegeven in een signalering onjuist is of onrechtmatig is ingevoerd, deelt hij dit zo spoedig mogelijk, maar niet later dan twee werkdagen nadat hij kennis heeft genomen van die aanwijzingen, mee aan de signalerende lidstaat door middel van de uitwisseling van aanvullende informatie. De signalerende lidstaat controleert de informatie en corrigeert of wist zo nodig onverwijld het betrokken gegeven.

6. Wanneer de lidstaten twee maanden nadat bewijs aan het licht zijn gekomen, nog geen overeenstemming hebben bereikt als bedoeld in lid 5 van dit artikel, legt de niet-signalerende lidstaat de zaak voor aan de betrokken toezichthoudende autoriteiten en aan de Europese Toezichthouder voor gegevensbescherming voor een beslissing ter zake, door middel van samenwerking overeenkomstig artikel 57.

7. De lidstaten wisselen aanvullende informatie uit, indien een klacht wordt ingediend door een persoon die stelt niet diegene wiens signalering is bedoeld. Indien na controle blijkt dat degene wiens signalering is bedoeld niet de klager is, wordt de klager ingelicht over de in artikel 47 bedoelde maatregelen en over het recht van beroep uit hoofde van artikel 54, lid 1.

Artikel 45

Beveiligingsincidenten

1. Elke gebeurtenis die gevolgen heeft of kan hebben voor de beveiliging van SIS of de SIS-gegevens of de aanvullende informatie kan beschadigen of verloren doen gaan, wordt beschouwd als een beveiligingsincident, met name wanneer onrechtmatige 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. De beheersing van beveiligingsincidenten is gericht op een snelle, doeltreffende en passende reactie.

3. Onverminderd de kennisgeving en de mededeling van een inbreuk in verband met persoonsgegevens overeenkomstig artikel 33 van Verordening (EU) 2016/679 of artikel 30 van Richtlijn (EU) 2016/680, melden de lidstaten, Europol en het Europees Grens- en kustwachtagentschap onverwijld aan de Commissie, eu-LISA, de bevoegde toezichthoudende autoriteit en de Europese Toezichthouder voor gegevensbescherming. eu-LISA meldt beveiligingsincidenten betreffende het centrale SIS onverwijld aan de Commissie en de Europese Toezichthouder voor gegevensbescherming.

4. Informatie over een beveiligingsincident dat gevolgen heeft of kan hebben voor de werking van SIS in een lidstaat of bij eu-LISA, voor de beschikbaarheid, de integriteit en de vertrouwelijkheid van de gegevens die door andere lidstaten zijn ingevoerd of toegezonden, of voor uitgewisselde aanvullende informatie, wordt onverwijld verstrekt aan alle lidstaten en gerapporteerd in overeenstemming met het door eu-LISA voorgelegde incidentenbeheersingsplan.

5. De lidstaten en eu-LISA werken in het geval van een beveiligingsincident samen.

6. De Commissie meldt ernstige incidenten onmiddellijk aan het Europees Parlement en de Raad. Die verslagen worden overeenkomstig de toepasselijke beveiligingsvoorschriften gerubriceerd als „EU RESTRICTED/RESTREINT UE".

7. Wanneer een beveiligingsincident is veroorzaakt door het oneigenlijke gebruik van gegevens, zien de lidstaten, Europol en het Europees Grens- en kustwachtagentschap erop toe dat sancties worden opgelegd overeenkomstig artikel 59.

Artikel 46

Onderscheid tussen personen met vergelijkbare kenmerken

1. Indien bij de invoering van een nieuwe signalering blijkt dat in SIS reeds een persoon met dezelfde identiteitsbeschrijving gesignaleerd is, neemt het Sirene-bureau binnen twaalf uur contact op met de signalerende lidstaat door de uitwisseling van aanvullende informatie om zich ervan te vergewissen of de twee signaleringen dezelfde persoon betreffen.

2. Indien uit het voorgaande blijkt dat de in de nieuwe signalering bedoelde persoon en de reeds in SIS gesignaleerde persoon inderdaad dezelfde persoon zijn, volgt het Sirene-bureau de in artikel 23 bedoelde procedure voor invoering van meervoudige signaleringen.

3. Indien uit die controle blijkt dat het om twee verschillende personen gaat, bekrachtigt het Sirene-bureau het verzoek om opneming van de tweede signalering en voegt het de nodige gegevens toe om verkeerde identificatie te voorkomen.

Artikel 47

Extra gegevens teneinde om te gaan met misbruikte identiteiten

1. Wanneer de met de signalering bedoelde 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. Een persoon van wie de identiteit is misbruikt, heeft het recht zijn instemming met de verwerking van de extra persoonsgegevens in te trekken.

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 met de signalering bedoelde persoon, en

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 en voor zover de persoon wiens identiteit is misbruikt daar uitdrukkelijk voor elke gegevenscategorie mee instemt, mogen slechts de volgende persoonsgegevens van de persoon wiens identiteit is misbruikt in SIS worden ingevoerd en verwerkt:

a) achternamen;

b) voornamen;

c) namen bij de geboorte;

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

e) bijzondere, onveranderlijke objectieve fysieke kenmerken;

f) geboorteplaats;

g) geboortedatum;

h) geslacht;

i) foto's en gezichtsopnamen;

j) vingerafdrukken, handpalmafdrukken of beide

k) alle voorgaande en huidige nationaliteiten;

l) categorie van de identificatiedocumenten;

m) land van afgifte van de identificatiedocumenten;

n) het (de) nummer(s) van de identificatiedocumenten;

o) datum van afgifte van de identificatiedocumenten;

p) adres van de persoon;

q) naam van de vader van de persoon;

r) naam van de moeder van de persoon.

