

**EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2018/1862****av den 28 november 2018****om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU**

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 82.1 andra stycket d, 85.1, 87.2 a och 88.2 a,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

i enlighet med det ordinarie lagstiftningsförfarandet <sup>(1)</sup>, och

av följande skäl:

- (1) Schengens informationssystem (SIS) är ett grundläggande verktyg för tillämpningen av bestämmelserna i Schengenregelverket, såsom det införlivats inom Europeiska unionens ramar. SIS är en av de centrala kompensationsåtgärder som bidrar till upprätthållandet av en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen genom att stödja det operativa samarbetet mellan nationella behöriga myndigheter, särskilt gränskontrolltjänstemän, polis- och tullmyndigheter, invandringsmyndigheter, myndigheter som ansvarar för att förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder.
- (2) SIS inrättades ursprungligen på grundval av bestämmelserna i avdelning IV i konventionen av den 19 juni 1990 om tillämpning av Schengenavtalet av den 14 juni 1985 mellan regeringarna i Beneluxstaterna, Förbundsrepubliken Tyskland och Franska republiken om gradvis avskaffande av kontroller vid de gemensamma gränserna <sup>(2)</sup> (konventionen om tillämpning av Schengenavtalet). Kommissionen fick genom rådets förordning (EG) nr 2424/2001 <sup>(3)</sup> och rådets beslut 2001/886/RIF <sup>(4)</sup> i uppdrag att utveckla andra generationen av SIS (SIS II). Det inrättades senare genom Europaparlamentets och rådets förordning (EG) nr 1987/2006 <sup>(5)</sup> och rådets beslut 2007/533/RIF <sup>(6)</sup>. SIS II ersatte det SIS som inrättades genom konventionen om tillämpning av Schengenavtalet.
- (3) Tre år efter det att SIS II togs i bruk utförde kommissionen en utvärdering av systemet i enlighet med förordning (EG) nr 1987/2006 och beslut 2007/533/RIF. Den 21 december 2016 lade kommissionen fram rapporten om utvärderingen av andra generationen av Schengens informationssystem (SIS II) i enlighet med artiklarna 24.5, 43.3 och 50.5 i förordning (EG) nr 1987/2006 och artiklarna 59.3 och 66.5 i beslut 2007/533/RIF och ett åtföljande arbetsdokument till Europaparlamentet och rådet. Denna förordning bör, i tillämpliga fall, återspegla rekommendationerna i dessa dokument.
- (4) Denna förordning utgör den rättsliga grunden för SIS avseende frågor som omfattas av kapitlen 4 och 5 i tredje delen avdelning V i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Europaparlamentets och rådets förordning (EU) 2018/1861 <sup>(7)</sup> utgör den rättsliga grunden för SIS avseende frågor som omfattas av kapitel 2 i tredje delen avdelning V i EUF-fördraget.

<sup>(1)</sup> Europaparlamentets ståndpunkt av den 24 oktober 2018 (ännu ej offentliggjord i EUT) och rådets beslut av den 19 november 2018.

<sup>(2)</sup> EGT L 239, 22.9.2000, s. 19.

<sup>(3)</sup> Rådets förordning (EG) nr 2424/2001 av den 6 december 2001 om utvecklingen av andra generationen av Schengens informationssystem (SIS II) (EGT L 328, 13.12.2001, s. 4).

<sup>(4)</sup> Rådets beslut 2001/886/RIF av den 6 december 2001 om utvecklingen av andra generationen av Schengens informationssystem (SIS II) (EGT L 328, 13.12.2001, s. 1).

<sup>(5)</sup> Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 381, 28.12.2006, s. 4).

<sup>(6)</sup> Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 205, 7.8.2007, s. 63).

<sup>(7)</sup> Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006 (se sidan 14 i detta nummer av EUT).

- (5) Det faktum att den rättsliga grunden för SIS består av separata instrument påverkar inte principen att SIS är ett enda informationssystem som bör fungera som ett enda system. Det bör inbegripa ett enda nätverk av nationella kontor kallade Sirenekontor, för att säkerställa utbyte av tilläggsinformation. Vissa av bestämmelserna i dessa instrument bör därför vara identiska.
- (6) Det är nödvändigt att ange målen för SIS, vissa aspekter av dess tekniska struktur samt dess finansiering, fastställa bestämmelser om den genomgående driften och användningen av systemet samt fastställa ansvarsfördelningen. Det är också nödvändigt att bestämma vilka kategorier av uppgifter som ska föras in i systemet, för vilka syften uppgifterna ska föras in och behandlas samt kriterier för införande. Regler krävs också för radering av registreringar, vilka myndigheter som ska ha åtkomst till uppgifterna, hur biometrisk uppgifter ska användas och för att närmare fastställa regler om dataskydd och databehandling.
- (7) Registreringar i SIS innehåller endast den information som är nödvändig för att identifiera en person eller ett föremål och för att fastställa vilken åtgärd som ska vidtas. Medlemsstaterna bör därför utbyta tilläggsinformation om registreringar vid behov.
- (8) SIS omfattar ett centralt system (nedan kallat *det centrala SIS*) och nationella system. De nationella systemen kan innehålla en fullständig eller partiell kopia av SIS-databasen, som kan vara gemensam för två eller flera medlemsstater. Med tanke på att SIS är det viktigaste instrumentet för informationsutbyte i Europa för säkerställande av säkerhet och ändamålsenlig gränsförvaltning är det nödvändigt att säkerställa att det fungerar utan avbrott såväl på central som på nationell nivå. Tillgången till SIS bör bevakas noga på central nivå och på medlemsstatsnivå, och alla tillfällen när SIS inte är tillgängligt för slutanvändarna bör registreras och rapporteras till berörda parter på nationell nivå och unionsnivå. Varje medlemsstat bör inrätta en backup av sitt nationella system. Medlemsstaterna bör också säkerställa en oavbruten uppkoppling till det centrala SIS genom att ha flera likadana anslutningar som är fysiskt och geografiskt åtskilda. Driften av det centrala SIS och av kommunikationsinfrastrukturen bör ske på ett sådant sätt att det säkerställer att de fungerar dygnet runt veckans alla dagar. I detta syfte bör Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (nedan kallad *eu-LISA*), inrättad genom Europaparlamentets och rådets förordning (EU) 2018/1726 <sup>(1)</sup>, genomföra tekniska lösningar för att stärka den oavbrutna tillgången till SIS, med förbehåll för en oberoende konsekvensbedömning och kostnads-nyttoanalys.
- (9) Det är nödvändigt med en uppdaterad handbok med närmare bestämmelser om utbytet av tilläggsinformation om åtgärder påkallade av registreringar (nedan kallad *Sirenehandboken*). Sirenekontoren bör säkerställa ett snabbt och effektivt utbyte av sådan information.
- (10) För att säkerställa ett effektivt utbyte av tilläggsinformation, bland annat om de åtgärder som ska vidtas enligt registreringen, är det lämpligt att stärka Sirenekontorens verksamhet genom att specificera kraven i fråga om tillgängliga resurser och fortbildning för användare samt svarstider för förfrågningar som de mottar från andra Sirenekontor.
- (11) Medlemsstaterna bör säkerställa att personalen vid deras Sirenekontor har de språkkunskaper och de kunskaper om relevanta lagar och förfaranderegler som är nödvändiga för att de ska kunna utföra sina uppgifter.
- (12) För att kunna dra fördel av funktionerna i SIS fullt ut bör medlemsstaterna säkerställa att slutanvändarna och Sirenekontorens personal får regelbunden utbildning, bland annat om datasäkerhet och dataskydd samt om uppgifternas kvalitet. Sirenekontoren bör delta i utarbetandet av utbildningsprogram. Sirenekontoren bör i möjligaste mån även organisera personalutbyten med andra Sirenekontor minst en gång om året. Medlemsstaterna uppmanas att vidta lämpliga åtgärder för att undvika att personalförändringar leder till kompetens- och erfarenhetsförluster.
- (13) Den operativa förvaltningen av de centrala delarna av SIS sköts av eu-LISA. För att eu-LISA ska kunna avdela de finansiella resurser och personalresurser som behövs för alla aspekter av den operativa förvaltningen av det centrala SIS och kommunikationsinfrastrukturen bör dess uppgifter fastställas i detalj i denna förordning, i synnerhet när det gäller de tekniska aspekterna på utbytet av tilläggsinformation.
- (14) Utan att det påverkar medlemsstaternas ansvar för att de uppgifter som förs in i SIS är korrekta eller Sirenekontorens uppgift som kvalitetssamordnare bör eu-LISA vara ansvarig för att förbättra uppgifternas kvalitet genom att införa ett centralt kvalitetskontrollverktyg, och bör regelbundet tillhandahålla kommissionen och

<sup>(1)</sup> Europaparlamentets och rådets förordning (EU) 2018/1726 av den 14 november 2018 om Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA), om ändring av förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF och om upphävande av förordning (EU) nr 1077/2011 (EUT L 295, 21.11.2018, s. 99).

medlemsstaterna rapporter. Kommissionen bör rapportera till Europaparlamentet och rådet om problem som uppstått i fråga om uppgifternas kvalitet. För att ytterligare öka kvaliteten på uppgifterna i SIS bör eu-LISA också erbjuda de nationella utbildningsorganen och om möjligt även Sirenekontoren och slutanvändarna utbildning i hur man använder SIS.

- (15) För att möjliggöra bättre övervakning av användningen av SIS och i syfte att analysera tendenser i fråga om brott bör eu-LISA kunna utveckla en avancerad kapacitet för statistisk rapportering till medlemsstaterna, Europaparlamentet, rådet, kommissionen, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån utan att dataintegriteten äventyras. Därför bör en central databas inrättas. Den statistik som lagras i eller erhålls från den databasen bör inte innehålla några personuppgifter. Medlemsstaterna bör tillhandahålla statistik avseende utövat av rätten till åtkomst, rättelse av oriktiga uppgifter och radering av olagligt lagrade uppgifter inom ramen för samarbete mellan tillsynsmyndigheter och Europeiska datatillsynsmannen i enlighet med denna förordning.
- (16) Nya uppgiftskategorier bör införas i SIS för att göra det möjligt för slutanvändarna att fatta välgrundade beslut utifrån en registrering utan att förlora någon tid. För att underlätta identifiering och upptäckt av flera identiteter bör registreringen även, när sådan information finns tillgänglig, innehålla en hänvisning till den berörda personens personliga id-handling eller numret på id-handlingen och en kopia, om möjligt i färg, av handlingen.
- (17) Om det är absolut nödvändigt bör de behöriga myndigheterna även ha möjlighet att i SIS föra in särskild information om en persons eventuella särskilda, objektiva och fysiska egenskaper som inte kan ändras, såsom tatueringar, märken eller ärr.
- (18) Om de är tillgängliga bör alla relevanta uppgifter, i synnerhet den berörda personens förnamn, föras in när en registrering skapas, i syfte att minimera risken för falska träffar och onödigt operativ verksamhet.
- (19) I SIS bör man inte lagra några uppgifter som används för att utföra sökningar, med undantag av loggar för att kontrollera att sökningen är laglig, övervaka att databehandlingen sker på ett lagligt sätt, utföra egenkontroll och säkerställa att ett de nationella systemen fungerar på ett korrekt sätt samt för dataintegritet och datasäkerhet.
- (20) SIS bör möjliggöra behandling av biometriska uppgifter för att bidra till tillförlitlig identifiering av berörda personer. Införande av fotografier, ansiktsbilder eller fingeravtrycksuppgifter i SIS och användning av sådana uppgifter bör begränsas till vad som är nödvändigt för att uppnå de mål som eftersträvas, bör vara tillåten enligt unionsrätten, bör respektera de grundläggande rättigheterna, bland annat barnets bästa, och bör vara förenlig med unionsrätten i fråga om dataskydd, inklusive relevanta bestämmelser om dataskydd i denna förordning. För att undvika problem orsakade av felidentifiering bör SIS även möjliggöra behandling av uppgifter om personer vars identitet missbrukats, med förbehåll för särskilda skyddsåtgärder, den berörda personens samtycke för varje uppgiftskategori, i synnerhet handavtryck, och en sträng begränsning av de syften för vilka sådana personuppgifter lagligen får behandlas.
- (21) Medlemsstaterna bör vidta nödvändiga tekniska åtgärder så att en slutanvändare som gör en berättigad sökning i en nationell polis- eller immigrationsdatabas varje gång parallellt även söker i SIS, med förbehåll för principerna i artikel 4 i Europaparlamentets och rådets direktiv (EU) 2016/680<sup>(1)</sup> och artikel 5 i Europaparlamentets och rådets förordning (EU) 2016/679<sup>(2)</sup>. Detta bör säkerställa att SIS fungerar som den främsta kompensationsåtgärden inom området utan inre gränskontroller och bättre beaktar den gränsöverskridande dimensionen av brottslighet och brottslingarnas rörlighet.
- (22) I denna förordning bör det fastställas villkor för användning av fingeravtrycksuppgifter, fotografier och ansiktsbilder för identifiering och kontroll. Ansiktsbilder och fotografier bör, för identifiering, inledningsvis användas endast vid reguljära gränsövergångsställen. Sådan användning bör vara föremål för en rapport från kommissionen som bekräftar att tekniken är tillgänglig, klar att tas i bruk och tillförlitlig.

<sup>(1)</sup> Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

<sup>(2)</sup> Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskydds-förordning) (EUT L 119, 4.5.2016, s. 1).

- (23) Införandet av ett automatiskt system för identifiering av fingeravtryck i SIS kompletterar den befintliga Prümmekanismen för gemensam gränsöverskridande onlineåtkomst till utvalda nationella DNA-databaser och automatiska system för identifiering av fingeravtryck, i enlighet med vad som föreskrivs i rådets beslut 2008/615/RIF<sup>(1)</sup> och 2008/616/RIF<sup>(2)</sup>. Sökningen på fingeravtrycksuppgifter i SIS möjliggör ett aktivt sökande efter gärningsmannen. Därför bör det vara möjligt att ladda upp en okänd gärningsmans fingeravtrycksuppgifter i SIS, förutsatt att det med mycket stor sannolikhet kan fastställas att den person som dessa uppgifter tillhör har begått ett grovt brott eller en terroristhandling. Detta gäller speciellt om fingeravtrycksuppgifterna hittas på ett vapen eller något annat föremål som har använts för brottet. Blotta förekomsten av fingeravtrycksuppgifter på brottsplatsen bör inte anses tyda på en mycket stor sannolikhet att fingeravtrycksuppgifterna tillhör gärningsmannen. En ytterligare förutsättning för skapandet av en sådan registrering bör vara att den misstänktes identitet inte kan fastställas på grundval av uppgifter från någon annan relevant databas på nationell nivå, unionsnivå eller internationell nivå. Om en sökning på fingeravtrycksuppgifter leder till en potentiell matchning bör medlemsstaten utföra ytterligare kontroller, med medverkan av experter, för att fastställa om fingeravtrycken tillhör den misstänkte vars avtryck finns lagrade i SIS och bör fastställa personens identitet. Förfarandena bör regleras i nationell rätt. En sådan identifiering kan bidra till utredningen på ett betydande sätt och kan leda till gripande, förutsatt att alla villkor för ett gripande är uppfyllda.
- (24) Det bör vara tillåtet att söka fingeravtrycksuppgifter som lagras i SIS med fullständiga eller ofullständiga uppsättningar fingeravtryck eller handavtryck som hittas på en brottsplats om det med stor sannolikhet kan fastställas att de tillhör den person som begått det grova brottet eller terroristbrottet, förutsatt att en sökning samtidigt görs i de relevanta nationella fingeravtrycksdatabaserna. Särskild vikt bör läggas vid att fastställa kvalitetsstandarder som är tillämpliga på lagring av biometriska uppgifter, inbegripet latent fingeravtrycksuppgifter.
- (25) Om en persons identitet inte kan fastställas på något annat sätt bör fingeravtrycksuppgifter användas för att försöka identifiera personen. Det bör i samtliga fall vara tillåtet att identifiera en person med hjälp av fingeravtrycksuppgifter.
- (26) Det bör vara möjligt att lägga till en DNA-profil i en registrering i tydligt definierade fall där inga fingeravtrycksuppgifter finns att tillgå. Den DNA-profilen bör endast vara tillgänglig för behöriga användare. DNA-profiler torde underlätta identifiering av försvunna personer i behov av skydd och i synnerhet försvunna barn, bland annat genom att det blir möjligt att använda DNA-profiler från släktingar i rakt upp- eller nedstigande led och från syskon för identifiering. DNA-uppgifterna bör endast innehålla den minsta mängd information som är nödvändig för att identifiera den försvunna personen.
- (27) DNA-profiler bör hämtas från SIS endast om en identifiering är nödvändig och proportionell för de syften som fastställs i denna förordning. DNA-profiler bör inte hämtas eller behandlas för några andra syften än de för vilka de fördes in i SIS. De bestämmelser om dataskydd och datasäkerhet som fastställs i denna förordning bör vara tillämpliga. Ytterligare skyddsåtgärder bör vid behov införas vid användning av DNA-profiler, i syfte att undvika alla risker för felaktig positiv identifiering, hackande och obehörigt utlämnande till tredje parter.
- (28) SIS bör innehålla registreringar om personer som är efterlysta för att gripas och överlämnas samt personer som är efterlysta för att gripas och utlämnas. Utöver registreringar är det lämpligt att föreskriva ett sådant utbyte av tilläggsinformation genom Sirenekontoren som behövs för överlämnande- och utlämningsförfaranden. I synnerhet bör de uppgifter som avses i artikel 8 i rådets rambeslut 2002/584/RIF<sup>(3)</sup> behandlas i SIS. Av operativa skäl är det lämpligt att den registrerande medlemsstaten efter tillstånd från de rättsliga myndigheterna gör en befintlig registrering om gripande tillfälligt otillgänglig när en person som är föremål för en europeisk arresteringsorder söks intensivt och aktivt och slutanvändare som inte deltar i den konkreta spaningsinsatsen kan äventyra resultatet. Sådana registreringar bör i princip inte vara tillfälligt otillgängliga längre än 48 timmar.
- (29) Det bör vara möjligt att i SIS lägga till en översättning av de kompletterande uppgifter som förs in för överlämnande enligt den europeiska arresteringsordern och för utlämning.