4. De Commissie stelt uitvoeringshandelingen vast om technische voorschriften vast te leggen en te ontwikkelen die nodig zijn voor het invoeren en het verder verwerken van de in lid 3 van dit artikel bedoelde gegevens. Deze uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

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 48

Links tussen signaleringen

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

2. De link heeft geen gevolgen voor de te ondernemen specifieke actie op basis van elke gelinkte signalering of voor de toetsingstermijn van elk van de gelinkte signaleringen.

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

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

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

6. De Commissie stelt uitvoeringshandelingen vast om technische voorschriften vast te leggen en te ontwikkelen voor het linken van signaleringen. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure.

Artikel 49

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 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 ingevoerd, of over een signalering in verband waarmee op zijn grondgebied actie is ondernomen. De periode gedurende welke dergelijke gegevens in die bestanden mogen worden bewaard, wordt beheerst door het nationaal recht.

Artikel 50

Doorgifte van persoonsgegevens aan derden

In SIS verwerkte gegevens en de desbetreffende aanvullende informatie die overeenkomstig deze verordening is uitgewisseld worden niet doorgegeven aan of ter beschikking gesteld van derde landen of internationale organisaties.

HOOFDSTUK IX

GEGEVENSBESCHERMING

Artikel 51

Toepasselijke wetgeving

1. Wanneer eu-LISA of het Europees Grens- en kustwachtagentschap in uit hoofde van deze verordening persoonsgegevens verwerkt, is Verordening (EU) 2018/1725 van toepassing. Verordening (EU) 2016/794 is van toepassing op de verwerking van persoonsgegevens door Europol uit hoofde van deze verordening.

2. Wanneer de in artikel 34 van deze verordening bedoelde bevoegde autoriteiten in het kader van deze verordening persoonsgegevens verwerken, is Verordening (EU) 2016/679 van toepassing, tenzij het verwerkingen betreft met het oog op het voorkomen, opsporen, onderzoeken of vervolgen van strafbare feiten en voor de tenuitvoerlegging van strafrechtelijke sancties, met inbegrip van de bescherming tegen en de voorkoming van bedreigingen van de openbare veiligheid waarop Richtlijn (EU) 2016/680 van toepassing is.

Artikel 52

Recht op informatie

1. Aan in SIS gesignaleerde onderdanen van derde landen wordt overeenkomstig de artikelen 13 en 14 van Verordening (EU) 2016/679 of artikelen 12 en 13 van Richtlijn (EU) 2016/680 hierover 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, van deze verordening bedoelde nationale beslissing die aan de signalering ten grondslag ligt.

2. Deze informatie wordt niet verstrekt 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, opsporen, onderzoeken of vervolgen van strafbare feiten.

Artikel 53

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

1. De betrokkenen kunnen de rechten uitoefenen die zijn neergelegd in de artikelen 15, 16 en 17 van Verordening (EU) 2016/679 en in artikel 14 en artikel 16, leden 1 en 2, van Richtlijn (EU) 2016/680.

2. Een andere dan de signalerende lidstaat mag aan de betrokkene slechts informatie over persoonsgegevens van de betrokkene die worden verwerkt verstrekken voor zover die lidstaat de signalerende lidstaat vooraf de gelegenheid heeft geboden dienaangaande een standpunt te bepalen. De communicatie tussen die lidstaten geschiedt door middel van de uitwisseling van aanvullende informatie.

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

a) belemmering van officiële of justitiële 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, of

e) de rechten en vrijheden van anderen te beschermen.

In gevallen als bedoeld in de eerste alinea op de gebieden stelt de lidstaat de betrokkene schriftelijk en zonder onnodige vertraging in kennis van een eventuele weigering of beperking van de inzage en van de redenen voor die weigering of beperking. Die informatie kan achterwege worden gelaten wanneer de verstrekking daarvan een van de onder a) tot en met e) van de eerste alinea bedoelde redenen ondermijnen. De lidstaat stelt de betrokkene in kennis van de mogelijkheid om een klacht in te dienen bij een toezichthoudende instantie of om beroep in te stellen bij de rechter.

De lidstaat registreert de feitelijke of juridische redenen die ten grondslag liggen aan het besluit om geen informatie aan de betrokkene te verstrekken. Die informatie wordt ter beschikking gesteld van de toezichthoudende autoriteiten.

Voor deze gevallen kan de betrokkene zijn rechten ook uitoefenen via de bevoegde toezichthoudende instanties.

4. Bij ontvangst van een verzoek tot inzage, rectificatie of wissing informeert de lidstaat de betrokkene, ongeacht of hij zich in een derde land bevindt, zo spoedig mogelijk en in elk geval binnen de in artikel 12, lid 3, van Verordening (EU) 2016/679 genoemde termijnen, van het gevolg dat wordt gegeven aan de uitoefening van de rechten uit hoofde van dit artikel.

Artikel 54

Rechtsmiddelen

1. Onverminderd de bepalingen inzake rechtsmiddelen van Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680 heeft eenieder het recht om naar aanleiding van een hem betreffende signalering bij elk naar het nationale recht van elke lidstaat bevoegde instantie, waaronder de rechter, beroep in te stellen met het oog op inzage, rectificatie, wissing en op het verkrijgen van informatie of schadevergoeding in verband met zijn 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 artikel 58.

3. De lidstaten brengen jaarlijks aan het Europees Comité voor gegevensbescherming verslag uit over:

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

b) het aantal inzageverzoeken dat bij de 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 om 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 toezichthoudende autoriteit is ingediend;

e) het aantal aanhangig gemaakte rechtszaken;

f) het aantal zaken waarin de rechter de verzoeker in het gelijk heeft gesteld;

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

De Commissie stelt een model op voor de in dit lid bedoelde verslaglegging.

4. De verslagen van de lidstaten worden in het in artikel 57, lid 4, bedoelde gemeenschappelijk verslag opgenomen.

Artikel 55

Toezicht op N.SIS

1. De lidstaten zorgen ervoor dat hun aangewezen onafhankelijke nationale toezichthoudende autoriteit waaraan de bevoegdheden als bedoeld in hoofdstuk VI van Verordening (EU) 2016/679 of hoofdstuk VI van Richtlijn (EU) 2016/680 zijn toegekend, toeziet op de rechtmatigheid van de verwerking van persoonsgegevens in SIS op hun grondgebied, de doorgifte van die gegevens vanuit hun grondgebied en de uitwisseling en verdere verwerking van aanvullende informatie op hun grondgebied.

2. De toezichthoudende autoriteit ziet erop toe dat ten minste om de vier jaar een audit van de gegevensverwerking in zijn N.SIS wordt uitgevoerd overeenkomstig internationale auditnormen. De audit wordt uitgevoerd door de toezichthoudende autoriteit of wordt door de toezichthoudende autoriteit 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 toezichthoudende autoriteit staan.

3. De lidstaten zorgen ervoor dat hun toezichthoudende autoriteit over voldoende middelen beschikt om haar taken uit hoofde van deze verordening te kunnen vervullen, en toegang heeft tot advies van personen met voldoende kennis van biometrische gegevens.

Artikel 56

Toezicht op eu-LISA

1. De Europese Toezichthouder voor gegevensbescherming is verantwoordelijk voor het toezicht op de verwerking van persoonsgegevens door eu-LISA en draagt er zorg voor dat die activiteiten in overeenstemming zijn met deze verordening. De taken en bevoegdheden als bedoeld in de artikelen 57 en 58 van Verordening (EU) 2018/1725 van overeenkomstige toepassing.

2. De Europese Toezichthouder voor gegevensbescherming voert ten minste om de vier jaar een audit uit van de verwerking van persoonsgegevens door eu-LISA overeenkomstig internationale auditnormen. Het auditrapport wordt toegezonden aan het Europees Parlement, de Raad, eu-LISA, de Commissie en de toezichthoudende autoriteiten. Voordat het rapport wordt aangenomen, wordt eu-LISA in de gelegenheid gesteld opmerkingen te maken.

Artikel 57

Samenwerking tussen de toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming

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

2. De toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming 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 toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming ten minste tweemaal per jaar bijeen in het kader van het Europees Comité voor gegevensbescherming. De kosten en logistieke ondersteuning van deze bijeenkomsten zijn voor rekening van het Europees Comité voor gegevensbescherming. Tijdens de eerste bijeenkomst wordt een reglement van orde vastgesteld. Indien nodig worden in onderling overleg andere werkmethoden vastgesteld.

4. Jaarlijks zendt het Europees Comité voor gegevensbescherming een gezamenlijk activiteitenverslag over het gecoördineerde toezicht toe aan het Europees Parlement, de Raad en de Commissie.

HOOFDSTUK X

AANSPRAKELIJKHEID EN SANCTIES

Artikel 58

Aansprakelijkheid

1. Onverminderd het recht op vergoeding en enige aansprakelijkheid uit hoofde van Verordening (EU) 2016/679, Richtlijn (EU) 2016/680 en Verordening (EU) 2018/1725, geldt het volgende:

a) eenieder, respectievelijk elke lidstaat, die als gevolg van onrechtmatige gegevensverwerking door het gebruik van N. SIS, of een andere met deze verordening strijdige handeling vanwege een lidstaat, materiële of immateriële schade heeft geleden, is gerechtigd om van die lidstaat schadevergoeding te ontvangen, en

b) eenieder, respectievelijk elke lidstaat, die als gevolg van een met deze verordening strijdige handeling van eu-LISA, materiële of immateriële schade heeft geleden, is gerechtigd om van eu-LISA schadevergoeding te ontvangen.

Een lidstaat of eu-LISA wordt geheel of gedeeltelijk van zijn aansprakelijkheid uit hoofde van de eerste alinea ontheven indien hij kan aantonen niet verantwoordelijk te zijn voor het feit dat de schade heeft veroorzaakt.

2. Indien schade aan SIS ontstaat doordat een lidstaat zijn verplichtingen uit hoofde van deze verordening niet is nagekomen, is deze lidstaat voor deze schade aansprakelijk, tenzij en voor zover eu-LISA of een andere lidstaat die aan SIS deelneemt, heeft nagelaten redelijke maatregelen te treffen om het optreden van de schade te voorkomen of de omvang ervan zo veel mogelijk te beperken.