(1) Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (EUT L 210, 6.8.2008, s. 1).

(2) Rådets beslut 2008/616/RIF av den 23 juni 2008 om genomförande av beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (EUT L 210, 6.8.2008, s. 12).

(3) Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (EGTL 190, 18.7.2002, s. 1).

- (30) SIS bör innehålla registreringar om försvunna personer eller om sårbara personer som behöver hindras från att resa för att säkerställa deras säkerhet eller förebygga hot mot den allmänna säkerheten eller den allmänna ordningen. När det gäller barn bör dessa registreringar och motsvarande förfaranden tjäna barnets bästa i enlighet med artikel 24 i Europeiska unionens stadga om de grundläggande rättigheterna och artikel 3 i Förenta nationernas konvention om barnets rättigheter av den 20 november 1989. De behöriga myndigheterna, inklusive rättsliga myndigheter, bör vidta åtgärder och fatta beslut till följd av en registrering om ett barn i samarbete med barnskyddsmyndigheter. Det nationella journalnumret för försvunna barn bör informeras i förekommande fall.
- (31) Registreringar om försvunna personer som behöver ställas under beskydd bör föras in på den behöriga myndighetens begäran. Alla barn som har försvunnit från medlemsstaternas mottagningsanläggningar bör vara föremål för en registrering om försvunna personer i SIS.
- (32) Registreringar om barn som löper risk för bortförande bör föras in i SIS på begäran av behöriga myndigheter, inklusive rättsliga myndigheter som är behöriga i mål om föräldrans ansvar enligt nationell rätt. Registreringar om barn som löper risk för bortförande bör endast föras in i SIS om denna risk är konkret och uppenbar och under begränsade omständigheter. Det är därför nödvändigt att föreskriva stränga och lämpliga skyddsåtgärder. Vid bedömningen av om det föreligger en konkret och uppenbar risk för att ett barn omgående och olagligt kan avlägsnas från en medlemsstat bör den behöriga myndigheten ta hänsyn till barnets personliga förhållanden och omgivning.
- (33) Genom denna förordning bör det införas en ny kategori av registreringar för vissa kategorier av sårbara personer som behöver hindras från att resa. Personer som på grund av sin ålder, sin funktionsnedsättning eller sina familjeförhållanden behöver skydd bör anses vara sårbara.
- (34) Registreringar om barn som för sin egen säkerhet behöver hindras från att resa bör föras in i SIS om det föreligger en konkret och uppenbar risk för att de avlägsnas från eller lämnar en medlemsstats territorium. Sådana registreringar bör föras in om resan skulle innebära att de riskerar att bli offer för människohandel, tvångsåktenskap, kvinnlig könsstympning eller andra former av könsrelaterat våld, att bli offer för eller involveras i terroristbrott, att inkallas eller värvas till väpnade grupper eller att tvingas delta aktivt i fientligheter.
- (35) Registreringar om sårbara vuxna som för sin egen säkerhet behöver hindras från att resa bör föras in om resan skulle innebära att de riskerar att bli offer för människohandel eller könsrelaterat våld.
- (36) I syfte att garantera stränga och lämpliga skyddsåtgärder bör registreringar om barn eller andra sårbara personer som behöver hindras från att resa, om så krävs enligt nationell rätt, föras in i SIS till följd av ett beslut av en rättslig myndighet eller ett beslut av en behörig myndighet som har bekräftats av en rättslig myndighet.
- (37) En ny åtgärd bör införas för att göra det möjligt att stoppa och fråga ut en person så att den registrerande medlemsstaten ska få så noggranna uppgifter som möjligt. Denna åtgärd bör tillämpas i fall där en person på grundval av en tydlig indikation misstänks ha för avsikt att begå eller redan begå något av de brott som avses i artikel 2.1 och 2.2 i rambeslut 2002/584/RIF, om ytterligare uppgifter är nödvändiga för att verkställa ett fängelsestraff eller en annan frihetsberövande åtgärd avseende en person som har dömts för något av de brott som avses i artikel 2.1 och 2.2 i rambeslut 2002/584/RIF eller om det finns skäl att tro att han eller hon kommer att begå något av dessa brott. Denna åtgärd bör inte heller påverka befintliga mekanismer för ömsesidig rättslig hjälp. Den bör ge tillräckligt mycket information så att man kan besluta om ytterligare åtgärder. Denna nya åtgärd bör inte innebära att personen kroppsvisiteras eller grips. De misstänkta och de tilltalades processuella rättigheter enligt unionsrätten och nationell rätt bör upprätthållas, inbegripet deras rätt till tillgång till försvarare i enlighet med Europaparlamentets och rådets direktiv 2013/48/EU <sup>(1)</sup>.
- (38) Vid registreringar om föremål som ska beslagtas eller användas som bevis i brottmål bör föremålen i fråga beslagtas i enlighet med den nationella rätt som avgör om och i enlighet med vilka villkor ett föremål ska beslagtas, särskilt om det innehas av föremålets rättmätiga ägare.
- (39) SIS bör innehålla nya kategorier för föremål med högt värde, såsom it-produkter som kan identifieras och sökas med ett unikt identifieringsnummer.

<sup>(1)</sup> Europaparlamentets och rådets direktiv 2013/48/EU av den 22 oktober 2013 om rätt till tillgång till försvarare i straffrättsliga förfaranden och förfaranden i samband med en europeisk arresteringsorder samt om rätt att få en tredje part underrättad vid frihetsberövande och rätt att kontakta tredje parter och konsulara myndigheter under frihetsberövandet (EUT L 294, 6.11.2013, s. 1).

- (40) När det gäller registreringar som förts in i SIS beträffande handlingar för beslagtagande eller för användning som bevis i brottmål bör uttrycket "falsk" tolkas som att det omfattar både förfalskade och totalförfalskade handlingar.
- (41) En medlemsstat bör kunna särskilt märka en viss registrering med så kallad flaggning, vilket innebär att den åtgärd som registreringen avser inte kommer att vidtas på medlemsstatens territorium. När registreringar förs in om gripande för överlämnande bör inget i denna förordning tolkas som ett undantag från eller förhindra tillämpning av bestämmelserna i rambeslut 2002/584/RIF. Beslut om att förse en registrering med flaggning i syfte att inte verkställa en europeisk arresteringsorder bör fattas endast på grundval av de skäl för vägran som anges i rambeslutet.
- (42) När en registrering märkts med flaggning och det blir känt var den person som ska gripas för överlämnande befinner sig, bör detta alltid meddelas den utfärdande rättsliga myndigheten, som då kan besluta att översända en europeisk arresteringsorder till den behöriga rättsliga myndigheten, i enlighet med bestämmelserna i rambeslut 2002/584/RIF.
- (43) Medlemsstaterna bör ha möjlighet att länka samman olika registreringar i SIS. Det faktum att det finns länkar mellan två eller flera registreringar bör inte påverka den åtgärd som ska vidtas, tidsfristen för översyn av registreringar eller åtkomsträtten till registreringarna.
- (44) Registreringar bör inte bevaras i SIS längre än vad som är nödvändigt för att uppnå det specifika syfte för vilket de fördes in. Tidsfristerna för översyn av de olika kategorierna av registreringar bör vara lämpliga med hänsyn till deras syfte. Registreringar om föremål som är länkade till registreringar om personer bör bevaras endast så länge som registreringen om personen bevaras. Beslut att bibehålla registreringar om personer bör grundas på en noggrann individuell bedömning. Medlemsstaterna bör se över registreringar om personer och föremål inom de föreskrivna tidsfristerna för översyn och bör föra statistik över antalet registreringar för vilka lagringstiden har förlängts.
- (45) Införande av en registrering i SIS och förlängning av lagringstiden för en registrering i SIS bör vara föremål för en proportionalitetsprövning, med bedömning av om ett visst ärende är tillräckligt adekvat, relevant och viktigt för att motivera att en registrering förs in i SIS. När det gäller terroristbrott bör ärendet anses vara tillräckligt adekvat, relevant och viktigt för att motivera att det finns en registrering i SIS. Av skäl som rör allmän eller nationell säkerhet bör medlemsstaterna tillåtas att i undantagsfall avstå från att föra in en registrering i SIS, när det är sannolikt att detta skulle försvåra officiella eller rättsliga utredningar, undersökningar eller förfaranden.
- (46) Det är nödvändigt att fastställa bestämmelser om radering av registreringar. En registrering bör inte lagras längre än vad som är nödvändigt för att uppnå det syfte för vilket den förts in. Eftersom medlemsstaterna har olika praxis när det gäller att fastställa vid vilken tidpunkt en registrering har uppfyllt sitt syfte är det lämpligt att ange närmare kriterier för varje kategori av registrering för att kunna avgöra när den bör raderas.
- (47) SIS-uppgifternas integritet är av yttersta vikt. Därför bör lämpliga skyddsåtgärder införas för behandlingen av SIS-uppgifter både på central och på nationell nivå för att säkerställa att uppgifterna är skyddade från början till slut. De myndigheter som behandlar uppgifter bör omfattas av säkerhetskraven i denna förordning, och bör följa ett enhetligt förfarande för rapportering av tillbud. Deras personal bör ha lämplig utbildning och informeras om relevanta brott och sanktioner.
- (48) Uppgifter som behandlats i SIS och motsvarande tilläggsinformation som utbyts i enlighet med denna förordning bör inte överföras till eller göras tillgängliga för tredjeländer eller internationella organisationer.
- (49) Det är lämpligt att bevilja åtkomst till SIS för enheter som ansvarar för registrering av fordon, fartyg och luftfartyg för att de ska kunna kontrollera om transportmedlet i fråga söks i en medlemsstat för beslagtagande. Det är även lämpligt att bevilja åtkomst till SIS för enheter som ansvarar för registrering av skjutvapen för att de ska kunna kontrollera om det berörda skjutvapnet söks i en medlemsstat för beslagtagande eller om det finns en registrering om den person som ansöker om registreringen.
- (50) Direktåtkomst till SIS bör endast beviljas behöriga statliga enheter. Denna åtkomst bör begränsas till registreringar om respektive transportmedel och deras registreringsbevis eller nummerplåt eller skjutvapen och personer som ansöker om registrering. Varje träff i SIS bör rapporteras av dessa enheter till polismyndigheterna, som bör vidta ytterligare åtgärder i enlighet med den specifika registreringen i SIS och underrätta den registrerande medlemsstaten om träffen via Sirenekontoren.

- (51) Utan att det påverkar mer specifika bestämmelser i den här förordningen bör de nationella lagar och andra författningar som antagits i enlighet med direktiv (EU) 2016/680 vara tillämpliga på de nationella behöriga myndigheternas behandling, inbegripet insamling och utlämning, av personuppgifter enligt den här förordningen i syfte att förebygga, förhindra, avslöja, utreda eller lagföra terroristbrott eller andra grova brott eller verkställa straffrättsliga påföljder. Åtkomsten till uppgifter som förts in i SIS och rätten att söka i sådana uppgifter för nationella behöriga myndigheter som ansvarar för att förebygga, förhindra, avslöja, utreda eller lagföra terroristbrott eller andra grova brott eller verkställa straffrättsliga påföljder bör omfattas av alla relevanta bestämmelser i den här förordningen och i direktiv (EU) 2016/280, såsom det har införlivats i nationell rätt, och i synnerhet den övervakning som utförs av de tillsynsmyndigheter som avses i direktiv (EU) 2016/680.
- (52) Utan att det påverkar mer specifika bestämmelser om behandling av personuppgifter i den här förordningen bör förordning (EU) 2016/679 vara tillämplig på medlemsstaternas behandling av personuppgifter enligt den här förordningen, såvida inte behandlingen utförs av de nationella behöriga myndigheterna i syfte att förebygga, förhindra, utreda, avslöja eller lagföra terroristbrott eller andra grova brott.
- (53) Europaparlamentets och rådets förordning (EU) 2018/1725 <sup>(1)</sup> bör vara tillämplig på unionsinstitutionernas och unionsorganens behandling av personuppgifter när de fullgör sina skyldigheter enligt denna förordning.
- (54) Europaparlamentets och rådets förordning (EU) 2016/794 <sup>(2)</sup> bör vara tillämplig på Europols behandling av personuppgifter enligt den här förordningen.
- (55) I fall där en sökning i SIS som utförs av de nationella medlemmarna i Eurojust och deras biträdande medlemmar visar att det finns en registrering som förts in av en medlemsstat kan inte Eurojust vidta de åtgärder som begärs. Därför bör Eurojust meddela den berörda medlemsstaten så att den kan följa upp ärendet.
- (56) Vid användningen av SIS bör de behöriga myndigheterna säkerställa att man respekterar värdigheten och integriteten för de personer vars uppgifter behandlas. Behandling av personuppgifter enligt denna förordning får inte leda till diskriminering av personer på någon grund, vare sig kön, ras eller etniskt ursprung, religion eller övertygelse, funktionsnedsättning, ålder eller sexuell läggning.
- (57) När det gäller konfidentialitet bör relevanta bestämmelser i tjänsteföreskrifterna för Europeiska unionens tjänstemän och anställningsvillkoren för övriga anställda i unionen som fastställs i rådets förordning (EEG, Euratom, EGSK) nr 259/68 <sup>(3)</sup> (nedan kallade *tjänsteföreskrifterna*) vara tillämpliga på tjänstemän och övriga anställda vars arbete har samband med SIS.
- (58) Såväl medlemsstaterna som eu-LISA bör ha uppdaterade säkerhetsplaner för att underlätta genomförandet av säkerhetskrav och bör samarbeta med varandra så att de behandlar säkerhetsfrågor ur ett gemensamt perspektiv.
- (59) De nationella oberoende tillsynsmyndigheter som avses i förordning (EU) 2016/679 och direktiv (EU) 2016/680 (nedan kallade *tillsynsmyndigheter*) bör övervaka att medlemsstaternas behandling av personuppgifter enligt den här förordningen, inklusive utbytet av tilläggsinformation, sker på ett lagligt sätt. Tillsynsmyndigheterna bör ges tillräckliga resurser för att utföra denna uppgift. Man bör fastställa de registrerades rätt till åtkomst till, rättelse av och radering av sina personuppgifter som lagrats i SIS, och varje påföljande rättsmedel i nationella domstolar samt ömsesidigt erkännande av domar. Det är även lämpligt att kräva årlig statistik från medlemsstaterna.
- (60) Tillsynsmyndigheterna bör säkerställa att en revision av behandlingen av uppgifter i deras medlemsstats nationella system genomförs minst vart fjärde år i enlighet med internationella revisionsstandarder. Antingen bör revisionen utföras av tillsynsmyndigheterna, eller så bör tillsynsmyndigheterna begära revisionen direkt från en oberoende dataskyddsrevisor. Den oberoende revisorn bör kvarstå under de berörda tillsynsmyndigheternas kontroll och ansvar, och dessa bör därför själva ge anvisningar till revisorn och ange en tydligt fastställd avsikt, omfattning och metod för revisionen samt vägledning och tillsyn avseende revisionen och dess slutresultat.

<sup>(1)</sup> Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

<sup>(2)</sup> Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).

<sup>(3)</sup> EGT L 56, 4.3.1968, s. 1.