3. Op vorderingen tegen een lidstaat tot vergoeding van de in de leden 1 en 2 bedoelde schade is het nationale recht van die lidstaat van toepassing. Op vorderingen tegen eu-LISA tot vergoeding van de in de leden 1 en 2 bedoelde schade zijn de in de Verdragen bepaalde voorwaarden van toepassing.

Artikel 59

Sancties

De lidstaten zorgen ervoor dat misbruik of oneigenlijke verwerking van SIS-gegevens en de eventuele uitwisseling van aanvullende informatie in strijd met deze verordening, strafbaar is overeenkomstig het nationaal recht.

De vastgestelde sancties zijn doeltreffend, evenredig en afschrikkend.

HOOFDSTUK XI

SLOTBEPALINGEN

Artikel 60

Toezicht en statistieken

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

2. Met het oog op het technische onderhoud, verslaglegging, rapportage over gegevenskwaliteit en statistieken heeft eu-LISA toegang tot de daartoe vereiste informatie over de in het centrale SIS verrichte verwerkingen.

3. eu-LISA stelt zowel per lidstaat als voor alle lidstaten gezamenlijk, dag-, maand- en jaarstatistieken op over het aantal bestanden per signaleringscategorie. eu-LISA stelt ook zowel per lidstaat als voor alle lidstaten gezamenlijk jaarverslagen op over het aantal hits per signaleringscategorie, het aantal keren dat SIS is doorzocht en het aantal keren dat toegang tot SIS is verkregen om een signalering in te voeren, bij te werken of te wissen. Dergelijke statistieken omvatten statistieken over de in artikelen 27 tot en met 31 bedoelde uitwisseling van informatie. De opgestelde statistieken bevatten geen persoonsgegevens. Het statistische jaarverslag wordt openbaar gemaakt.

4. De lidstaten, Europol en het Europees Grens- en kustwachtagentschap verstrekken eu-LISA en de Commissie de informatie die nodig is om de in de leden 3, 5, 7 en 8 bedoelde verslagen op te stellen.

5. eu-LISA verstrekt alle statistische verslagen die het opstelt aan het Europees Parlement, de Raad, de lidstaten, de Commissie, Europol, het Europees Grens- en kustwachtagentschap en de Europese Toezichthouder voor gegevensbescherming.

Om toezicht te houden op de tenuitvoerlegging van rechtshandelingen van de Unie, met inbegrip van de toepassing van Verordening (EU) nr. 1053/2013, kan de Commissie eu-LISA vragen om, op gezette tijden of ad hoc, aanvullende gerichte statistische verslagen te verstrekken over de prestaties of het gebruik van SIS en over de uitwisseling van aanvullende informatie.

Het Europees Grens- en kustwachtagentschap kan met het oog op het uitvoeren van kwetsbaarheids- en risicobeoordelingen als bedoeld in de artikelen 11 en 13 van Verordening (EU) 2016/1624, eu-LISA verzoeken om op gezette tijden of ad hoc, aanvullende gerichte statistische verslagen te verstrekken.

6. Voor de toepassing van artikel 15, lid 4, en van de leden 3, 4 en 5 van dit artikel, wordt door eu-LISA op zijn technische locaties een centraal register opgezet, geïmplementeerd en gehost, met daarin de in artikel 15, lid 4, en in lid 3 van dit artikel bedoelde gegevens, aan de hand waarvan het niet mogelijk mag zijn personen te identificeren en aan de hand waarvan de Commissie en de in lid 5 van dit artikel bedoelde agentschappen verslagen en statistieken op maat kunnen verkrijgen. eu-LISA verleent op verzoek de lidstaten, de Commissie, Europol en het Europees Grens- en kustwachtagentschap toegang tot het centrale register, voor zover dat nodig is voor het vervullen van hun taken en door middel van beveiligde toegang via de communicatie-infrastructuur. eu-LISA voert toegangscontroles uit en maakt specifieke gebruikersprofielen aan om te verzekeren dat toegang tot het centraal register uitsluitend voor verslagleggingen statistieken verkregen kan worden.

7. Twee jaar na de datum van toepassing van deze verordening ingevolge artikel 66, lid 5, eerste alinea, en vervolgens om de twee jaar, legt eu-LISA aan het Europees Parlement en de Raad een verslag voor over de technische werking van het centrale SIS en van de communicatie-infrastructuur, alsmede over hun beveiliging, over het geautomatiseerd vingerafdrukidentificatiesysteem (AFIS) en over de bilaterale en multilaterale uitwisseling van aanvullende informatie tussen de lidstaten. Dit verslag bevat ook een evaluatie van het gebruik van gezichtsopnamen ter identificatie van personen, zodra deze technologie wordt gebruikt.

8. Drie jaar na de datum van toepassing van deze verordening ingevolge artikel 66, lid 5, eerste alinea, en vervolgens om de vier jaar, verricht de Commissie een algemene evaluatie 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, wordt 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. Het evaluatieverslag bevat ook een evaluatie van het AFIS en van de voorlichtingscampagnes over SIS die door de Commissie worden verricht overeenkomstig artikel 19.

Daarnaast bevat het evaluatieverslag statistieken over het aantal overeenkomstig artikel 24, lid 1, onder a), ingevoerde signaleringen alsmede statistieken over het aantal overeenkomstig punt b) van dat lid ingevoerde signaleringen. Voor signaleringen als bedoeld onder artikel 24, lid 1, onder a), bevat het verslag nadere details over het aantal signaleringen dat is ingevoerd naar aanleiding van de in artikel 24, lid 2, onder a), b) of c), bedoelde situaties. Het evaluatieverslag bevat ook een evaluatie over de toepassing van artikel 24 door de lidstaten.

De Commissie legt het evaluatieverslag voor aan het Europees Parlement en de Raad.

9. De Commissie stelt uitvoeringshandelingen vast om uitvoerige regels voor de werking van het centrale register als bedoeld in lid 6 van dit artikel en voor de gegevensbescherming en beveiligingsvoorschriften voor dat register vast te leggen. Deze uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 61

Uitoefening van de bevoegdheidsdelegatie

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

2. De in artikel 33, lid 4, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor onbepaalde tijd met ingang van 27 december 2018.

3. Het Europees Parlement of de Raad kan de in artikel 33, lid 4, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

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

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, stelt zij het Europees Parlement en de Raad daarvan gelijktijdig in kennis.

6. Een overeenkomstig artikel 33, lid 4, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 62

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 63

Wijzigingen in Verordening (EG) nr. 1987/2006

Verordening (EG) nr. 1987/2006 wordt als volgt gewijzigd:

1) Artikel 6 wordt vervangen door:

„*Artikel 6*

Nationale systemen

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

2. Iedere lidstaat is verantwoordelijk voor het waarborgen van de ononderbroken beschikbaarheid van SIS II-gegevens voor eindgebruikers.”.

2) Artikel 11 wordt vervangen door:

„*Artikel 11*

Vertrouwelijkheid — Lidstaten

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

2. Indien een lidstaat bij de uitvoering van enige taken in verband met SIS II samenwerkt met een externe contractant, ziet het nauwlettend toe op de werkzaamheden van die contractant om de naleving van alle bepalingen van deze verordening te waarborgen, met name inzake beveiliging, vertrouwelijkheid en gegevensbescherming.

3. Het operationeel beheer van N.SIS II of van technische kopieën wordt niet toevertrouwd aan particuliere ondernemingen of particuliere organisaties.".

3) Artikel 15 wordt als volgt gewijzigd:

a) het volgende lid wordt ingevoegd:

„3 bis. De beheersautoriteit ontwikkelt en onderhoudt een mechanisme en procedures voor het uitvoeren van kwaliteitscontroles op de gegevens in CS-SIS. Zij brengt hierover regelmatig verslag uit aan de lidstaten.

Zij rapporteert regelmatig aan de Commissie welke kwesties zijn geconstateerd en welke lidstaten hierbij zijn betrokken.

De Commissie legt aan het Europees Parlement en de Raad regelmatig een verslag voor over de aangetroffen problemen met de kwaliteit van de gegevens.";

b) lid 8 wordt vervangen door:

„8. Het operationele beheer van het centrale SIS II omvat alle taken die nodig zijn om het centrale SIS II 24 uur per dag en zeven dagen per week overeenkomstig deze verordening te laten functioneren, met name de voor de goede werking van het systeem onontbeerlijke onderhoudswerkzaamheden en technische ontwikkelingen. Die taken omvatten tevens de coördinatie, het beheer en de ondersteuning van testactiviteiten voor het centrale SIS II en N.SIS II, om het centrale SIS II en N.SIS II te laten functioneren overeenkomstig de vereisten voor de in artikel 9 bepaalde naleving van de technische normen.".

4) Aan artikel 17 worden de volgende leden toegevoegd:

„3. Indien de beheersautoriteit bij de uitvoering van taken in verband met SIS II samenwerkt met een externe contractant, ziet zij nauwlettend toe op de werkzaamheden van die contractant, om de naleving van alle bepalingen van deze verordening te waarborgen, met name inzake beveiliging, vertrouwelijkheid en gegevensbescherming.

4. Het operationeel beheer van de CS-SIS wordt niet toevertrouwd aan particuliere ondernemingen of particuliere organisaties.".

5) In artikel 20, lid 2, wordt het volgende punt ingevoegd:

„k bis) het soort strafbaar feit;".

6) Aan artikel 21 wordt de volgende alinea toegevoegd:

„Wanneer de in artikel 24, lid 2, bedoelde beslissing tot weigering van toegang en verblijf verband houdt met een terroristisch misdrijf, wordt de zaak beschouwd als gepast, relevant en belangrijk genoeg om een signalering in SIS II te rechtvaardigen. Om redenen van openbare en nationale veiligheid kunnen lidstaten bij uitzondering geen signalering invoeren, wanneer te verwachten valt dat die signalering officiële of justitiële onderzoeken, opsporingsonderzoeken of procedures zal belemmeren.".

7) Artikel 22 wordt vervangen door:

„*Artikel 22*

Specifieke voorschriften voor invoering, verificatie of doorzoeking met foto's en vingerafdrukken

1. Foto's en vingerafdrukken worden alleen ingevoerd nadat door middel van een speciale kwaliteitscontrole is vastgesteld dat aan minimale gegevenskwaliteitsnormen is voldaan. De speciale kwaliteitscontrole wordt gespecificeerd volgens de procedure van artikel 51, lid 2.