- (61) Europeiska datatillsynsmannen bör övervaka unionsinstitutionernas och unionsorganens verksamhet i samband med behandlingen av personuppgifter enligt denna förordning. Europeiska datatillsynsmannen och tillsynsmyndigheterna bör samarbeta när det gäller övervakningen av SIS.
- (62) Europeiska datatillsynsmannen bör tilldelas de resurser som krävs för att fullgöra de uppgifter som den åläggs enligt denna förordning, bland annat stöd från personer med sakkunskaper om biometriska uppgifter.
- (63) I förordning (EU) 2016/794 föreskrivs att Europol ska stödja och stärka de nationella behöriga myndigheternas insatser och deras samarbete vad gäller bekämpning av terrorism och grov brottslighet samt tillhandahålla analyser och hotbilda-bedomningar. Utvidgningen av Europols åtkomsträtt till registreringar om försvunna personer bör ytterligare förbättra Europols förmåga att ge nationella brottsbekämpande myndigheter omfattande operativa och analytiska produkter som rör människohandel och sexuell exploatering av barn, även online. Detta skulle bidra till bättre förebyggande och förhindrande av dessa brott, till skydd av potentiella offer och till utredningen om gärningsmännen. Europeiska it-brottscentrumet vid Europol skulle också gynnas av att Europol har åtkomst till registreringar om försvunna personer, till exempel i fall av resande sexualförbrytare och sexuellt utnyttjande av barn på internet, där gärningsmännen ofta påstår att de har tillgång till barn eller kan få tillgång till barn som kan ha registrerats som försvunna.
- (64) För att täppa till luckorna i utbytet av information om terrorism, i synnerhet om utländska terroriststridande – där övervakningen av deras rörlighet är avgörande – uppmanas medlemsstaterna att dela information om terrorismrelaterad verksamhet med Europol. Detta informationsutbyte bör ske genom utbyte av tilläggsinformation med Europol om berörda registreringar. För detta ändamål bör Europol upprätta en koppling till kommunikationsinfrastrukturen.
- (65) Det är också nödvändigt att fastställa klara och tydliga bestämmelser för Europol om behandling och nedladdning av SIS-uppgifter för att göra det möjligt för Europol att heltäckande använda SIS, förutsatt att standarder för dataskydd iakttas i enlighet med denna förordning och förordning (EU) 2016/794. I fall där en sökning som Europol utför i SIS visar att det finns en registrering som förts in av en medlemsstat kan Europol inte vidta de åtgärder som begärs. Därför bör Europol meddela den berörda medlemsstaten genom utbyte av tilläggsinformation med respektive Sirenekontor för att göra det möjligt för den medlemsstaten att följa upp ärendet.
- (66) Enligt Europaparlamentets och rådets förordning (EU) 2016/1624 <sup>(1)</sup> ska värdmedlemsstaten vid tillämpning av den förordningen tillåta medlemmarna i de enheter som avses i artikel 2.8 i den förordningen och som utplaceras av Europeiska gräns- och kustbevakningsbyrån att göra sådana sökningar i unionsdatabaser som är nödvändiga för att uppfylla operativa mål som anges i den operativa planen för in- och utresekontroller (i förordning (EU) 2016/1624 kallade *gränskontroller*), gränsövervakning (i förordning (EU) 2016/1624 kallat *gränsbevakning*) och återvändande. Andra berörda unionsbyråer, särskilt Europeiska stödkontoret för asylfrågor och Europol, får också placera ut experter, som inte är anställda vid de unionsbyråerna, i stödgrupperna för migrationshantering. Målet med utplaceringen av de enheter och grupper som avses i artikel 2.8 och 2.9 i förordning (EU) 2016/1624 är att ge tekniskt och operativt stöd till begärande medlemsstater, särskilt de som står inför oproportionellt stora migrationsutmaningar. För att de enheter och grupper som avses i artikel 2.8 och 2.9 i den förordningen ska kunna utföra sina arbetsuppgifter behöver de åtkomst till SIS genom ett tekniskt gränssnitt som kopplar Europeiska gräns- och kustbevakningsbyrån till det centrala SIS. I ärenden där en sökning i SIS som de enheter och grupper som avses i artikel 2.8 och 2.9 i förordning (EU) 2016/1624 eller personalen gör visar att det finns en registrering som förts in av en medlemsstat kan medlemmen i enheten eller gruppen eller personalen inte vidta de åtgärder som krävs utan tillstånd från värdmedlemsstaten. Därför bör värdmedlemsstaten informeras så att den kan följa upp ärendet. Värdmedlemsstaten bör genom utbyte av tilläggsinformation underrätta den registrerande medlemsstaten om träffen.
- (67) Vissa aspekter av SIS kan inte täckas på ett uttömmande sätt av denna förordning på grund av deras tekniska beskaffenhet, detaljnivå och behov av regelbunden uppdatering. Dessa aspekter inkluderar bland annat tekniska bestämmelser om införande av, uppdatering av, radering av och sökning i uppgifter, uppgifternas kvalitet och

<sup>(1)</sup> Europaparlamentets och rådets förordning (EU) 2016/1624 av den 14 september 2016 om en europeisk gräns- och kustbevakning och om ändring av Europaparlamentets och rådets förordning (EU) 2016/399 och upphävande av Europaparlamentets och rådets förordning (EG) nr 863/2007, rådets förordning (EG) nr 2007/2004 och rådets beslut 2005/267/EG (EUT L 251, 16.9.2016, s. 1).



bestämmelser om biometriska uppgifter, bestämmelser om överensstämmelse och prioriteringsordningen för av registreringar, länkar mellan registreringar, fastställande av lagringstiden för registreringar inom den längsta tillåtna tidsfristen och utbyte av tilläggsinformation. Kommissionen bör därför tilldelas genomförandebefogenheter avseende dessa aspekter. Tekniska bestämmelser om sökning i registreringar bör ta hänsyn till att de nationella tillämpningarna ska fungera smidigt.

- (68) För att säkerställa enhetliga villkor för genomförandet av denna förordning, bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011<sup>(1)</sup>. Förfarandet för antagande av genomförandeaakter bör vara detsamma för den här förordningen som för förordning (EU) 2018/1861.
- (69) För att säkerställa öppenhet bör eu-LISA två år efter inledandet av SIS-verksamheten enligt denna förordning utarbeta en rapport om hur det centrala SIS och kommunikationsinfrastrukturen fungerar tekniskt, inklusive säkerheten i dessa, och om det bilaterala och multilaterala utbytet av tilläggsinformation. Kommissionen bör lägga fram en övergripande utvärdering vart fjärde år.
- (70) I syfte att säkerställa att SIS fungerar smidigt bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på nya underkategorier av föremål som ska eftersökas enligt registreringar om föremål som ska beslagtas eller användas som bevis i brottmål, och fastställande av under vilka omständigheter användandet av fotografier och ansiktsbilder bör vara tillåtet för identifiering av personer i andra sammanhang än vid reguljära gränsövergångsställen. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning<sup>(2)</sup>. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.
- (71) Eftersom målen för denna förordning, nämligen att inrätta och reglera ett informationssystem inom unionen och utbytet av relaterad tilläggsinformation, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av deras natur, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (72) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna. Denna förordning respekterar i synnerhet fullt ut skyddet av personuppgifter i enlighet med artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna, samtidigt som den syftar till att säkerställa en trygg miljö för alla personer som vistas på unionens territorium och särskilt skydd för barn som kan ha fallit offer för människohandel eller bortförande. I fall som rör barn bör i första hand beaktas vad som bedöms vara barnets bästa.
- (73) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, deltar Danmark inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Danmark. Eftersom denna förordning är en utveckling av Schengenregelverket ska Danmark, i enlighet med artikel 4 i det protokollet, inom sex månader efter det att rådet har beslutat om denna förordning, besluta huruvida landet ska genomföra den i sin nationella rätt.
- (74) Förenade kungariket deltar i denna förordning i enlighet med artikel 5.1 i protokoll nr 19 om Schengenregelverket införlivat inom Europeiska unionens ramar, fogat till EU-fördraget och EUF-fördraget, och i enlighet med artikel 8.2 i rådets beslut 2000/365/EG<sup>(3)</sup>.
- (75) Irland deltar i denna förordning i enlighet med artikel 5.1 i protokoll nr 19 fogat till EU-fördraget och EUF-fördraget, och i enlighet med artikel 6.2 i rådets beslut 2002/192/EG<sup>(4)</sup>.

<sup>(1)</sup> Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

<sup>(2)</sup> EUT L 123, 12.5.2016, s. 1.

<sup>(3)</sup> Rådets beslut 2000/365/EG av den 29 maj 2000 om en begäran från Förenade konungariket Storbritannien och Nordirland om att få delta i vissa bestämmelser i Schengenregelverket (EGT L 131, 1.6.2000, s. 43).

<sup>(4)</sup> Rådets beslut 2002/192/EG av den 28 februari 2002 om Irlands begäran om att få delta i vissa bestämmelser i Schengenregelverket (EGT L 64, 7.3.2002, s. 20).

- (76) När det gäller Island och Norge utgör denna förordning, i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket <sup>(1)</sup>, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.G i rådets beslut 1999/437/EG <sup>(2)</sup>.
- (77) När det gäller Schweiz utgör denna förordning, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket <sup>(3)</sup>, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.G i beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2008/149/RIF <sup>(4)</sup>.
- (78) När det gäller Liechtenstein utgör denna förordning, i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Lichtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket <sup>(5)</sup>, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.G i beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2011/349/EU <sup>(6)</sup>.
- (79) När det gäller Bulgarien och Rumänien utgör denna förordning en akt som utvecklar Schengenregelverket eller som på annat sätt har samband med detta i den mening som avses i artikel 4.2 i 2005 års anslutningsakt och bör läsas jämförd med rådets beslut 2010/365/EU <sup>(7)</sup> och (EU) 2018/934 <sup>(8)</sup>.
- (80) När det gäller Kroatien utgör denna förordning en akt som utvecklar Schengenregelverket eller som på annat sätt har samband med detta i den mening som avses i artikel 4.2 i 2011 års anslutningsakt och bör läsas jämförd med rådets beslut (EU) 2017/733 <sup>(9)</sup>.
- (81) När det gäller Cypern utgör denna förordning en akt som utvecklar Schengenregelverket eller som på annat sätt har samband med detta i den mening som avses i artikel 3.2 i 2003 års anslutningsakt.
- (82) Denna förordning bör tillämpas på Irland från och med tidpunkter fastställda i enlighet med de förfaranden som avses i de berörda instrumenten för tillämpningen av Schengenregelverket på denna stat.
- (83) Genom denna förordning införs en rad förbättringar av SIS som kommer att öka dess effektivitet, stärka dataskyddet och utöka åtkomsträtten. Vissa av dessa förbättringar kräver inte någon komplex teknisk utveckling medan andra kräver tekniska förändringar av varierande omfattning. För att förbättringarna av systemet ska bli tillgängliga för slutanvändarna så snart som möjligt införs genom denna förordning ändringar av beslut 2007/533/RIF i flera faser. En rad förbättringar av systemet bör tillämpas omedelbart efter det att denna förordning har trätt i kraft medan andra bör tillämpas antingen ett eller två år efter det att den har trätt i kraft. Denna förordning bör vara tillämplig i sin helhet inom tre år efter det att den har trätt i kraft. För att undvika att tillämpningen försenas bör det stegvisa genomförandet av denna förordning noga övervakas.

<sup>(1)</sup> EGT L 176, 10.7.1999, s. 36.

<sup>(2)</sup> Rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtal som har ingåtts mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EGT L 176, 10.7.1999, s. 31).

<sup>(3)</sup> EUT L 53, 27.2.2008, s. 52.

<sup>(4)</sup> Rådets beslut 2008/149/RIF av den 28 januari 2008 om ingående på Europeiska unionens vägnar av avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 53, 27.2.2008, s. 50).

<sup>(5)</sup> EUT L 160, 18.6.2011, s. 21.

<sup>(6)</sup> Rådets beslut 2011/349/EU av den 7 mars 2011 om ingående på Europeiska unionens vägnar av protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, särskilt om polissamarbete och straffrättsligt samarbete (EUT L 160, 18.6.2011, s. 1).

<sup>(7)</sup> Rådets beslut 2010/365/EU av den 29 juni 2010 om tillämpningen av de bestämmelser i Schengenregelverket som rör Schengens informationssystem i Republiken Bulgarien och Rumänien (EUT L 166, 1.7.2010, s. 17).

<sup>(8)</sup> Rådets beslut (EU) 2018/934 av den 25 juni 2018 om inledande av tillämpningen av återstående bestämmelser i Schengenregelverket rörande Schengens informationssystem i Republiken Bulgarien och Rumänien (EUT L 165, 2.7.2018, s. 37).

<sup>(9)</sup> Rådets beslut (EU) 2017/733 av den 25 april 2017 om tillämpningen av de bestämmelser i Schengenregelverket som rör Schengens informationssystem i Republiken Kroatien (EUT L 108, 26.4.2017, s. 31).

- (84) Europaparlamentets och rådets förordning (EG) nr 1986/2006 <sup>(1)</sup>, beslut 2007/533/RIF och kommissionens beslut 2010/261/EU <sup>(2)</sup> bör upphöra att gälla med verkan från och med den dag då här förordningen tillämpas fullt ut.
- (85) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 <sup>(3)</sup> och avgav sitt yttrande den 3 maj 2017.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

#### KAPITEL I

### Allmänna bestämmelser

#### Artikel 1

### Allmänt syfte med SIS

Syftet med SIS ska vara att med hjälp av information som överförs genom detta system säkerställa en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, inbegripet bevarande av allmän säkerhet och allmän ordning och skydd av säkerheten på medlemsstaternas territorier, samt att säkerställa tillämpningen av bestämmelserna i kapitlen 4 och 5 i tredje delen avdelning V i EUF-fördraget avseende rörlighet för personer på deras territorier.

#### Artikel 2

### Syfte

1. I denna förordning fastställs villkor och förfaranden för införande och behandling av registreringar i SIS om personer och föremål samt för utbyte av tilläggsinformation och kompletterande uppgifter som används för polissamarbete och straffrättsligt samarbete.
2. Denna förordning innehåller också bestämmelser om den tekniska strukturen för SIS, om ansvarsområden för medlemsstaterna och Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (nedan kallad *eu-LISA*), om databehandling, om berörda personers rättigheter samt om skadeståndsansvar.

#### Artikel 3

### Definitioner

I denna förordning avses med

1. *registrering*: en sammanställning av uppgifter som förts in i SIS och med hjälp av vilka de behöriga myndigheterna kan identifiera en person eller ett föremål med avseende på en specifik åtgärd som ska vidtas.
2. *tilläggsinformation*: information som inte ingår i registreringsuppgifterna i SIS, men som har samband med registreringar i SIS och som ska utbytas genom Sirenekontoren
  - a) för att medlemsstaterna ska kunna samråda med eller underrätta varandra när de för in en registrering,
  - b) för att lämpliga åtgärder ska kunna vidtas vid en träff,
  - c) när den begärda åtgärden inte kan vidtas,
  - d) när SIS-uppgifternas kvalitet hanteras,
  - e) när registreringarnas överensstämmelse och prioritet hanteras,
  - f) när åtkomsträttigheter hanteras.
3. *kompletterande uppgifter*: sådana uppgifter i SIS som har samband med registreringar i SIS och som ska vara omedelbart tillgängliga för de behöriga myndigheterna när en person om vilken uppgifter har förts in i SIS lokaliseras till följd av att en sökning utförs i SIS.

<sup>(1)</sup> Europaparlamentets och rådets förordning (EG) nr 1986/2006 av den 20 december 2006 om tillträde till andra generationen av Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon (EUT L 381, 28.12.2006, s. 1).

<sup>(2)</sup> Kommissionens beslut 2010/261/EU av den 4 maj 2010 om en säkerhetsplan för det centrala SIS II och kommunikationsinfrastrukturen (EUT L 112, 5.5.2010, s. 31).

<sup>(3)</sup> Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

4. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.
5. *behandling av personuppgifter*: en åtgärd eller kombination av åtgärder beträffande personuppgifter, eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, loggning, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
6. *matchning*: förekomsten av följande steg:
  - a) en slutanvändare har utfört en sökning i SIS,
  - b) den sökningen har påvisat en registrering som förts in i SIS av en annan medlemsstat, och
  - c) uppgifterna i registreringen i SIS matchar sökuppgifterna.
7. *träff*: en matchning som uppfyller följande kriterier:
  - a) den har bekräftats av
    - i) slutanvändaren, eller
    - ii) den behöriga myndigheten i enlighet med nationella förfaranden, om den berörda matchningen grundades på en jämförelse av biometriska uppgifter,och
  - b) ytterligare åtgärder begärs.
8. *flaggning*: tillfälligt upphävande av giltigheten på nationell nivå för en registrering, som kan fogas till registreringar om gripande, registreringar om försvunna och sårbara personer och registreringar om diskreta kontroller, undersökningskontroller och särskilda kontroller.
9. *registrerande medlemsstat*: den medlemsstat som har fört in registreringen i SIS.
10. *verkställande medlemsstat*: den medlemsstat som vidtar eller har vidtagit de begärda åtgärderna till följd av en träff.
11. *slutanvändare*: en anställd vid en behörig myndighet som har befogenhet att söka direkt i CS-SIS, N.SIS eller en teknisk kopia.
12. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska eller fysiologiska kännetecken och som möjliggör eller bekräftar den unika identifieringen av denna fysiska person, nämligen fotografier, ansiktsbilder, fingeravtrycksuppgifter och DNA-profil.
13. *fingeravtrycksuppgifter*: uppgifter om fingeravtryck och handavtryck som på grund av sin unika karaktär och de referenspunkter som de innefattar möjliggör exakta och entydiga jämförelser för att fastställa en persons identitet.
14. *ansiktsbild*: digitala bilder av ansiktet med tillräcklig bildupplösning och kvalitet för att de ska kunna användas för automatiserad biometrisk matchning.
15. *DNA-profil*: en bokstavs- eller nummerkod som representerar en rad identifikationsuppgifter i den icke-kodifierande delen av ett analyserat mänskligt DNA-prov, dvs. den särskilda molekyllära strukturen vid de olika DNA-lokusen.
16. *terroristbrott*: sådana brott enligt nationell rätt som avses i artiklarna 3–14 i Europaparlamentets och rådets direktiv (EU) 2017/541 <sup>(1)</sup> eller som är likvärdiga med ett av dessa brott för de medlemsstater som inte är bundna av det direktivet.
17. *hot mot folkhälsan*: ett hot mot folkhälsan enligt definitionen i artikel 2.21 i Europaparlamentets och rådets förordning (EU) 2016/399 <sup>(2)</sup>.

<sup>(1)</sup> Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017, s. 6).

<sup>(2)</sup> Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna) (EUT L 77, 23.3.2016, s. 1).

## Artikel 4

**Teknisk struktur och drift av SIS**

1. SIS ska bestå av följande delar:

- a) Ett centralt system (nedan kallat *det centrala SIS*) bestående av
  - i) en teknisk stödfunktion (nedan kallat *CS-SIS*) som innehåller en databas (nedan kallad *SIS-databasen*), och inklusive en backup av CS-SIS,
  - ii) ett enhetligt nationellt gränssnitt (nedan kallat *NI-SIS*).
- b) Ett nationellt system (nedan kallat *N.SIS*) i var och en av medlemsstaterna, bestående av de nationella datasystem som står i förbindelse med det centrala SIS, inklusive minst en nationell eller gemensam backup av N.SIS.
- c) En kommunikationsinfrastruktur som förenar CS-SIS och dess backup samt NI-SIS (nedan kallad *kommunikationsinfrastrukturen*) och som tillhandahåller ett krypterat virtuellt nätverk särskilt avsett för SIS-uppgifter och utbytet av uppgifter mellan Sirenekontoren i enlighet med vad som avses i artikel 7.2.

Ett N.SIS som avses i led b får innehålla en datafil (nedan kallad *nationell kopia*) med en fullständig eller partiell kopia av SIS-databasen. Två eller flera medlemsstater får i ett av sina N.SIS upprätta en gemensam kopia som dessa medlemsstater får använda gemensamt. En sådan gemensam kopia ska betraktas som var och en av dessa medlemsstaters nationella kopia.

En gemensam backup av N.SIS som avses i led b får användas gemensamt av två eller flera medlemsstater. I sådana fall ska den gemensamma backupen av N.SIS betraktas som var och en av de dessa medlemsstaters backup av N.SIS. N.SIS och dess backup får användas samtidigt för att säkerställa oavbruten tillgång för slutanvändarna.

De medlemsstater som avser att upprätta en gemensam kopia eller en gemensam backup av N.SIS som ska användas gemensamt ska skriftligen komma överens om sina respektive ansvarsområden. De ska underrätta kommissionen om sin överenskommelse.

Kommunikationsinfrastrukturen ska stödja och bidra till att säkerställa oavbruten tillgång till SIS. Den ska inbegripa redundanta och separata sökvägar för anslutningarna mellan CS-SIS och dess backup och även inbegripa redundanta och separata sökvägar för anslutningarna mellan varje nationell SIS-nätanslutningspunkt och CS-SIS och dess backup.

2. Medlemsstaterna ska föra in, uppdatera, radera och söka i SIS-uppgifter genom sina egna N.SIS. De medlemsstater som använder en partiell eller fullständig nationell kopia eller en partiell eller fullständig gemensam kopia ska göra den kopian tillgänglig för automatisk sökning på var och en av de medlemsstaternas territorium. Den partiella nationella eller gemensamma kopian ska innehålla åtminstone de uppgifter som förtecknas i artikel 20.3 a–v. Det ska inte vara möjligt att söka i datafilerna i andra medlemsstaters N.SIS utom när det gäller gemensamma kopior.

3. CS-SIS ska användas för teknisk tillsyn och administration och ha en backup av CS-SIS, varigenom alla funktioner i CS-SIS-huvudsystemet kan säkerställas om det systemet skulle sluta fungera. CS-SIS och dess backup ska vara belägna i eu-LISA:s två tekniska anläggningar.

4. eu-LISA ska genomföra tekniska lösningar för att förstärka den oavbrutna tillgången till SIS antingen via samtidig drift av CS-SIS och dess backup, förutsatt att backupen alltjämt kan säkerställa driften av SIS om CS-SIS skulle sluta att fungera, eller genom överlappning av systemet eller dess delar. Trots de förfarandekrav som fastställs i artikel 10 i förordning (EU) 2018/1726 ska eu-LISA senast den 28 december 2019 genomföra en undersökning av möjliga tekniska lösningar, som innehåller en oberoende konsekvensbedömning och en kostnads-nyttoanalys.

5. Vid behov får eu-LISA i undantagsfall tillfälligt upprätta ytterligare en kopia av SIS-databasen.

6. CS-SIS ska tillhandahålla de tjänster som krävs för införande och behandling av SIS-uppgifter, inbegripet sökningar i SIS-databasen. För de medlemsstater som använder en nationell eller gemensam kopia ska CS-SIS

- a) tillhandahålla uppdatering online av de nationella kopiorna,
- b) säkerställa synkronisering och enhetlighet mellan de nationella kopiorna och SIS-databasen, och
- c) hantera initialisering och återställande av de nationella kopiorna.

7. CS-SIS ska säkra oavbruten tillgång.

*Artikel 5***Kostnader**

1. Kostnaderna för drift, underhåll och vidareutveckling av det centrala SIS och kommunikationsinfrastrukturen ska belasta unionens allmänna budget. Dessa kostnader ska innefatta sådant arbete med CS-SIS som görs för att säkerställa tillhandahållandet av de tjänster som avses i artikel 4.6.
2. Kostnaderna för inrättande, drift, underhåll och vidareutveckling av varje enskilt N.SIS ska belasta den berörda medlemsstatens budget.

*KAPITEL II***Medlemsstaternas ansvar***Artikel 6***Nationella system**

Varje medlemsstat ska ansvara för att inrätta, driva, underhålla och vidareutveckla sitt N.SIS och ansluta sitt N.SIS till NI-SIS.

Varje medlemsstat ska ansvara för att säkerställa oavbruten tillgång till SIS-uppgifter för slutanvändarna.

Varje medlemsstat ska överföra sina registreringar genom sitt N.SIS.

*Artikel 7***N.SIS-byrå och Sirenekontor**

1. Varje medlemsstat ska utse en myndighet (nedan kallad *N.SIS-byrån*) som ska ha det centrala ansvaret för dess N.SIS.

Den myndigheten ska ansvara för att N.SIS fungerar smidigt och för dess säkerhet, säkerställa att de behöriga myndigheterna har åtkomst till SIS och vidta nödvändiga åtgärder för att säkerställa att denna förordning följs. Myndigheten ska ansvara för att säkerställa att alla funktioner i SIS är vederbörligen tillgängliga för slutanvändarna.

2. Varje medlemsstat ska utse en nationell myndighet (nedan kallat *Sirenekontoret*) som ska vara i drift dygnet runt alla dagar i veckan och som ska säkerställa utbyte av och tillgång till all tilläggsinformation i enlighet med Sirenehandboken. Varje Sirenekontor ska fungera som en enda kontaktpunkt för sin medlemsstat för utbyte av tilläggsinformation om registreringar och för att underlätta vidtagandet av begärda åtgärder när registreringar om personer eller föremål har förts in i SIS och dessa personer eller föremål lokaliseras till följd av en träff.

Varje Sirenekontor ska i enlighet med nationell rätt ha lätt, direkt eller indirekt, tillgång till all relevant nationell information, bland annat nationella databaser och all information om sin medlemsstats registreringar, och till expertrådgivning för att snabbt och inom de tidsfrister som fastställs i artikel 8 kunna reagera på en begäran om tilläggsinformation.

Sirenekontoren ska samordna kontrollen av kvaliteten på den information som förs in i SIS. För dessa ändamål ska de ha tillgång till de uppgifter som behandlas i SIS.

3. Medlemsstaterna ska förse eu-LISA med uppgifter om sin N.SIS-byrå och om sitt Sirenekontor. eu-LISA ska offentliggöra en förteckning över N.SIS-byråerna och Sirenekontoren tillsammans med den förteckning som avses i artikel 56.7.

*Artikel 8***Utbyte av tilläggsinformation**

1. Tilläggsinformation ska utbytas i enlighet med Sirenehandboken, via kommunikationsinfrastrukturen. Medlemsstaterna ska tillhandahålla de tekniska resurser och personalresurser som behövs för att säkerställa oavbruten tillgång till och snabbt och effektivt utbyte av tilläggsinformation. Om kommunikationsinfrastrukturen inte är tillgänglig ska medlemsstaterna använda annan tillfredsställande säker teknik för att utbyta tilläggsinformation. En förteckning över tillfredsställande säker teknik ska fastställas i Sirenehandboken.

2. Tilläggsinformationen ska bara användas för det syfte för vilket den överförts i enlighet med artikel 64, om inte förhandstillstånd för annan användning har inhämtats från den registrerande medlemsstaten.

3. Sirenekontoren ska utföra sina uppgifter snabbt och effektivt, i synnerhet genom att besvara en begäran om tilläggsinformation så snart som möjligt, dock senast 12 timmar efter det att begäran mottagits. Vid registreringar om terroristbrott, registreringar om personer som är efterlysta för att gripas och överlämnas eller utlämnas och registreringar om barn i enlighet med vad som avses i artikel 32.1 c ska Sirenekontoren agera omedelbart.

En begäran om tilläggsinformation med högsta prioritet ska förses med påskriften "URGENT" i Sireneformuläret och en förklaring till varför ärendet är brådskande.

4. Kommissionen ska anta genomförandeakter för att fastställa närmare bestämmelser om Sirenekontorens uppgifter enligt denna förordning och om utbytet av tilläggsinformation i form av en handbok kallad *Sirenehandboken*. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 9

### Teknisk och funktionell överensstämmelse

1. Varje medlemsstat ska, för snabb och effektiv dataöverföring, när den inrättar sitt N.SIS följa de gemensamma standarder, protokoll och tekniska förfaranden som har fastställts för att säkerställa kompatibilitet mellan dess N.SIS och centrala SIS.

2. Om en medlemsstat använder en nationell kopia, ska den med hjälp av de tjänster som tillhandahålls av CS-SIS och genom de automatiska uppdateringar som avses i artikel 4.6 säkerställa att de uppgifter som lagrats i den nationella kopian överensstämmer med och är identiska med dem i SIS-databasen och att en sökning i den nationella kopian ger samma resultat som en sökning i SIS-databasen.

3. Slut användarna ska få de uppgifter som krävs för att de ska kunna utföra sina uppgifter, i synnerhet och vid behov alla tillgängliga uppgifter som gör det möjligt att identifiera den registrerade och vidta begärda åtgärder.

4. Medlemsstaterna och eu-LISA ska genomföra regelbundna tester för att kontrollera den tekniska överensstämmelsen hos de nationella kopior som avses i punkt 2. Resultaten av dessa tester ska beaktas som en del av den mekanism som inrättats genom rådets förordning (EU) nr 1053/2013 <sup>(1)</sup>.

5. Kommissionen ska anta genomförandeakter för att fastställa och utveckla de gemensamma standarder, protokoll och tekniska förfaranden som avses i punkt 1 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 10

### Säkerhet – Medlemsstaterna

1. Varje medlemsstat ska med avseende på sitt eget N.SIS vidta de nödvändiga åtgärderna, bland annat anta en säkerhetsplan, en driftskontinuitetsplan och en katastrofplan, för att

- a) fysiskt skydda uppgifter, bland annat genom att utarbeta beredskapsplaner för skydd av kritisk infrastruktur,
- b) hindra obehöriga från att få tillträde till databehandlingsanläggningar som används för behandling av personuppgifter (kontroll av tillträde till anläggningar),
- c) förhindra obehörig läsning, kopiering och ändring eller obehörigt avlägsnande av datamedier (kontroll av datamedier),
- d) hindra obehörig inmatning av uppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter (lagringskontroll),
- e) förhindra att obehöriga använder ett automatiskt databehandlingssystem med hjälp av datakommunikationsutrustning (användarkontroll),
- f) förhindra att uppgifter i SIS obehörigt behandlas samt att uppgifter som behandlas i SIS obehörigt ändras eller raderas (kontroll av uppgiftsinmatningen),
- g) säkerställa att personer som är behöriga att använda ett automatiskt databehandlingssystem har åtkomst endast till de uppgifter som omfattas av deras åtkomstbehörighet och endast med hjälp av individuella och unika användaridentifikationer och skyddade åtkomstmetoder (åtkomstkontroll),

<sup>(1)</sup> Rådets förordning (EU) nr 1053/2013 av den 7 oktober 2013 om inrättande av en utvärderings- och övervakningsmekanism för kontroll av tillämpningen av Schengenregelverket och om upphävande av verkställande kommitténs beslut av den 16 september 1998 om inrättande av Ständiga kommittén för genomförande av Schengenkonventionen (EUT L 295, 6.11.2013, s. 27).

- h) säkerställa att alla myndigheter med åtkomsträtt till SIS eller rätt till tillträde till databehandlingsanläggningar skapar profiler som beskriver uppgifter och ansvar för personer som är behöriga att få åtkomst till, föra in, uppdatera, radera och söka i uppgifter och på begäran och utan dröjsmål ger de tillsynsmyndigheter som avses i artikel 69.1 tillgång till dessa profiler (personalprofiler),
  - i) säkerställa möjlighet att kontrollera och fastställa till vilka organ personuppgifter får överföras via datakommunikationsutrustning (kommunikationskontroll),
  - j) säkerställa möjlighet till efterföljande kontroll och fastställande av vilka personuppgifter som matats in i ett automatiskt databehandlingssystem samt när, av vem och för vilket ändamål (inmatningskontroll),
  - k) hindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med såväl överföring av personuppgifter som transport av datamedier, särskilt med hjälp av lämplig krypteringsteknik (transportkontroll),
  - l) övervaka att de säkerhetsåtgärder som avses i denna punkt är ändamålsenliga och vidta nödvändiga organisatoriska åtgärder i fråga om intern övervakning för att säkerställa att denna förordning efterlevs (egenrevision),
  - m) säkerställa att det installerade systemet i händelse av driftavbrott kan återställas till normal drift (återställande), och
  - n) säkerställa att SIS utför sina funktioner korrekt, att fel rapporteras (funktionssäkerhet) och att personuppgifter som lagras i SIS inte kan förvanskas genom funktionsfel (dataintegritet).
2. Medlemsstaterna ska vidta åtgärder som är likvärdiga med dem som avses i punkt 1 när det gäller säkerheten vid behandling och utbyte av tilläggsinformation, bland annat genom att säkra Sirenekontorens lokaler.
3. Medlemsstaterna ska vidta åtgärder som är likvärdiga med dem som avses i punkt 1 i den här artikeln när det gäller säkerheten vid behandling av SIS-uppgifterna av de myndigheter som avses i artikel 44.
4. De åtgärder som beskrivs i punkterna 1, 2 och 3 får ingå i en allmän säkerhetsstrategi och säkerhetsplan på nationell nivå som omfattar flera it-system. I sådana fall ska de krav som anges i denna artikel och deras tillämplighet på SIS tydligt framgå i och säkerställas genom den planen.

#### Artikel 11

##### **Konfidentialitet – Medlemsstaterna**

1. Varje medlemsstat ska i enlighet med sin nationella rätt tillämpa sina regler avseende tystnadsplikt eller motsvarande konfidentialitetskrav på alla personer och organ som arbetar med SIS-uppgifter och tilläggsinformation. Denna skyldighet ska gälla även efter det att personerna lämnat sin tjänst eller anställning eller efter det att organens verksamhet upphört.
2. Om en medlemsstat samarbetar med externa entreprenörer i samband med SIS-relaterade uppgifter, ska den noga övervaka entreprenörens verksamhet för att säkerställa att alla bestämmelser i denna förordning följs, särskilt i fråga om säkerhet, konfidentialitet och dataskydd.
3. Den operativa förvaltningen av N.SIS eller av tekniska kopior får inte anförtros privata företag eller privata organisationer.

#### Artikel 12

##### **Loggar på nationell nivå**

1. Medlemsstaterna ska säkerställa att all åtkomst till och alla utbyten av personuppgifter i CS-SIS loggas i deras N.SIS för att möjliggöra kontroll av huruvida sökningen var laglig, övervakning av att databehandlingen sker på ett lagligt sätt, egenkontroll, säkerställande av att N.SIS fungerar tillfredsställande samt för dataintegritet och datasäkerhet. Detta krav gäller inte de automatiska processer som avses i artikel 4.6 a, b och c.
2. Loggarna ska i synnerhet visa registreringshistoriken, dag och tidpunkt för databehandlingen, vilka uppgifter som användes för sökningen, en hänvisning till de uppgifter som behandlades och de individuella och unika användaridentifikationerna för den behöriga myndighet och den person som behandlade uppgifterna.
3. Om sökningen görs med fingeravtrycksuppgifter eller en ansiktsbild i enlighet med artikel 43 ska loggarna, genom undantag från punkt 2 i den här artikeln, visa vilken typ av uppgifter som användes för sökningen i stället för de faktiska uppgifterna.



4. Loggarna får endast användas för det ändamål som avses i punkt 1 och ska raderas tre år efter det att de skapades. De loggar som omfattar registreringshistorik ska raderas tre år efter det att registreringarna raderats.
5. Loggarna får sparas längre än de perioder som avses i punkt 4 om de behövs för kontrollförfaranden som redan pågår.
6. De nationella behöriga myndigheter som är ansvariga för kontroll av huruvida sökningen är laglig, övervakning av att databehandlingen sker på ett lagligt sätt, egenkontroll, säkerställande av att N.SIS fungerar tillfredsställande samt dataintegritet och datasäkerhet ska inom gränserna för sin behörighet på begäran ha åtkomst till loggarna, så att de kan fullgöra sina uppgifter.
7. Då medlemsstaterna i enlighet med nationell rätt utför automatiska skanningssökningar av motorfordons nummerplåtar med automatiska nummerplåtsavläsningsystem ska de föra en logg över sökningarna i enlighet med nationell rätt. Vid behov får en fullständig sökning göras i SIS för att kontrollera om en träff har erhållits. Punkterna 1–6 ska tillämpas på alla fullständiga sökningar.
8. Kommissionen ska anta genomförandeakter för att fastställa innehållet i den logg som avses i punkt 7 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 13

### Egenkontroll

Medlemsstaterna ska säkerställa att varje myndighet som har åtkomsträtt till SIS-uppgifter vidtar de åtgärder som är nödvändiga för att följa denna förordning och vid behov samarbetar med tillsynsmyndigheten.

#### Artikel 14

### Personalutbildning

1. Personalen vid de myndigheter som har åtkomsträtt till SIS ska, innan de får behörighet att behandla uppgifter som lagras i SIS och regelbundet efter det att åtkomst till SIS-uppgifter beviljats, utbildas på lämpligt sätt om datasäkerhet, om grundläggande rättigheter, inbegripet dataskydd, och om de regler och förfaranden för databehandling som anges i Sirenehandboken. Personalen ska informeras om relevanta bestämmelser om brott och sanktioner, inklusive de som fastställs i artikel 73.
2. Medlemsstaterna ska ha ett nationellt utbildningsprogram för SIS som ska omfatta utbildning för både slutanvändarna och Sirenekontorens personal.

Utbildningsprogrammet får ingå i ett allmänt utbildningsprogram på nationell nivå som omfattar utbildning på andra relevanta områden.

3. I syfte att förbättra samarbetet mellan Sirenekontoren ska det minst en gång om året anordnas gemensam utbildning på unionsnivå.

#### KAPITEL III

### eu-LISA:S ansvarsområden

#### Artikel 15

### Operativ förvaltning

1. eu-LISA ska ansvara för den operativa förvaltningen av det centrala SIS. I samarbete med medlemsstaterna ska eu-LISA säkerställa att bästa tillgängliga teknik alltid används för det centrala SIS, med förbehåll för en kostnads-nyttöanalys.
2. eu-LISA ska även ansvara för följande uppgifter avseende kommunikationsinfrastrukturen:
  - a) Övervakning.
  - b) Säkerhet.
  - c) Samordning av förbindelserna mellan medlemsstaterna och leverantören.
  - d) Uppgifter avseende budgetens genomförande.
  - e) Förvärv och förnyande.
  - f) Avtalsfrågor.