2. Indien foto's en vingerafdrukgegevens beschikbaar zijn in een signalering in SIS II, worden dergelijke foto's en vingerafdrukgegevens gebruikt om de identiteit te bevestigen van een persoon die naar aanleiding van een alfanumerieke doorzoeking van SIS II is gelokaliseerd.

3. Vingerafdrukgegevens mogen altijd worden doorzocht om een persoon te identificeren. Vingerafdrukgegevens worden echter doorzocht voor identificatiedoeleinden, indien de identiteit van de persoon niet met behulp van andere middelen kan worden vastgesteld. Daartoe omvat het centrale SIS II een geautomatiseerd vingerafdrukidentificatiesysteem (AFIS).

4. Vingerafdrukgegevens in SIS II in verband met overeenkomstig artikelen 24 en 26 ingevoerde signaleringen mogen tevens worden doorzocht aan de hand van volledige of onvolledige reeksen vingerafdrukken die zijn aangetroffen op de plaats delict van ernstige strafbare feiten of terroristische misdrijven die worden onderzocht, indien met een hoge mate van waarschijnlijkheid kan worden vastgesteld dat die afdrukken van een dader zijn en op voorwaarde dat de doorzoeking tegelijkertijd in de relevante nationale vingerafdrukdatabanken van de lidstaat wordt uitgevoerd.".

8) Artikel 26 wordt vervangen door:

„*Artikel 26*

Voorwaarden voor de invoering van signaleringen van onderdanen van derde landen ten aanzien van wie een beperkende maatregel is genomen

1. Signaleringen van onderdanen van derde landen ten aanzien van wie overeenkomstig een rechtshandeling 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 SIS II ingevoerd met het oog op weigering van toegang en verblijf, voor zover aan de eisen inzake de kwaliteit van de gegevens is voldaan.

2. De signaleringen worden ingevoerd, geactualiseerd en gewist door de bevoegde autoriteit van de lidstaat die het voorzitterschap van de Raad van de Europese Unie bekleedde wanneer de maatregel is genomen. Indien die lidstaat geen toegang heeft tot SIS II of tot overeenkomstig artikel 24 van deze verordening ingevoerde signaleringen, wordt die verantwoordelijkheid opgenomen door de lidstaat die het volgende voorzitterschap bekleedt en wel toegang heeft tot SIS II of tot signaleringen overeenkomstig deze verordening.

De lidstaten voorzien in de nodige procedures voor het invoeren, bijwerken en wissen van deze signaleringen.”.

9) De volgende artikelen worden ingevoegd:

„*Artikel 27 bis*

Toegang van Europol tot gegevens in SIS II

1. Het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) ingesteld bij Verordening (EU) 2016/794 van het Europees Parlement en de Raad (*), heeft, indien nodig voor de vervulling van zijn mandaat, recht op toegang tot en doorzoeking van gegevens in SIS II. Europol kan ook aanvullende informatie uitwisselen en vragen overeenkomstig de bepalingen van het Sirene-handboek.

2. Indien Europol bij een doorzoeking een signalering in SIS II aantreft, stelt Europol de signalerende lidstaat daarvan in kennis door de uitwisseling van aanvullende informatie door middel van de communicatie-infrastructuur en overeenkomstig het Sirene-handboek. Totdat Europol de functies voor de uitwisseling van aanvullende informatie kan gebruiken, stelt het de signalerende lidstaat in kennis via de in Verordening (EU) 2016/794 bepaalde kanalen.

3. Europol mag de hem door de lidstaten verstrekte aanvullende informatie verwerken die door de lidstaten is verstrekt voor vergelijking met zijn databanken en voor operationele analyseprojecten, om connecties of andere relevante verbanden op te sporen en voor de onder a), b) en c), van artikel 18, lid 2, van Verordening (EU) 2016/794 bedoelde strategische, thematische of operationele analyses. De verwerking van aanvullende informatie door Europol voor de toepassing van dit artikel geschiedt overeenkomstig die verordening.

4. Door doorzoeking van SIS II of door de verwerking van aanvullende informatie verkregen informatie wordt door Europol alleen gebruikt indien de signalerende lidstaat daarmee instemt. Indien de lidstaat het gebruik van dergelijke informatie toestaat, wordt deze door Europol behandeld overeenkomstig Verordening (EU) 2016/794. Europol deelt die informatie alleen mee aan derde landen en organen indien de signalerende lidstaat daarmee instemt, met volledige naleving van het Unierecht inzake gegevensbescherming.

5. Europol is ertoe gehouden:

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

b) niettegenstaande artikel 31, lid 1, van Verordening (EU) 2016/794, uiterlijk een jaar nadat de betreffende signalering is gewist, aanvullende informatie die persoonsgegevens bevat te wissen. In afwijking daarvan kan Europol, indien het informatie in zijn databanken of operationele analyseprojecten heeft over een geval dat met de aanvullende informatie verband houdt, de aanvullende informatie bij wijze van uitzondering verder bewaren, voor zover dit nodig is om zijn taken uit te voeren. Europol informeert de signalerende en de uitvoerende lidstaat over de verdere bewaring van die aanvullende informatie en rechtvaardigt die verdere opslag;

c) de toegang tot gegevens in SIS II, met inbegrip van aanvullende informatie, te beperken tot specifiek daartoe gemachtigd personeel van Europol dat deze toegang nodig heeft om zijn taken te kunnen uitoefenen;

d) maatregelen als bedoeld in de artikelen 10, 11 en 13, vast te stellen en toe te passen om beveiliging, vertrouwelijkheid en intern toezicht te waarborgen;

e) ervoor te zorgen dat personeel dat gemachtigd is SIS II-gegevens te verwerken een geschikte opleiding en informatie krijgt overeenkomstig artikel 14, en

f) onverminderd Verordening (EU) 2016/794, de Europese Toezichthouder voor gegevensbescherming in de gelegenheid te stellen toezicht te houden op de activiteiten die Europol verricht op grond van zijn recht op toegang tot en doorzoeking van gegevens in SIS II, en op de uitwisseling en verwerking van aanvullende informatie, en dit alles te evalueren.