3. eu-LISA ska även ansvara för följande uppgifter avseende Sirenekontoren och kommunikationen mellan Sirenekontoren:

- a) Samordning och förvaltning av samt stöd till tester.
- b) Underhåll och uppdatering av tekniska specifikationer för utbytet av tilläggsinformation mellan Sirenekontoren och kommunikationsinfrastrukturen.
- c) Hantering av effekterna av tekniska förändringar som påverkar både SIS och utbytet av tilläggsinformation mellan Sirenekontoren.

4. eu-LISA ska utveckla och underhålla en mekanism och förfaranden för kvalitetskontroll av uppgifterna i CS-SIS. Den ska i det avseendet regelbundet rapportera till medlemsstaterna.

eu-LISA ska regelbundet rapportera till kommissionen om problem som uppstått och vilka medlemsstater som berörs.

Kommissionen ska regelbundet rapportera till Europaparlamentet och rådet om problem som har uppstått i fråga om uppgifternas kvalitet.

5. eu-LISA ska också utföra uppgifter som rör tillhandahållande av utbildning om teknisk användning av SIS och om åtgärder för att förbättra kvaliteten på SIS-uppgifter.

6. Den operativa förvaltningen av det centrala SIS ska omfatta alla de uppgifter som krävs för att det centrala SIS ska kunna fungera dygnet runt sju dagar i veckan i enlighet med denna förordning, särskilt det underhåll och den tekniska utveckling som krävs för att systemet ska kunna fungera smidigt. Dessa uppgifter ska även omfatta samordning och förvaltning av samt stöd till tester för det centrala SIS och N.SIS, som säkerställer att det centrala SIS och N.SIS fungerar i enlighet med de krav på teknisk och funktionell överensstämmelse som anges i artikel 9.

7. Kommissionen ska anta genomförandeakter för att fastställa de tekniska kraven för kommunikationsinfrastrukturen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 16

#### Säkerhet – eu-LISA

1. eu-LISA ska vidta de nödvändiga åtgärderna, bland annat anta en säkerhetsplan, en driftskontinuitetsplan och en katastrofplan för det centrala SIS och kommunikationsinfrastrukturen, för att

- a) fysiskt skydda uppgifter, bland annat genom att utarbeta beredskapsplaner för skydd av kritisk infrastruktur,
- b) hindra obehöriga från att få tillträde till databehandlingsanläggningar som används för behandling av personuppgifter (kontroll av tillträde till anläggningar),
- c) förhindra obehörig läsning, kopiering och ändring eller obehörigt avlägsnande av datamedier (kontroll av datamedier),
- d) hindra obehörig inmatning av uppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter (lagringskontroll),
- e) förhindra att obehöriga använder ett automatiskt databehandlingssystem med hjälp av datakommunikationsutrustning (användarkontroll),
- f) förhindra att uppgifter i SIS obehörigt behandlas samt att uppgifter som behandlas i SIS obehörigt ändras eller raderas (kontroll av uppgiftsinmatningen),
- g) säkerställa att personer som är behöriga att använda ett automatiskt databehandlingssystem har åtkomst endast till de uppgifter som omfattas av deras åtkomstbehörighet och endast med hjälp av individuella och unika användaridentifikationer och skyddade åtkomstmetoder (åtkomstkontroll),
- h) skapa profiler som beskriver uppgifter och ansvar för personer som har behörighet att få åtkomst till uppgifterna eller tillträde till databehandlingsanläggningarna och på begäran och utan dröjsmål ge Europeiska datatillsynsmannen tillgång till dessa profiler (personalprofiler),
- i) säkerställa möjlighet att kontrollera och fastställa till vilka organ personuppgifter får överföras via datakommunikationsutrustning (kommunikationskontroll),
- j) säkerställa möjlighet till efterföljande kontroll och granskning av vilka personuppgifter som matats in i ett automatiskt databehandlingssystem samt när och av vem (inmatningskontroll),

- k) hindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med såväl överföring av personuppgifter som transport av datamedier, särskilt med hjälp av lämplig krypteringsteknik (transportkontroll),
  - l) övervaka att de säkerhetsåtgärder som avses i denna punkt är ändamålsenliga och vidta nödvändiga organisatoriska åtgärder i fråga om intern övervakning för att säkerställa att denna förordning efterlevs (egenrevision),
  - m) säkerställa att det installerade systemet i händelse av driftavbrott kan återställas till normal drift (återställande),
  - n) säkerställa att SIS utför sina funktioner korrekt, att fel rapporteras (funktionssäkerhet) och att personuppgifter som lagras i SIS inte kan förvanskas genom funktionsfel (dataintegritet), och
  - o) säkerställa att dess tekniska anläggningar är säkra.
2. eu-LISA ska vidta åtgärder som är likvärdiga med dem som avses i punkt 1 när det gäller säkerheten vid behandling och utbyte av tilläggsinformation via kommunikationsinfrastrukturen.

#### Artikel 17

### Konfidentialitet – eu-LISA

1. Utan att det påverkar tillämpningen av artikel 17 i tjänsteföreskrifterna ska eu-LISA tillämpa lämpliga regler om tystnadsplikt eller motsvarande konfidentialitetskrav som är jämförbara med dem som anges i artikel 11 i denna förordning på all personal som arbetar med SIS-uppgifter. Den skyldigheten ska gälla även efter det att personerna lämnat sin tjänst eller anställning eller efter det att verksamheten upphört.
2. eu-LISA ska vidta åtgärder som är likvärdiga med de åtgärder som avses i punkt 1 när det gäller konfidentialitet vid utbyte av tilläggsinformation via kommunikationsinfrastrukturen.
3. Om eu-LISA samarbetar med externa entreprenörer i samband med SIS-relaterade uppgifter, ska den noga övervaka entreprenörens verksamhet för att säkerställa att alla bestämmelser i denna förordning följs, särskilt i fråga om säkerhet, konfidentialitet och dataskydd.
4. Den operativa förvaltningen av CS-SIS får inte anförtros privata företag eller privata organisationer.

#### Artikel 18

### Loggar på central nivå

1. eu-LISA ska säkerställa att all åtkomst till personuppgifter i CS-SIS och alla utbyten av sådana uppgifter i CS-SIS loggas för de ändamål som anges i artikel 12.1.
2. Loggarna ska i synnerhet visa registreringshistoriken, dag och tidpunkt för databehandlingen, vilka uppgifter som användes för sökningen, en hänvisning till de uppgifter som behandlades och de individuella och unika användaridentifikationer för den behöriga myndighet som behandlade uppgifterna.
3. Om sökningen görs med fingeravtrycksuppgifter eller ansiktsbilder i enlighet med artikel 43 ska loggarna, genom undantag från punkt 2 i den här artikeln, visa vilken typ av uppgifter som användes för sökningen i stället för de faktiska uppgifterna.
4. Loggarna får endast användas för de ändamål som avses i punkt 1 och ska raderas tre år efter det att de skapades. De loggar som omfattar registreringshistorik ska raderas tre år efter det att registreringarna raderats.
5. Loggar får bevaras längre än de perioder som avses i punkt 4 om de behövs för kontrollförfaranden som redan pågår.
6. För att möjliggöra egenkontroll och säkerställande av att CS-SIS fungerar tillfredsställande samt dataintegritet och datasäkerhet, ska eu-LISA ha åtkomst till loggarna inom gränserna för sin behörighet.

Europeiska datatillsynsmannen ska på begäran ha åtkomst till dessa loggar inom gränserna för sin behörighet och i syfte att fullgöra sina uppgifter.

## KAPITEL IV

**Information till allmänheten**

## Artikel 19

**Informationskampanjer om SIS**

När denna förordning börjar tillämpas ska kommissionen, i samarbete med tillsynsmyndigheterna och Europeiska datatillsynsmannen, genomföra en informationskampanj för att informera allmänheten om målen med SIS, vilka uppgifter som lagras i SIS, vilka myndigheter som har åtkomst till SIS och de registrerades rättigheter. Kommissionen ska upprepa sådana kampanjer regelbundet, i samarbete med tillsynsmyndigheterna och Europeiska datatillsynsmannen. Kommissionen ska upprätthålla en webbplats som är tillgänglig för allmänheten och tillhandahåller all relevant information om SIS. Medlemsstaterna ska, i samarbete med sina tillsynsmyndigheter, utforma och genomföra de nödvändiga strategierna för att ge sina medborgare och invånare allmän information om SIS.

## KAPITEL V

**Uppgiftskategorier och flaggning**

## Artikel 20

**Uppgiftskategorier**

1. Utan att det påverkar tillämpningen av artikel 8.1 eller de bestämmelser i denna förordning som gäller lagring av kompletterande uppgifter ska SIS endast innehålla de uppgiftskategorier som lämnas av varje medlemsstat, så som krävs för de syften som fastställs i artiklarna 26, 32, 34, 36, 38 och 40.
2. Uppgiftskategorierna ska vara följande:
  - a) Uppgifter om personer för vilka en registrering har förts in.
  - b) Uppgifter om de föremål som avses i artiklarna 26, 32, 34, 36 och 38.
3. En registrering i SIS som omfattar uppgifter om personer får endast innehålla följande:
  - a) Efternamn.
  - b) Förnamn.
  - c) Namn vid födelsen.
  - d) Tidigare använda namn och alias.
  - e) Särskilda, objektiva, fysiska kännetecken som inte förändras.
  - f) Födelseort.
  - g) Födelsedatum.
  - h) Kön.
  - i) Samtliga medborgarskap.
  - j) Huruvida personen
    - i) är beväpnad,
    - ii) är våldsbenägen,
    - iii) har avvikit eller rymt,
    - iv) är självmordsbenägen,
    - v) utgör ett hot mot folkhälsan eller
    - vi) deltar i en verksamhet som avses i artiklarna 3–14 i direktiv (EU) 2017/541.
  - k) Orsak till registreringen.
  - l) Myndighet som skapade registreringen.
  - m) Hänvisning till det beslut som gett upphov till registreringen.
  - n) Åtgärd som ska vidtas vid en träff.
  - o) Länkar till andra registreringar i enlighet med artikel 63.
  - p) Typ av brott.
  - q) Personens registreringsnummer i ett nationellt register.
  - r) För de registreringar som avses i artikel 32.1, en kategorisering av ärendetypen.
  - s) Identifieringshandlingarnas kategori.

- t) Land som utfärdat identifieringshandlingarna.
- u) Identifieringshandlingarnas nummer.
- v) Identifieringshandlingarnas utfärdandedatum.
- w) Fotografier och ansiktsbilder.
- x) Relevanta DNA-profiler i enlighet med artikel 42.3.
- y) Fingeravtrycksuppgifter.
- z) En kopia av identifieringshandlingarna, om möjligt i färg.

4. Kommissionen ska anta genomförandeakter för att fastställa och utveckla de tekniska bestämmelser som är nödvändiga för att föra in, uppdatera, radera och söka i de uppgifter som avses i punkterna 2 och 3 i den här artikeln samt de gemensamma standarder som avses i punkt 5 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

5. De tekniska bestämmelserna ska vara snarlika för sökningar i CS-SIS, i nationella eller gemensamma kopior och i tekniska kopior som avses i artikel 56.2. De ska bygga på gemensamma standarder.

#### Artikel 21

### Proportionalitet

1. Innan medlemsstaterna för in en registrering och när de förlänger en registrerings giltighetstid ska de pröva om ärendet är tillräckligt adekvat, relevant och viktigt för att motivera en registrering i SIS.
2. Om en person eller ett föremål söks i samband med en registrering med anknytning till ett terroristbrott ska ärendet anses vara tillräckligt adekvat, relevant och viktigt för att motivera en registrering i SIS. Av skäl som rör allmän eller nationell säkerhet kan medlemsstaterna i undantagsfall avstå från att föra in en registrering, när denna sannolikt skulle försvåra officiella eller rättsliga utredningar, undersökningar eller förfaranden.

#### Artikel 22

### Krav vid införande av en registrering

1. Den minimiuppsättning uppgifter som krävs för att föra in en registrering i SIS ska vara de uppgifter som avses i artikel 20.3 a, g, k och n, förutom i de situationer som avses i artikel 40. De övriga uppgifter som avses i den punkten ska också föras in i SIS, om de finns tillgängliga.
2. De uppgifter som avses i artikel 20.3 e i den här förordningen får endast föras in när detta är absolut nödvändigt för att identifiera den berörda personen. När sådana uppgifter förs in ska medlemsstaterna säkerställa att artikel 10 i direktiv (EU) 2016/680 efterlevs.

#### Artikel 23

### Överensstämmelse mellan registreringar

1. Innan medlemsstaten för in en registrering ska den kontrollera huruvida den berörda personen eller föremålet redan är föremål för en registrering i SIS. För att kontrollera om personen redan är föremål för en registrering ska en kontroll med fingeravtrycksuppgifter också göras om sådana uppgifter är tillgängliga.
2. Endast en registrering per person eller per föremål per medlemsstat får föras in i SIS. Där så är nödvändigt får nya registreringar om samma person eller föremål föras in av andra medlemsstater, i enlighet med punkt 3.
3. Om en person eller ett föremål redan är föremål för en registrering i SIS ska en medlemsstat som önskar föra in en ny registrering kontrollera att registreringarna inte är sinsemellan oförenliga. Om de inte är oförenliga får medlemsstaten föra in den nya registreringen. Om registreringarna är oförenliga ska de berörda medlemsstaternas Sirenekontor samråda med varandra genom att utbyta tilläggsinformation för att nå en överenskommelse. Bestämmelser om överensstämmelse mellan registreringar ska fastställas i Sirenehandboken. Bestämmelserna om överensstämmelse får frångås efter samråd mellan medlemsstaterna om viktiga nationella intressen står på spel.
4. Vid träffar på flera registreringar om samma person eller föremål ska den verkställande medlemsstaten iaktta den prioritetsordning för registreringar som fastställs i Sirenehandboken.

Om en person är föremål för flera registreringar som förts in av olika medlemsstater ska registreringar om gripande som förts in i enlighet med artikel 26 verkställas i första hand om inte annat följer av artikel 25.

#### Artikel 24

### Allmänna bestämmelser om flaggning

1. Om en medlemsstat anser att verkställandet av en registrering som förts in i enlighet med artikel 26, 32 eller 36 är oförenlig med dess nationella rätt, internationella förpliktelser eller viktiga nationella intressen, får den kräva att registreringen förses med en flagga, vilken innebär att den åtgärd som ska vidtas på grund av registreringen inte kommer att vidtas på dess territorium. Flaggan ska läggas till av Sirenekontoret i den registrerande medlemsstaten.
2. För att medlemsstaterna ska kunna kräva att en registrering som förts in i enlighet med artikel 26 förses med en flagga ska alla medlemsstater genom utbyte av tilläggsinformation automatiskt underrättas om att en ny registrering av denna kategori har lagts in.
3. Om en registrerande medlemsstat i särskilt brådskande och allvarliga ärenden begär att åtgärden ska verkställas, ska den verkställande medlemsstaten pröva om den flaggning som lagts till på dess begäran kan dras tillbaka. Om den verkställande medlemsstaten kan gå med på detta ska den vidta de åtgärder som krävs för att säkerställa att åtgärden kan verkställas omedelbart.

#### Artikel 25

### Flaggning av registreringar om gripande för överlämnande

1. När rambeslut 2002/584/RIF är tillämpligt ska en medlemsstat begära att den registrerande medlemsstaten lägger till en flagga som förhindrar gripandet av en person som en uppföljning till en registrering om gripande för överlämnande, om den rättsliga myndighet som enligt nationell rätt är behörig att verkställa en europeisk arresteringsorder har vägrat att verkställa ordern på grund av att det finns skäl för att inte verkställa den och om tillägget av en flagga har krävts.

En medlemsstat får också kräva att en flagga läggs till registreringen om dess behöriga rättsliga myndighet under överlämnandeförfarandet friger den person som är föremål för registreringen.

2. På begäran av en rättslig myndighet som enligt nationell rätt är behörig, på grundval av en allmän instruktion eller i särskilda fall, får en medlemsstat även begära att den registrerande medlemsstaten lägger till en flagga till en registrering om gripande för överlämnande om det är uppenbart att verkställandet av den europeiska arresteringsordern ska vägras.

#### KAPITEL VI

### Registreringar om personer som är efterlysta för att gripas och överlämnas eller utlämnas

#### Artikel 26

### Syfte och villkor för införande av registreringar

1. Registreringar om personer som är efterlysta för att gripas och överlämnas på grundval av en europeisk arresteringsorder eller registreringar om personer som är efterlysta för att gripas och utlämnas ska föras in på begäran av den rättsliga myndigheten i den registrerande medlemsstaten.
2. Registreringar om gripande för överlämnande ska också föras in på grundval av arresteringsorder som utfärdats i enlighet med avtal som, på grundval av fördragen, ingåtts mellan unionen och tredjeländer om överlämnande av personer på grundval av en arresteringsorder och som medger att en sådan arresteringsorder översänds via SIS.
3. Alla hänvisningar i denna förordning till bestämmelser i rambeslut 2002/584/RIF ska anses inbegripa motsvarande bestämmelser i avtal som på grundval av fördragen, ingåtts mellan unionen och tredjeländer om överlämnande av personer på grundval av en arresteringsorder och som medger att en sådan arresteringsorder översänds via SIS.
4. Under en pågående insats får den registrerande medlemsstaten tillfälligt göra en befintlig registrering om gripande som förts in i enlighet med denna artikel otillgänglig för sökningar av slutanvändarna i de medlemsstater som är involverade i insatsen. I sådana fall ska registreringen endast vara åtkomlig för Sirenekontoren. Medlemsstaterna ska endast göra en registrering otillgänglig om
  - a) insatsens syfte inte kan uppnås genom andra åtgärder,
  - b) ett förhandstillstånd har beviljats av den behöriga rättsliga myndigheten i den registrerande medlemsstaten, och
  - c) alla medlemsstater som är involverade i insatsen har informerats genom utbyte av tilläggsinformation.

Den funktion som föreskrivs i första stycket får endast användas under en period på högst 48 timmar. Om det är operativt nödvändigt får den dock förlängas med ytterligare perioder på 48 timmar. Medlemsstaterna ska föra statistik om antalet registreringar för vilka denna funktion har använts.

5. Om det finns tydliga tecken på att de föremål som avses i artikel 38.2 a, b, c, e, g, h, j och k har koppling till en person som är föremål för en registrering enligt punkterna 1 och 2 i den här artikeln får registreringar om dessa föremål föras in för att lokalisera personen. I sådana fall ska registreringen om personen och registreringen om föremålet länkas i enlighet med artikel 63.

6. Kommissionen ska anta genomförandeakter för att fastställa och utveckla bestämmelser som är nödvändiga för att föra in, uppdatera, radera och söka i de uppgifter som avses i punkt 5 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 27

##### **Kompletterande uppgifter om personer som är efterlysta för att gripas och överlämnas**

1. Om en person är efterlyst för att gripas och överlämnas på grundval av en europeisk arresteringsorder ska den registrerande medlemsstaten föra in en kopia av originalet av den europeiska arresteringsordern i SIS.

En medlemsstat får föra in en kopia av fler än en europeisk arresteringsorder i en registrering om gripande för överlämnande.

2. Den registrerande medlemsstaten får också föra in en kopia av en översättning av den europeiska arresteringsordern på ett eller flera av unionens institutioners officiella språk.

#### Artikel 28

##### **Tilläggsinformation om personer som är efterlysta för att gripas och överlämnas**

Den registrerande medlemsstaten för en registrering om gripande för överlämnande ska lämna de uppgifter som avses i artikel 8.1 i rambeslut 2002/584/RIF till de övriga medlemsstaterna genom utbyte av tilläggsinformation.

#### Artikel 29

##### **Tilläggsinformation om personer som är efterlysta för att gripas och utlämnas**

1. Den registrerande medlemsstaten för en registrering om utlämning ska lämna följande uppgifter till samtliga övriga medlemsstater genom utbyte av tilläggsinformation:

- a) Vilken myndighet som begärt gripandet.
- b) Huruvida det finns en arresteringsorder eller någon annan handling med samma rättsverkan eller en verkställbar dom.
- c) Brottets art och brottsrubriceringen.
- d) En beskrivning av de omständigheter under vilka brottet begåtts, inbegripet tidpunkt, plats och i vilken grad den registrerade personen varit delaktig i brottet.
- e) Så långt möjligt, brottets konsekvenser.
- f) Annan information som är användbar eller nödvändig för verkställande av registreringen.

2. De uppgifter som avses i punkt 1 i den här artikeln ska inte lämnas om de uppgifter som avses i artikel 27 eller 28 redan har lämnats och de anses vara tillräckliga för att den verkställande medlemsstaten ska kunna verkställa registreringen.

#### Artikel 30

##### **Konvertering av en åtgärd som ska vidtas angående registreringar om gripande för överlämnande eller utlämning**

Om ett gripande inte kan verkställas antingen på grund av att den anmodade medlemsstaten vägrar att göra detta i enlighet med förfarandena för flaggning i artikel 24 eller 25 eller, när det gäller en registrering om gripande för utlämning, på grund av att en utredning ännu inte har avslutats, ska den medlemsstat som anmodas att utföra gripandet vidta åtgärder på grundval av registreringen genom att meddela var den berörda personen befinner sig.

*Artikel 31***Verkställande av en åtgärd på grundval av en registrering om gripande för överlämnande eller utlämning**

1. En registrering som förts in i SIS i enlighet med artikel 26 och de kompletterande uppgifter som avses i artikel 27 ska tillsammans utgöra, och ha samma verkan som, en europeisk arresteringsorder som utfärdats i enlighet med rambeslut 2002/584/RIF när det rambeslutet är tillämpligt.
2. När rambeslut 2002/584/RIF inte är tillämpligt ska en registrering som förts in i SIS i enlighet med artiklarna 26 och 29 ha samma rättsliga verkan som en framställning om provisoriskt anhållande enligt artikel 16 i den europeiska utlämningskonventionen av den 13 december 1957, eller artikel 15 i Beneluxfördraget om utlämning och inbördes rättshjälp i brottmål av den 27 juni 1962.

*KAPITEL VII****Registreringar om försvunna personer eller sårbara personer som behöver hindras från att resa****Artikel 32***Syfte och villkor för införande av registreringar**

1. Registreringar ska föras in i SIS om följande kategorier av personer på begäran av den behöriga myndigheten i den registrerande medlemsstaten:
  - a) Försvunna personer som behöver ställas under beskydd
    - i) med hänsyn till deras egen säkerhet,
    - ii) för att förebygga ett hot mot den allmänna ordningen eller den allmänna säkerheten.
  - b) Försvunna personer som inte behöver ställas under beskydd.
  - c) Barn som löper risk att bortföras av en förälder, familjemedlem eller vårdnadshavare och som behöver hindras från att resa.
  - d) Barn som behöver hindras från att resa på grund av en konkret och uppenbar risk för att de avlägsnas från eller lämnar en medlemsstats territorium och
    - i) blir offer för människohandel, eller för tvångsäktenskap, kvinnlig könsstympning eller andra former av könsrelaterat våld,
    - ii) blir offer för eller involveras i terroristbrott, eller
    - iii) blir inkallade eller värvas till väpnade grupper eller tvingas delta aktivt i fientligheter.
  - e) Sårbara myndiga personer som för sin egen säkerhet behöver hindras från att resa på grund av en konkret och uppenbar risk för att de avlägsnas från eller lämnar en medlemsstats territorium och blir offer för människohandel eller könsrelaterat våld.
2. Punkt 1 a ska särskilt vara tillämplig på barn och på personer som måste placeras på institution till följd av ett beslut av en behörig myndighet.
3. En registrering om ett barn som avses i punkt 1 c ska föras in till följd av ett beslut av de behöriga myndigheterna, inklusive de rättsliga myndigheter i medlemsstaterna som är behöriga i mål om föräldraansvar, om det föreligger en konkret och uppenbar risk att barnet olagligt och omgående kan avlägsnas från den medlemsstat där de behöriga myndigheterna är belägna.
4. En registrering om de personer som avses i punkt 1 d och e ska föras in till följd av ett beslut av de behöriga myndigheterna, inklusive rättsliga myndigheter.
5. Den registrerande medlemsstaten ska regelbundet se över behovet av att behålla de registreringar som avses i punkt 1 c, d och e i den här artikeln i enlighet med artikel 53.4.
6. Den registrerande medlemsstaten ska säkerställa att:
  - a) de uppgifter som den för in i SIS anger till vilken av kategorierna i punkt 1 personen som berörs av registreringen hör,
  - b) de uppgifter som den för in i SIS anger vilken ärendetyp som föreligger, om detta är känt, och
  - c) dess Sirenekontor har tillgång till all relevant information, när det gäller registreringar som förts in i enlighet med punkt 1 c, d och e, vid tidpunkten för skapandet av registreringen.



7. Fyra månader innan ett barn som är föremål för en registrering enligt denna artikel når myndighetsålder i enlighet med nationell rätt i den registrerande medlemsstaten ska CS-SIS automatiskt underrätta den registrerande medlemsstaten om antingen att grunden för registreringen och den åtgärd som ska vidtas måste uppdateras eller att registreringen måste raderas.

8. Om det finns tydliga tecken på att de föremål som avses i artikel 38.2 a, b, c, e, g, h och k har koppling till en person som är föremål för en registrering i enlighet med punkt 1 i den här artikeln får registreringar om dessa föremål föras in för att lokalisera personen. I sådana fall ska registreringen om personen och registreringen om föremålet länkas i enlighet med artikel 63.

9. Kommissionen ska anta genomförandeakter för att fastställa och utveckla bestämmelser om kategorisering av ärendetyp och om införande av de uppgifter som avses i punkt 6. Ärendetyperna rörande försvunna personer som är barn ska omfatta bland annat, men inte vara begränsade till, barn som rymt, ensamkommande barn i samband med migration och barn som löper risk för bortförande.

Kommissionen ska också anta genomförandeakter för att fastställa och utveckla tekniska bestämmelser som är nödvändiga för att föra in, uppdatera, radera och söka i de uppgifter som avses i punkt 8.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

### Artikel 33

#### Verkställande av åtgärder på grundval av en registrering

1. När en person som avses i artikel 32 lokaliseras ska den verkställande medlemsstatens behöriga myndigheter, med förbehåll för kraven i punkt 4, underrätta den registrerande medlemsstaten om var personen befinner sig.

2. När det gäller personer som behöver ställas under beskydd som avses i artikel 32.1 a, c, d och e ska den verkställande medlemsstaten omedelbart samråda med sina egna behöriga myndigheter och de behöriga myndigheterna i den registrerande medlemsstaten genom utbyte av tilläggsinformation för att utan dröjsmål komma överens om vilka åtgärder som ska vidtas. De behöriga myndigheterna i den verkställande medlemsstaten får, i enlighet med nationell rätt, föra sådana personer till en säker plats för att förhindra dem från att fortsätta sin resa.

3. När det gäller barn ska alla beslut om de åtgärder som ska vidtas eller alla beslut om att föra barnet till en säker plats i enlighet med punkt 2 fattas utifrån barnets bästa. Sådana beslut ska fattas omedelbart och senast 12 timmar efter det att barnet har lokaliserats, i förekommande fall i samråd med berörda barnskyddsmyndigheter.

4. Uppgifter om en försvunnen myndig person som har lokaliserats får inte vidarebefordras utan dennas samtycke, utom mellan de behöriga myndigheterna. De behöriga myndigheterna får emellertid meddela den person som har rapporterat personen som försvunnen att registreringen har raderats eftersom den försvunna personen har lokaliserats.

### KAPITEL VIII

#### Registreringar om personer som söks för att delta i ett rättsligt förfarande

### Artikel 34

#### Syfte och villkor för införande av registreringar

1. I syfte att meddela personernas vistelseort eller hemvist ska medlemsstaterna på begäran av en behörig myndighet i SIS föra in SIS-registreringar om

- a) vittnen,
- b) personer som har kallats eller personer som söks för att kallas att inställa sig inför rättsliga myndigheter i samband med ett brottmålsförfarande för att stå till svars för gärningar som de åtalas för,
- c) personer som ska delges en dom i ett brottmål eller andra handlingar i samband med ett brottmålsförfarande för att stå till svars för gärningar som de åtalas för,
- d) personer som ska delges en kallelse att inställa sig för verkställighet av ett frihetsberövande straff.

2. Om det finns tydliga tecken på att de föremål som avses i artikel 38.2 a, b, c, e, g, h och k har koppling till en person som är föremål för en registrering i enlighet med punkt 1 i den här artikeln får registreringar om dessa föremål föras in för att lokalisera personen. I sådana fall ska registreringarna om personen och registreringen om föremålet länkas i enlighet med artikel 63.

3. Kommissionen ska anta genomförandeakter för att fastställa och utveckla de tekniska bestämmelser som är nödvändiga för införandet, uppdateringen och raderingen av samt sökningen i de uppgifter som avses i punkt 2 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 35

### Verkställande av åtgärder på grundval av en registrering

De begärda uppgifterna ska lämnas till den registrerandemedlemsstaten genom utbyte av tilläggsinformation.

#### KAPITEL IX

### **Registreringar om personer och föremål för diskreta kontroller, undersökningskontroller eller särskilda kontroller**

#### Artikel 36

### Syfte och villkor för införande av registreringar

1. Registreringar om personer, om föremål som avses i artikel 38.2 a, b, c, e, g, h, j, k och l samt om andra betalningsmedel än kontanter ska föras in i överensstämmelse med nationell rätt i den registrerande medlemsstaten, i syfte att genomföra diskreta kontroller, undersökningskontroller eller särskilda kontroller i enlighet med artikel 37.3, 37.4 och 37.5.

2. När registreringar förs in för diskreta kontroller, undersökningskontroller eller särskilda kontroller, och om den information som den registrerande medlemsstaten eftersöker är kompletterande till de uppgifter som föreskrivs i artikel 37.1 a–h, ska den registrerande medlemsstaten i registreringen lägga till vilken information som eftersöks. Om denna information rör särskilda kategorier av personuppgifter som avses i artikel 10 i direktiv (EU) 2016/680 får den endast eftersökas om det är absolut nödvändigt för registreringens specifika syfte och i samband med det brott för vilket registreringen har förts in.

3. Registreringar om personer för diskreta kontroller, undersökningskontroller eller särskilda kontroller får föras in för att förebygga, förhindra, avslöja, utreda eller lagföra brott, verkställa en straffrättslig påföljd och förebygga hot mot den allmänna säkerheten under en eller flera av följande omständigheter:

- a) Om det finns tydliga tecken på att en person avser att begå, eller redan begår, något av de brott som avses i artikel 2.1 och 2.2 i rambeslut 2002/584/RIF.
- b) Om den information som avses i artikel 37.1 är nödvändig för att verkställa ett fängelsestraff eller en annan frihetsberövande åtgärd för en person som dömts för något av de brott som avses i artikel 2.1 och 2.2 i rambeslut 2002/584/RIF.
- c) Om en allmän bedömning av en person, särskilt på grundval av redan begångna brott, leder till misstanke om att den personen kan komma att begå de brott som avses i artikel 2.1 och 2.2 i rambeslut 2002/584/RIF i framtiden.

4. På begäran av de myndigheter som ansvarar för den nationella säkerheten får registreringar om personer för diskreta kontroller, undersökningskontroller eller särskilda kontroller dessutom föras in i enlighet med nationell rätt om det finns konkreta tecken på att de uppgifter som avses i artikel 37.1 är nödvändiga för att avvärja ett allvarligt hot som den berörda personen utgör eller andra allvarliga hot mot statens inre eller yttre säkerhet. Den medlemsstat som förde in registreringen i enlighet med denna punkt ska informera de övriga medlemsstaterna om en sådan registrering. Varje medlemsstat ska besluta till vilka myndigheter informationen ska överlämnas. Informationen ska överföras genom Sirenekontoren.

5. Om det finns tydliga tecken på att föremål som avses i artikel 38.2 a, b, c, e, g, h, j, k och l eller andra betalningsmedel än kontanter har samband med de grova brott som avses i punkt 3 i den här artikeln eller de allvarliga hot som avses i punkt 4 i den här artikeln får registreringar föras in om dessa föremål och länkas till de registreringar som förts in i enlighet med punkterna 3 och 4 i den här artikeln.

6. Kommissionen ska anta genomförandeakter för att fastställa och utveckla de tekniska bestämmelser som är nödvändiga för att föra in, uppdatera, radera och söka i de uppgifter som avses i punkt 5 i den här artikeln samt den kompletterande information som avses i punkt 2 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

## Artikel 37

**Verkställande av åtgärder på grundval av en registrering**

1. I syfte att genomföra diskreta kontroller, undersökningskontroller eller särskilda kontroller ska den verkställande medlemsstaten samla in och översända samtliga eller vissa av följande uppgifter till den registrerande medlemsstaten:
  - a) Det faktum att den person som är föremål för en registrering eller föremål som avses i artikel 38.2 a, b, c, e, g, h, j, k och l eller andra betalningsmedel än kontanter som är föremål för en registrering har lokaliserats.
  - b) Plats och tid för samt anledning till kontrollen.
  - c) Resväg och målet för resan.
  - d) Personer som åtföljer föremålet för registreringen, eller passagerare i fordonet, fartyget eller luftfartyget, eller personer som medföljer innehavaren av det officiella blankodokumentet eller de utfärdade id-handlingarna, vilka rimligen kan antas ha anknytning till föremålet för registreringen.
  - e) Varje avslöjad identitet och varje personlig beskrivning av den person som använder det officiella blankodokumentet eller de utfärdade id-handlingar som är föremål för registreringen.
  - f) De föremål som avses i artikel 38.2 a, b, c, e, g, h, j, k och l eller andra betalningsmedel än kontanter som använts.
  - g) Medförda föremål, även resehandlingar.
  - h) De omständigheter under vilka personen, de föremål som avses i artikel 38.2 a, b, c, e, g, h, j, k och l eller andra betalningsmedel än kontanter lokaliserades.
  - i) All annan information som eftersöks av den registrerande medlemsstaten i enlighet med artikel 36.2.

Om den information som avses i första stycket led i i denna punkt rör de särskilda kategorier av personuppgifter som avses i artikel 10 i direktiv (EU) 2016/680 ska den behandlas i enlighet med de villkor som fastställs i den artikeln och endast om den kompletterar andra personuppgifter som behandlas för samma ändamål.

2. Den verkställande medlemsstaten ska lämna den information som avses i punkt 1 genom utbyte av tilläggsinformation.
3. En diskret kontroll ska bestå av diskret insamling av så många av de uppgifter som beskrivs i punkt 1 som möjligt i samband med den rutinmässiga verksamhet som utförs av den verkställande medlemsstatens nationella behöriga myndigheter. Insamlingen av denna information får inte äventyra kontrollernas diskreta karaktär, och den person som är föremål för registreringen får inte på något sätt göras medveten om att det finns en registrering.
4. En undersökningskontroll ska bestå av en utfrågning av personen, bland annat på grundval av information eller specifika frågor som den registrerande medlemsstaten i enlighet med artikel 36.2 har lagt till registreringen. Utfrågningen ska utföras i enlighet med den nationella rätten i den verkställande medlemsstaten.
5. Inom ramen för särskilda kontroller får personer kroppsvisiteras och fordon, fartyg, luftfartyg, containrar och medförda föremål genomsökas för de syften som anges i artikel 36. Kroppsvisitering och genomsökning ska ske i enlighet med den verkställande medlemsstatens nationella rätt.
6. Om den verkställande medlemsstatens nationella rätt inte tillåter särskilda kontroller ska kontrollerna i den medlemsstaten ersättas med undersökningskontroller. Om den verkställande medlemsstatens nationella rätt inte tillåter undersökningskontroller ska kontrollerna i den medlemsstaten ersättas med diskreta kontroller. Om direktiv 2013/48/EU är tillämpligt ska medlemsstaterna säkerställa att rätten till tillgång till försvarare för misstänkta och tilltalade respekteras på de villkor som fastställs i det direktivet.
7. Punkt 6 ska inte påverka medlemsstaternas skyldighet att göra den information som eftersöks i enlighet med artikel 36.2 tillgänglig för slutanvändarna.