6. Europol mag uitsluitend gegevens kopiëren uit SIS II voor technische doeleinden, indien dat noodzakelijk is voor een rechtstreekse doorzoeking door naar behoren gemachtigd Europol-personeel. Deze verordening is van toepassing op dergelijke kopieën. De technische kopie wordt enkel gebruikt om SIS II-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 II-gegevens. Europol kopieert geen signaleringsgegevens of extra gegevens die door de lidstaten zijn verstrekt of uit CS-SIS II afkomstig zijn, in andere Europol-systemen.

7. Om de rechtmatigheid van de gegevensverwerking te verifiëren, intern toezicht en een adequate beveiliging en integriteit van de gegevens te waarborgen, houdt Europol overeenkomstig de bepalingen van artikel 12 logbestanden bij van elke toegang tot en doorzoeking van SIS II. Deze logbestanden en documentatie worden niet beschouwd als illegale downloads of kopieën van een deel van SIS II.

8. De lidstaten informeren Europol door aanvullende informatie uit te wisselen over hits bij signaleringen in verband met terroristische misdrijven. De lidstaten kunnen in uitzonderlijke gevallen Europol niet informeren indien dit lopende onderzoeken of de veiligheid van een persoon in gevaar zou brengen of tegen de wezenlijke belangen van de veiligheid van de signalerende lidstaat zou indruisen.

9. Lid 8 is van toepassing vanaf de datum waarop Europol aanvullende informatie overeenkomstig lid 1 kan ontvangen.

Artikel 27 ter

Toegang tot gegevens in SIS II 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 van het Europees Parlement en de Raad (**) hebben de leden van de teams als bedoeld in artikel 2, punten 8 en 9, van die verordening, binnen de grenzen van hun mandaat en op voorwaarde dat zij gemachtigd zijn controles uit te voeren overeenkomstig artikel 27, lid 1, van deze verordening en de nodige opleiding hebben genoten overeenkomstig artikel 14 van deze verordening, recht op toegang tot gegevens in SIS II en doorzoeking van die gegevens voor zover dat noodzakelijk is voor de uitvoering van hun taak en voor zover vereist door het operationele plan voor een specifieke operatie. Toegang tot gegevens in SIS II wordt niet verleend aan andere teamleden.

2. De in lid 1 bedoelde teamleden oefenen het recht op toegang tot en doorzoeking van gegevens in SIS II uit overeenkomstig lid 1, via een technische interface. De technische interface wordt opgezet en onderhouden door het Europees Grens- en kustwachtagentschap en voorziet in een rechtstreekse verbinding met het centrale SIS II.

3. Wanneer een van de in lid 1 van dit artikel bedoelde teamleden bij een doorzoeking een signalering in SIS II 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 II-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. Om de rechtmatigheid van de gegevensverwerking te verifiëren, intern toezicht en een adequate beveiliging en integriteit van de gegevens te waarborgen, houdt het Europees Grens- en kustwachtagentschap overeenkomstig de bepalingen van artikel 12 logbestanden bij van elke toegang tot en doorzoeking van SIS II.

5. Het Europees Grens- en kustwachtagentschap stelt maatregelen als bedoeld in de artikelen 10, 11 en 13, vast en past deze toe om beveiliging, vertrouwelijkheid en intern toezicht te waarborgen en zorgt ervoor dat de teams als bedoeld in lid 1 van dit artikel deze maatregelen toepassen.

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 van het Europees Grens- en kustwachtagentschap voor onrechtmatige of incorrecte verwerking van gegevens door haar.

7. Onverminderd lid 2 is het niet toegestaan om delen van SIS II te verbinden met een computersysteem voor gegevensverzameling en -verwerking dat door de teams bedoeld in lid 1 of door het Europees Grens- en kustwachtagentschap wordt gebruikt, noch om gegevens in SIS II waartoe die teams toegang hebben, over te dragen naar een dergelijk systeem. Er mogen geen delen van SIS II worden gedownload of gekopieerd. Het registreren van de toegang en de doorzoeking in logbestanden wordt niet beschouwd als illegaal downloaden of kopiëren van SIS II-gegevens.

8. Het Europees Grens- en kustwachtagentschap geeft de Europese Toezichthouder voor gegevensbescherming toestemming om toezicht te houden op de activiteiten van de in dit artikel bedoelde teams bij het uitoefenen van hun recht op toegang tot en doorzoeking van gegevens in SIS II, en om die activiteiten te evalueren. Dit laat de verdere bepalingen van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad (***) onverlet.

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

(**) 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).

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

Artikel 64

Wijziging van de overeenkomst ter uitvoering van het Akkoord van Schengen

Artikel 25 van de overeenkomst ter uitvoering van het Akkoord van Schengen wordt geschrapt.

Artikel 65

Intrekking

Verordening (EG) nr. 1987/2006 wordt ingetrokken met ingang van de in artikel 66, lid 5, eerste alinea, bepaalde datum van toepassing van deze verordening.

Verwijzingen naar de ingetrokken verordening gelden als verwijzingen naar deze verordening en worden gelezen in samenhang met de concordantietabel in de bijlage.

Artikel 66

Inwerkingtreding, aanvang van werkzaamheden en toepassing

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

2. Uiterlijk op 28 december 2021 neemt de Commissie een besluit tot vaststelling van de datum waarop ingevolge deze verordening SIS-werkzaamheden aanvangen, nadat zij heeft gecontroleerd dat aan de volgende voorwaarden is voldaan:

a) de voor de toepassing van deze verordening vereiste uitvoeringshandelingen zijn vastgesteld;

b) de lidstaten hebben aan de Commissie 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, en

c) eu-LISA heeft aan de Commissie meegedeeld dat alle tests van de CS-SIS en de interactie tussen CS-SIS en N.SIS succesvol zijn afgerond.

3. De Commissie ziet nauwlettend toe op het proces van geleidelijke vervulling van de in lid 2 genoemde voorwaarden en stelt het Europees Parlement en de Raad in kennis van het resultaat van de in dat lid bedoelde controle.

4. Uiterlijk op 28 december 2019 en vervolgens elk jaar totdat het in lid 2 bedoelde besluit van de Commissie is vastgesteld, dient de Commissie bij het Europees Parlement en de Raad een verslag in over de stand van de voorbereidingen voor de volledige tenuitvoerlegging van deze verordening. Dat verslag bevat ook gedetailleerde informatie over de gemaakte kosten en over eventuele risico's die van invloed kunnen zijn op de totale kosten.

5. Deze verordening is van toepassing met ingang van de datum die overeenkomstig lid 2 is vastgesteld.

In afwijking van de eerste alinea:

a) zijn artikel 4, lid 4, artikel 5, artikel 8, lid 4, artikel 9, leden 1 en 5, artikel 15, lid 7, artikel 19, artikel 20, leden 3 en 4, artikel 32, lid 4, artikel 33, lid 4, artikel 47, lid 4, artikel 48, lid 6, artikel 60, leden 6 en 9, artikel 61, artikel 62, artikel 63, punten 1 tot en met 6 en 8, en de leden 3 en 4 van dit artikel van toepassing met ingang van de datum van inwerkingtreding van deze verordening;

b) is artikel 63, punt 9, van toepassing met ingang van 28 december 2019;

c) is artikel 63, punt 7, van toepassing met ingang van 28 december 2020.

6. Het in lid 2 bedoelde besluit van de Commissie wordt bekendgemaakt in het *Publicatieblad van de Europese Unie*.

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

Gedaan te Brussel, 28 november 2018.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
A. TAJANI	K. EDTSTADLER

BIJLAGE

CONCORDANTIETABEL

Verordening (EG) nr. 1987/2006	Deze verordening
Artikel 1	Artikel 1
Artikel 2	Artikel 2
Artikel 3	Artikel 3
Artikel 4	Artikel 4
Artikel 5	Artikel 5
Artikel 6	Artikel 6
Artikel 7	Artikel 7
Artikel 8	Artikel 8
Artikel 9	Artikel 9
Artikel 10	Artikel 10
Artikel 11	Artikel 11
Artikel 12	Artikel 12
Artikel 13	Artikel 13
Artikel 14	Artikel 14
Artikel 15	Artikel 15
Artikel 16	Artikel 16
Artikel 17	Artikel 17
Artikel 18	Artikel 18
Artikel 19	Artikel 19
Artikel 20	Artikel 20
Artikel 21	Artikel 21
Artikel 22	Artikelen 32 en 33
Artikel 23	Artikel 22
—	Artikel 23
Artikel 24	Artikel 24
Artikel 25	Artikel 26
Artikel 26	Artikel 25
—	Artikel 27
—	Artikel 28
—	Artikel 29
—	Artikel 30
—	Artikel 31
Artikel 27	Artikel 34
Artikel 27 bis	Artikel 35
Artikel 27 ter	Artikel 36
—	Artikel 37
Artikel 28	Artikel 38
Artikel 29	Artikel 39
Artikel 30	Artikel 40
Artikel 31	Artikel 41

Verordening (EG) nr. 1987/2006	Deze verordening
Artikel 32	Artikel 42
Artikel 33	Artikel 43
Artikel 34	Artikel 44
—	Artikel 45
Artikel 35	Artikel 46
Artikel 36	Artikel 47
Artikel 37	Artikel 48
Artikel 38	Artikel 49
Artikel 39	Artikel 50
Artikel 40	—
—	Artikel 51
Artikel 41	Artikel 53
Artikel 42	Artikel 52
Artikel 43	Artikel 54
Artikel 44	Artikel 55
Artikel 45	Artikel 56
Artikel 46	Artikel 57
Artikel 47	—
Artikel 48	Artikel 58
Artikel 49	Artikel 59
Artikel 50	Artikel 60
—	Artikel 61
Artikel 51	Artikel 62
Artikel 52	—
—	Artikel 63
—	Artikel 64
Artikel 53	—
—	Artikel 65
Artikel 54	—
Artikel 55	Artikel 66