## KAPITEL X

**Registreringar om föremål som ska beslagtas eller användas som bevis i brottmål**

## Artikel 38

**Syfte och villkor för införande av registreringar**

1. Medlemsstaterna ska föra in registreringar i SIS om föremål som eftersöks för att antingen beslagtas eller användas som bevis i brottmål.

2. Registreringar ska föras in om följande kategorier av lätt identifierbara föremål:
  - a) Motorfordon oavsett framdrivningssystem.
  - b) Släpvagnar med en tjänstevikt överstigande 750 kg.
  - c) Husvagnar.
  - d) Industriell utrustning.
  - e) Fartyg.
  - f) Fartygsmotorer.
  - g) Containrar.
  - h) Luftfartyg.
  - i) Flygmotorer.
  - j) Skjutvapen.
  - k) Officiella blankodokument som är stulna, bortförda eller försvunna eller ger intryck av att vara sådana handlingar men är falska.
  - l) Utfärdade identitetshandlingar, till exempel pass, id-kort, uppehållstillstånd, resehandlingar och körkort, vilka är stulna, bortförda, försvunna eller ogiltiga eller ger intryck av att vara sådana handlingar men är falska.
  - m) Fordonsregistreringsbevis och nummerplåtar som är stulna, bortförda, försvunna eller ogiltiga eller ger intryck av att vara sådana bevis eller nummerplåtar men är falska.
  - n) Sedlar (registrerade sedlar) och falska sedlar.
  - o) It-produkter.
  - p) Identifierbara beståndsdelar av motorfordon.
  - q) Identifierbara beståndsdelar av industriell utrustning.
  - r) Andra identifierbara föremål av högt värde, enligt definitionen i enlighet med punkt 3.

När det gäller de handlingar som avses i leden k, l och m får den registrerande medlemsstaten specificera huruvida dessa handlingar är stulna, bortförda, försvunna, ogiltiga eller falska.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 75 för att ändra denna förordning genom att fastställa nya underkategorier av föremål i punkt 2 o, p, q och r i den här artikeln.

4. Kommissionen ska anta genomförandeakter för att fastställa och utveckla de tekniska bestämmelser som är nödvändiga för att föra in, uppdatera, radera eller söka i de uppgifter som avses i punkt 2 i den här artikeln. Dessa genomförande akter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 39

### Verkställande av åtgärder på grundval av en registrering

1. Om en sökning visar att det finns en registrering om ett lokaliserat föremål ska den behöriga myndigheten i enlighet med sin nationella rätt beslagta föremålet och kontakta den registrerande medlemsstatens myndighet för att komma överens om vilka åtgärder som ska vidtas. För detta ändamål får även personuppgifter översändas i enlighet med denna förordning.
2. Den information som avses i punkt 1 ska lämnas genom utbyte av tilläggsinformation.
3. Den verkställande medlemsstaten ska vidta de begärda åtgärderna i enlighet med nationell rätt.

#### KAPITEL XI

### Registreringar om okända efterlysta personer för identifiering i enlighet med nationell rätt

#### Artikel 40

### Registreringar om okända efterlysta personer för identifiering i enlighet med nationell rätt

Medlemsstaterna får föra in registreringar i SIS om okända efterlysta personer som innehåller endast fingeravtrycksuppgifter. Dessa fingeravtrycksuppgifter ska antingen vara fullständiga eller ofullständiga uppsättningar fingeravtryck eller handavtryck som upptäckts på platsen för ett terroristbrott eller annat grovt brott som utreds. De ska endast föras in i SIS om det kan fastställas att de med mycket hög sannolikhet tillhör en gärningsman.

Om den behöriga myndigheten i den registrerande medlemsstaten inte kan fastställa den misstänktes identitet på grundval av uppgifter från någon annan relevant nationell eller internationell databas eller unionsdatabas får de fingeravtrycksuppgifter som avses i första stycket endast föras in i denna kategori av registreringar som *okänd efterlyst person* för identifiering av en sådan person.

#### Artikel 41

### Verkställande av åtgärder på grundval av en registrering

Vid en träff med de uppgifter som förs in enligt artikel 40 ska personens identitet fastställas i enlighet med nationell rätt, tillsammans med en expertkontroll av att fingeravtrycksuppgifterna i SIS tillhör den personen. De verkställande medlemsstaterna ska lämna information om personens identitet och om var personen befinner sig till den registrerande medlemsstaten genom utbyte av tilläggsinformation för att underlätta att ärendet utreds snabbt.

#### KAPITEL XII

### Särskilda bestämmelser för biometriska uppgifter

#### Artikel 42

### Särskilda bestämmelser för införande av fotografier, ansiktsbilder, fingeravtrycksuppgifter och DNA-profiler

1. Endast fotografier, ansiktsbilder och fingeravtrycksuppgifter som avses i artikel 20.3 w och y och som uppfyller minimistandarder för uppgiftskvalitet och tekniska specifikationer ska föras in i SIS. Innan sådana uppgifter förs in ska en kvalitetskontroll utföras i syfte att fastställa att minimistandarderna för uppgifternas kvalitet och de tekniska specifikationerna är uppfyllda.
2. Fingeravtrycksuppgifter som förs in i SIS får bestå av ett till tio platta fingeravtryck och ett till tio rullade fingeravtryck. De får också inbegripa upp till två handavtryck.
3. En DNA-profil får endast läggas till i registreringar i de situationer som anges i artikel 32.1 a och endast efter en kvalitetskontroll med syftet att fastställa huruvida minimistandarderna för uppgifternas kvalitet och de tekniska specifikationerna är uppfyllda samt enbart om det inte finns några fotografier, ansiktsbilder eller fingeravtrycksuppgifter tillgängliga eller om de inte lämpar sig för identifiering. DNA-profiler från personer som är släktingar i rakt upp- eller nedstigande led eller syskon till den person som är föremål för registreringen får läggas till i registreringen förutsatt att de berörda personerna ger sitt uttryckliga samtycke. Om en DNA-profil läggs till i en registrering ska den profilen innehålla det minimum av information som är absolut nödvändig för att identifiera den försvunna personen.
4. Minimistandarder för uppgiftskvalitet och tekniska specifikationer ska fastställas i enlighet med punkt 5 i den här artikeln för lagring av de biometriska uppgifter som avses i punkterna 1 och 3 i den här artikeln. Dessa minimistandarder för uppgiftskvalitet och tekniska specifikationer ska fastställa den kvalitetsnivå som krävs för användning av uppgifterna för att kontrollera en persons identitet i enlighet med artikel 43.1 och för användning av uppgifterna för att identifiera en person i enlighet med artikel 43.2–43.4.
5. Kommissionen ska anta genomförandeakter för att fastställa de minimistandarder för uppgiftskvalitet och tekniska specifikationer som avses i punkterna 1, 3 och 4 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 43

### Särskilda bestämmelser om kontroll eller sökning med fotografier, ansiktsbilder, fingeravtrycksuppgifter och DNA-profiler

1. Om fotografier, ansiktsbilder, fingeravtrycksuppgifter och DNA-profiler finns tillgängliga i en registrering i SIS ska sådana fotografier, ansiktsbilder, fingeravtrycksuppgifter och DNA-profiler användas för att bekräfta identiteten på en person som har lokaliserats efter en alfanumerisk sökning i SIS.
2. En sökning i fingeravtrycksuppgifter för att identifiera en person får göras i samtliga fall. En sökning i fingeravtrycksuppgifter ska dock göras för att identifiera en person om det inte går att fastställa personens identitet på annat sätt. Det centrala SIS ska därför innehålla ett automatiskt fingeravtrycksidentifieringssystem (Afis).
3. En sökning i fingeravtrycksuppgifter i SIS avseende registreringar som förts in i enlighet med artiklarna 26, 32, 36 och 40 får också göras med användande av fullständiga eller ofullständiga uppsättningar fingeravtryck eller handavtryck som upptäckts på platsen för ett grovt brott eller terroristbrott som utreds, om det med stor sannolikhet kan fastställas att dessa uppsättningar avtryck tillhör en gärningsman, förutsatt att sökningen görs samtidigt i medlemsstaternas relevanta nationella fingeravtrycksdatabaser.

4. Fotografier och ansiktsbilder får användas för identifiering av personer vid reguljära gränsövergångsställen så snart detta blir tekniskt möjligt, förutsatt att man säkerställer att identifieringen är mycket tillförlitlig.

Innan denna funktion har genomförts i SIS ska kommissionen lägga fram en rapport om huruvida den teknik som krävs är klar att tas i bruk, finns tillgänglig och är tillförlitlig. Europaparlamentet ska höras om rapporten.

Efter det att funktionen har börjat tillämpas vid reguljära gränsövergångsställen ska kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 75 för att komplettera denna förordning med avseende på fastställande av andra omständigheter under vilka fotografier och ansiktsbilder får användas för identifiering av personer.

#### KAPITEL XIII

### Åtkomsträtt och översyn av registreringar

#### Artikel 44

#### Nationella behöriga myndigheter med åtkomsträtt till uppgifter i SIS

1. Nationella behöriga myndigheter ska ha åtkomst till uppgifter som förts in i SIS och rätt att söka i sådana uppgifter direkt eller i en kopia av uppgifter i SIS-databasen för följande syften:

- a) Gränskontroller, i enlighet med förordning (EU) 2016/399.
- b) Polisens och tullens kontroller inom den berörda medlemsstaten och de utsedda myndigheternas samordning av sådana kontroller.
- c) Förebyggande, förhindrande, avslöjande, utredning eller lagföring av terroristbrott eller andra grova brott eller verkställande av straffrättsliga påföljder, i den berörda medlemsstaten, förutsatt att direktiv (EU) 2016/680 är tillämpligt.
- d) Granskning av villkoren och beslutsfattande i samband med tredjelandsmedborgares inresa till och vistelse på medlemsstaternas territorium, även när det gäller uppehållstillstånd och viseringar för längre vistelse, och i samband med återvändande av tredjelandsmedborgare samt utförandet av kontroller av tredjelandsmedborgare som olagligen reser in till eller vistas på medlemsstaternas territorium.
- e) Säkerhetskontroller av tredjelandsmedborgare som ansöker om internationellt skydd, om de myndigheter som utför kontrollerna inte utgör *beslutande myndigheter* enligt definitionen i artikel 2 f i Europaparlamentets och rådets direktiv 2013/32/EU <sup>(1)</sup>, och, i tillämpliga fall, tillhandahållande av rådgivning i enlighet med rådets förordning (EG) nr 377/2004 <sup>(2)</sup>.

2. Åtkomsträtten till uppgifter i SIS och rätten att söka i sådana uppgifter direkt får – vid handläggning av en ansökan om naturalisation – utövas av nationella behöriga myndigheter som är ansvariga för naturalisation, i enlighet med nationell rätt.

3. Åtkomsträtten till uppgifter som har förts in i SIS och rätten att söka i sådana uppgifter direkt får också utövas av nationella rättsliga myndigheter, inbegripet de myndigheter som är ansvariga för att väcka allmänt åtal inom ramen för ett brottmålsförfarande och för rättsliga utredningar som föregår åtal mot en person, när de utför sina uppgifter i enlighet med nationell rätt, samt av deras samordningsmyndigheter.

4. De behöriga myndigheter som avses i denna artikel ska tas med i den förteckning som avses i artikel 56.7.

#### Artikel 45

#### Fordonsregistreringsenheter

1. De enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon, vilka avses i rådets direktiv 1999/37/EG <sup>(3)</sup>, ska ha åtkomst till uppgifter som förts in i SIS i enlighet med artikel 38.2 a, b, c, m och p i denna förordning endast för att kontrollera om de fordon och åtföljande registreringsbevis samt nummerplåtar som anmäls för registrering är stulna, bortförda, försvunna, ger intryck av att vara sådana handlingar men är falska eller eftersöks som bevis i brottmål.

Åtkomst till de uppgifter för de enheter som avses i första stycket ska regleras av nationell rätt och ska begränsas till de berörda enheternas specifika behörighet.

2. Om de enheter som avses i punkt 1 är statliga enheter ska de ha direkt åtkomsträtt till uppgifterna i SIS.

<sup>(1)</sup> Europaparlamentets och rådets direktiv 2013/32/EU av den 26 juni 2013 om gemensamma förfaranden för att bevilja och återkalla internationellt skydd (EUT L 180, 29.6.2013, s. 60).

<sup>(2)</sup> Rådets förordning (EG) nr 377/2004 av den 19 februari 2004 om inrättande av ett nätverk av sambandsmän för invandring (EUT L 64, 2.3.2004, s. 1).

<sup>(3)</sup> Rådets direktiv 1999/37/EG av den 29 april 1999 om registreringsbevis för fordon (EGT L 138, 1.6.1999, s. 57).

3. Om de enheter som avses i punkt 1 i den här artikeln inte är statliga enheter ska de endast ha indirekt åtkomst till uppgifter i SIS genom en myndighet som avses i artikel 44. Den myndigheten ska ha direkt åtkomsträtt till uppgifterna och rätt att vidarebefordra dem till den berörda enheten. Den berörda medlemsstaten ska säkerställa att den berörda enheten och dess anställda är förpliktade att iakttä alla begränsningar av användningen av de uppgifter som förmedlats av myndigheten.

4. Artikel 39 ska inte vara tillämplig på åtkomst till SIS av det slag som avses i den här artikeln. All förmedling från de enheter som avses i punkt 1 i den här artikeln till polis eller andra rättsliga myndigheter av uppgifter som erhållits genom åtkomst till SIS ska regleras i nationell rätt.

#### Artikel 46

### Registreringsenheter för fartyg och luftfartyg

1. De enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis eller säkerställa trafikledning för fartyg, även fartygsmotorer, och luftfartyg, även flygmotorer, ska ha åtkomst till följande uppgifter som förts in i SIS i enlighet med artikel 38.2 endast för att kontrollera om fartyg, även fartygsmotorer, och luftfartyg, även flygmotorer, som anmäls för registrering eller görs till föremål för trafikledning är stulna, bortförda, försvunna eller eftersöks som bevis i brottmål:

- a) Uppgifter om fartyg.
- b) Uppgifter om fartygsmotorer.
- c) Uppgifter om luftfartyg.
- d) Uppgifter om flygmotorer.

Åtkomst till de uppgifter för de enheter som avses i första stycket ska regleras av nationell rätt och ska begränsas till de berörda enheternas specifika behörighet.

2. Om de enheter som avses i punkt 1 är statliga enheter ska de ha direkt åtkomsträtt till uppgifterna i SIS.

3. Om de enheter som avses i punkt 1 i den här artikeln inte är statliga enheter ska de endast ha indirekt åtkomst till uppgifter i SIS genom en myndighet som avses i artikel 44. Den myndigheten ska ha direkt åtkomsträtt till uppgifterna och rätt att vidarebefordra dem till den berörda enheten. Den berörda medlemsstaten ska säkerställa att den berörda enheten och dess anställda är förpliktade att iakttä alla begränsningar av användningen av de uppgifter som förmedlats till dem av myndigheten.

4. Artikel 39 ska inte vara tillämplig på åtkomst till SIS av det slag som avses i den här artikeln. All förmedling från de enheter som avses i punkt 1 i den här artikeln till polis eller andra rättsliga myndigheter av uppgifter som erhållits genom åtkomst till SIS ska regleras i nationell rätt.

#### Artikel 47

### Registreringsmyndigheter för skjutvapen

1. De enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för skjutvapen ska ha åtkomst till registreringar om personer som förts in i SIS i enlighet med artiklarna 26 och 36 och till registreringar om skjutvapen som förts in i SIS i enlighet med artikel 38.2. Denna åtkomst ska utövas för att kontrollera om den person som ansöker om registrering är efterlyst för att gripas och överlämnas eller utlämnas eller för diskreta kontroller, undersökningskontroller eller särskilda kontroller eller om de skjutvapen som anmäls för registrering eftersöks för att beslagtas eller användas som bevis i brottmål.

2. Åtkomst till de uppgifter för de enheter som avses i punkt 1 ska regleras av nationell rätt och ska begränsas till de berörda enheternas specifika behörighet.

3. Om de enheter som avses i punkt 1 är statliga enheter ska de ha direkt åtkomsträtt till uppgifterna i SIS.

4. Om de enheter som avses i punkt 1 inte är statliga enheter ska de endast ha indirekt åtkomst till uppgifter i SIS genom en myndighet som avses i artikel 44. Den myndigheten ska ha direkt åtkomsträtt till uppgifterna och ska informera den berörda enheten om huruvida skjutvapnet kan registreras. Den berörda medlemsstaten ska säkerställa att den berörda enheten och dess anställda är förpliktade att iakttä alla begränsningar av användningen av de uppgifter som förmedlats till dem av den förmedlande myndigheten.

5. Artikel 39 är inte tillämplig på åtkomst till SIS som ges i enlighet med den här artikeln. All förmedling från de enheter som avses i punkt 1 i den här artikeln till polis eller andra rättsliga myndigheter av uppgifter som erhållits igenom åtkomst till SIS ska regleras i nationell rätt.

## Artikel 48

**Europols åtkomst till uppgifter i SIS**

1. Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol), inrättad genom förordning (EU) 2016/794, ska, där så krävs för att Europol ska fullgöra sitt uppdrag, ha rätt att få åtkomst till och söka i uppgifter i SIS. Europol får även utbyta och begära ytterligare tilläggsinformation i enlighet med bestämmelserna i Sirenehandboken.
2. Om en sökning som Europol utför visar att det finns en registrering i SIS ska Europol informera den registrerande medlemsstaten genom att utbyta tilläggsinformation via kommunikationsinfrastrukturen och i enlighet med bestämmelserna i Sirenehandboken. Fram till dess att Europol har möjlighet att använda funktionerna för utbyte av tilläggsinformation ska Europol informera de registrerande medlemsstaterna genom de kanaler som fastställs i förordning (EU) 2016/794.
3. Europol får behandla den tilläggsinformation som har erhållits från medlemsstater för att jämföra den med sina databaser och projekt för operativa analyser som syftar till att kartlägga kopplingar eller andra relevanta samband mellan uppgifter och för analyser av strategisk eller tematisk karaktär eller operativa analyser som avses i artikel 18.2 a, b och c i förordning (EU) 2016/794. All Europols behandling av tilläggsinformation vid tillämpning av denna artikel ska ske i överensstämmelse med den förordningen.
4. Europols användning av uppgifter från sökning i SIS eller från behandling av tilläggsinformation kräver tillstånd från den registrerande medlemsstaten. Om medlemsstaten tillåter användning av uppgifterna ska Europols behandling av dem regleras av förordning (EU) 2016/794. Europol får endast meddela sådana uppgifter till tredjeländer eller utomstående instanser med den registrerande medlemsstatens tillstånd och med fullständig efterlevnad av unionsrätten om dataskydd.
5. Europol,
  - a) får utan att det påverkar tillämpningen av punkterna 4 och 6, inte sammankoppla några delar av SIS med, eller överföra de uppgifter i SIS till vilka Europol har åtkomst till, något system för insamling och behandling av uppgifter drivet av eller vid Europol, eller ladda ned eller på annat sätt kopiera några delar av SIS,
  - b) ska, utan hinder av vad som sägs i artikel 31.1 i förordning (EU) 2016/794, radera tilläggsinformation som innehåller personuppgifter senast ett år efter det att motsvarande registrering raderats. Genom undantag får Europol, i de fall där Europol har information i sina databaser eller projekt för operativa analyser om ett ärende med koppling till tilläggsinformationen, för att kunna utföra sina arbetsuppgifter undantagsvis fortsätta att lagra tilläggsinformationen där så är nödvändigt. Europol ska informera den registrerande och den verkställande medlemsstaten om den fortsatta lagringen av sådan tilläggsinformation och lämna en motivering till detta,
  - c) ska begränsa åtkomsten till uppgifter i SIS, inklusive tilläggsinformation, till personal med särskild behörighet vid Europol som behöver åtkomst till sådana uppgifter för att kunna utföra sina uppgifter,
  - d) ska vidta och tillämpa åtgärder för att säkerställa säkerhet, konfidentialitet och egenkontroll i enlighet med artiklarna 10, 11 och 13,
  - e) ska säkerställa att dess personal som har behörighet att behandla uppgifter i SIS får lämplig utbildning och information i enlighet med artikel 14.1, och
  - f) ska, utan att det påverkar tillämpningen av förordning (EU) 2016/794, låta Europeiska datatillsynsmannen övervaka och se över hur Europol utövat rätten att få åtkomst till och söka i uppgifter i SIS samt hur utbytet och behandlingen av tilläggsinformation hanterats.
6. Europol får endast kopiera uppgifter från SIS för tekniska ändamål om sådan kopiering krävs för att vederbörligen bemyndigad personal vid Europol ska kunna göra direkta sökningar. Dessa kopior ska omfattas av denna förordning. Den tekniska kopian får endast användas för lagring av SIS-uppgifter medan man söker i uppgifterna. När sökningen i uppgifterna är slutförd ska de raderas. Sådan användning ska inte anses vara en olaglig nedladdning eller kopiering av SIS-uppgifter. Europol får inte kopiera registreringsuppgifter eller kompletterande uppgifter införda av medlemsstaterna eller uppgifter från CS-SIS till andra Europolsystem.
7. Europol ska i enlighet med bestämmelserna i artikel 12 föra loggar över all åtkomst till och sökning i SIS för att kontrollera om databehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa en lämplig nivå för datasäkerhet och dataintegritet. Sådana loggar och sådan dokumentation ska inte anses vara en olaglig nedladdning eller kopiering av någon del av SIS.
8. Medlemsstaterna ska informera Europol genom att utbyta tilläggsinformation om alla träffar på registreringar med anknytning till terroristbrott. Undantagsvis får medlemsstaterna avstå från att informera Europol om detta skulle äventyra pågående utredningar eller en enskild persons säkerhet, eller strida mot den registrerande medlemsstatens väsentliga säkerhetsintressen.
9. Punkt 8 ska tillämpas från och med den dag då Europol kan ta emot tilläggsinformation i enlighet med punkt 1.



## Artikel 49

**Eurojusts åtkomst till uppgifter i SIS**

1. Endast de nationella medlemmarna i Eurojust och deras assistenter ska, när så är nödvändigt för att de ska fullgöra sitt mandat, ha rätt att få åtkomst till och söka i uppgifter i SIS inom ramen för deras mandat i enlighet med artiklarna 26, 32, 34, 38 och 40.
2. Om en sökning som en nationell medlem i Eurojust utför visar att det finns en registrering i SIS, ska denna nationella medlem informera den registrerande medlemsstaten. Eurojust får endast vidarebefordra uppgifter som erhålls genom en sådan sökning till tredjeländer och utomstående instanser med den registrerande medlemsstatens tillstånd och med fullständig efterlevnad av unionsrätten om dataskydd.
3. Denna artikel ska inte påverka tillämpningen av bestämmelserna i Europaparlamentets och rådets förordning (EU) 2018/1727 <sup>(1)</sup> och förordning (EU) 2018/1725 beträffande dataskydd och skadeståndsansvar om nationella medlemmar i Eurojust eller deras assistenter behandlar uppgifter på ett otillåtet eller felaktigt sätt, eller Europeiska datatillsynsmannens befogenheter i enlighet med dessa förordningar.
4. Eurojust ska föra loggar i enlighet med bestämmelserna i artikel 12 över all åtkomst till och sökning i SIS som gjorts av en nationell medlem i Eurojust eller en assistent för att kontrollera om databehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa en lämplig nivå för datasäkerhet och dataintegritet.
5. Ingen del av SIS får sammankopplas till något annat system för insamling och behandling av uppgifter som drivs av eller vid Eurojust, inte heller får de uppgifter i SIS som de nationella medlemmarna eller deras biträdande medlemmar har åtkomst till överföras till ett sådant system. Ingen del av SIS får laddas ned eller kopieras. Loggning av åtkomst och sökningar ska inte anses vara en olaglig nedladdning eller kopiering av SIS-uppgifter.
6. Eurojust ska anta och tillämpa åtgärder för att säkerställa säkerhet, konfidentialitet och egenkontroll i enlighet med artiklarna 10, 11 och 13.

## Artikel 50

**Åtkomst till uppgifter i SIS för de europeiska gräns- och kustbevakningsenheterna, enheter med personal som arbetar med återvändande och medlemmarna i stödgrupperna för migrationshantering**

1. I enlighet med artikel 40.8 i förordning (EU) 2016/1624 ska medlemmarna i de enheter och grupper som avses i artikel 2.8 och 2.9 i den förordningen, inom ramen för sitt mandat och under förutsättning att de är behöriga att göra kontroller i enlighet med artikel 44.1 i den här förordningen och har fått den utbildning som krävs i enlighet med artikel 14.1 i den här förordningen, ha rätt att få åtkomst till och söka i uppgifter i SIS i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter och i den mån det krävs enligt den operativa planen för en särskild insats. Åtkomst till uppgifter i SIS får inte beviljas någon annan medlem i enheten eller gruppen.
2. Medlemmar i de enheter och grupper som avses i punkt 1 ska utöva denna rätt att få åtkomst till och söka i uppgifter i SIS i enlighet med punkt 1 genom ett tekniskt gränssnitt. Det tekniska gränssnittet ska inrättas och underhållas av Europeiska gräns- och kustbevakningsbyrån och ska möjliggöra direktkoppling till det centrala SIS.
3. Om en sökning som utförs av en medlem i de enheter och grupper som avses i punkt 1 i den här artikeln visar att det finns en registrering i SIS, ska den registrerande medlemsstaten informeras. I enlighet med artikel 40 i förordning (EU) 2016/1624 får medlemmarna i enheterna eller grupperna endast vidta åtgärder utifrån en registrering i SIS i enlighet med anvisningar från och, som en allmän regel, endast i närvaro av gränsbevakningstjänstemän eller personal som arbetar med återvändande i den värdmedlemsstat där de är verksamma. Värdmedlemsstaten får ge medlemmar i enheterna eller grupperna tillstånd att agera för dess räkning.
4. Europeiska gräns- och kustbevakningsbyrån ska föra loggar över varje åtkomst till och sökning i SIS i enlighet med bestämmelserna i artikel 12 för att kontrollera om databehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa en lämplig nivå för datasäkerhet och dataintegritet.
5. Europeiska gräns- och kustbevakningsbyrån ska anta och tillämpa åtgärder för att säkerställa säkerhet, konfidentialitet och egenkontroll i enlighet med artiklarna 10, 11 och 13, och säkerställa att de enheter och grupper som avses i punkt 1 i den här artikeln tillämpar dessa åtgärder.
6. Ingenting i denna artikel ska tolkas som att det påverkar bestämmelserna i förordning (EU) 2016/1624 beträffande dataskydd eller skadeståndsansvar för Europeiska gräns- och kustbevakningsbyrån om den behandlar uppgifter på ett otillåtet eller felaktigt sätt.

<sup>(1)</sup> Europaparlamentets och rådets förordning (EU) 2018/1727 av den 14 november 2018 om Europeiska unionens byrå för straffrättsligt samarbete (Eurojust), och om ersättning och upphävande av rådets beslut 2002/187/RIF (EUT L 295, 21.11.2018, s. 138).

7. Utan att det påverkar tillämpningen av punkt 2 får inga delar av SIS sammankopplas med något system för insamling och behandling av uppgifter som drivs av de enheter eller grupper som avses i punkt 1 eller av Europeiska gräns- och kustbevakningsbyrån; inte heller får de uppgifter i SIS som dessa enheter och grupper har åtkomst till överföras till ett sådant system. Ingen del av SIS får laddas ned eller kopieras. Loggning av åtkomst och sökningar ska inte anses vara en olaglig nedladdning eller kopiering av SIS-uppgifter.

8. Europeiska gräns- och kustbevakningsbyrån ska tillåta att Europeiska datatillsynsmannen övervakar och ser över den verksamhet som bedrivs av de enheter och grupper som avses i denna artikel när de utövar sin rätt till åtkomst och sökning i uppgifter i SIS. Detta påverkar inte tillämpningen av ytterligare bestämmelser i förordning (EU) 2018/1725.

#### Artikel 51

### Utvärdering av Europols, Eurojusts och Europeiska gräns- och kustbevakningsbyråns användning av SIS

1. Kommissionen ska minst vart femte år utvärdera driften och användningen av SIS av Europol, de nationella medlemmarna i Eurojust och deras assistenter samt de enheter och grupper som avses i artikel 50.1.
2. Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån ska säkerställa lämplig uppföljning av resultaten och rekommendationerna från utvärderingen.
3. En rapport om resultaten av utvärderingen och uppföljningen av denna ska översändas till Europaparlamentet och rådet.

#### Artikel 52

### Åtkomstens omfattning

Slutanvändarna, däribland Europol, de nationella medlemmarna i Eurojust och deras assistenter samt medlemmarna i de enheter och grupper som avses i artikel 2.8 och 2.9 i förordning (EU) 2016/1624, får endast ha åtkomst till de uppgifter som de behöver för att de ska kunna fullgöra sina uppgifter.

#### Artikel 53

### Tidsfrist för översyn av registreringar om personer

1. Registreringar får inte lagras längre än vad som är nödvändigt för att uppnå de syften för vilka de fördes in.
2. En medlemsstat får föra in en registrering om en person för de syften som avses i artiklarna 26 och 32.1 a och b för en period på fem år. Den registrerande medlemsstaten ska se över behovet av att behålla registreringen inom denna femårsperiod.
3. En medlemsstat får föra in en registrering om en person för de syften som avses i artiklarna 34 och 40 för en period på tre år. Den registrerande medlemsstaten ska se över behovet av att behålla registreringen inom denna treårsperiod.
4. En medlemsstat får föra in en registrering om en person för de syften som avses i artiklarna 32.1 c, d och e och 36 för en period på ett år. Den registrerande medlemsstaten ska se över behovet av att behålla registreringen inom denna ettårsperiod.
5. Där så är lämpligt ska varje medlemsstat bestämma kortare tidsfrister för denna översyn i enlighet med sin nationella rätt.
6. Den registrerande medlemsstaten får inom den tidsfrist för översyn som avses i punkterna 2, 3 och 4 efter en noggrann individuell bedömning, som ska dokumenteras, besluta att registreringen om personen ska behållas längre än tidsfristen för översyn, om detta visar sig nödvändigt för och står i proportion till de syften för vilka den förts in. I ett sådant fall ska punkt 2, 3 eller 4 även vara tillämplig på förlängningen. Varje sådan förlängning ska meddelas CS-SIS.
7. Registreringar om personer ska raderas automatiskt när den tidsfrist för översyn som avses i punkterna 2, 3 och 4 har löpt ut, utom i fall där den registrerande medlemsstaten har informerat CS-SIS om en förlängning i enlighet med punkt 6. CS-SIS ska fyra månader i förväg automatiskt informera medlemsstaterna om planerad radering av uppgifter.
8. Medlemsstaterna ska föra statistik över antalet registreringar om personer vars lagringstid har förlängts i enlighet med punkt 6 i den här artikeln och på begäran översända dem till de tillsynsmyndigheter som avses i artikel 69.

9. Så snart det står klart för ett Sirenekontor att en registrering om en person har uppnått sitt syfte och därför bör raderas, ska det omedelbart underrätta den myndighet som skapade registreringen. Myndigheten ska inom femton kalenderdagar från det att den mottagit detta meddelande svara att registreringen har raderats eller ska raderas, eller ange skäl för att behålla registreringen. Om inget svar har erhållits när femtondagarsperioden har löpt ut ska Sirenekontoret säkerställa att registreringen raderas. I de fall där detta är tillåtligt enligt nationell rätt ska Sirenekontoret radera registreringen. Sirenekontoren ska rapportera eventuella återkommande problem de stöter på när de agerar i enlighet med denna punkt till sin tillsynsmyndighet.

#### Artikel 54

### Tidsfrist för översyn av registreringar om föremål

1. Registreringar om föremål får inte lagras längre än vad som är nödvändigt för att uppnå de syften för vilka de fördes in.
2. En medlemsstat får föra in en registrering om ett föremål för de syften som avses i artiklarna 36 och 38 för en period på tio år. Den registrerande medlemsstaten ska se över behovet av att behålla registreringen inom tioårsperioden.
3. Registreringar om föremål som förts in i enlighet med artiklarna 26, 32, 34 och 36 ska, när de är länkade till en registrering om en person, ses över i enlighet med artikel 53. Sådana registreringar får bevaras endast så länge som registreringen om personen bevaras.
4. Den registrerande medlemsstaten får inom den tidsfrist för översyn som avses i punkterna 2 och 3 besluta att registreringen om föremålet ska behållas längre än tidsfristen för översyn om detta visar sig nödvändigt för de syften för vilka den förts in. I ett sådant fall ska punkt 2 eller 3, beroende på vad som är lämpligt, vara tillämplig.
5. Kommissionen får anta genomförandeakter för att fastställa kortare tidsfrister för översyn för vissa kategorier av registreringar om föremål. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.
6. Medlemsstaterna ska föra statistik över antalet registreringar om föremål vars lagringstid har förlängts i enlighet med punkt 4.

#### KAPITEL XIV

### Radering av registreringar

#### Artikel 55

### Radering av registreringar

1. Registreringar om gripande för överlämnande eller utlämning enligt artikel 26 ska raderas när personen har överlämnats eller utlämnats till de behöriga myndigheterna i den registrerande medlemsstaten. De ska också raderas när det rättsliga avgörande som registreringen grundades på har återkallats av den behöriga rättsliga myndigheten i enlighet med nationell rätt. De ska även raderas då tidsfristen för registreringen löper ut i enlighet med artikel 53.
2. Registreringar om försvunna personer eller sårbara personer som behöver hindras från att resa enligt artikel 32 ska raderas enligt följande regler:
  - a) När det gäller försvunna barn och barn som löper risk att bortföras ska en registrering raderas när
    - i) ärendet är avslutat, till exempel om barnet har lokaliserats eller återbördats eller de behöriga myndigheterna i den verkställande medlemsstaten har fattat beslut om vårdnaden av barnet,
    - ii) lagringstiden för registreringen har löpt ut i enlighet med artikel 53, eller
    - iii) en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.
  - b) När det gäller försvunna vuxna då inga skyddsåtgärder har begärts ska en registrering raderas när
    - i) den berörda åtgärden har genomförts, om den verkställande medlemsstaten har fastställt var de befinner sig,
    - ii) lagringstiden för registreringen har löpt ut i enlighet med artikel 53, eller
    - iii) en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.
  - c) När det gäller försvunna vuxna då skyddsåtgärder har begärts ska en registrering raderas när
    - i) den berörda åtgärden har genomförts, om personen har ställts under beskydd,

- ii) lagringstiden för registreringen har löpt ut i enlighet med artikel 53, eller
  - iii) en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.
- d) När det gäller sårbara myndiga personer som för sin egen säkerhet behöver hindras från att resa och barn som behöver hindras från att resa ska en registrering raderas när
- i) den berörda åtgärden har genomförts, såsom att personen har ställts under beskydd,
  - ii) lagringstiden för registreringen har löpt ut i enlighet med artikel 53, eller
  - iii) en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.

Om en person har placerats på institution till följd av ett beslut av en behörig myndighet får en registrering behållas till dess att personen har återvänt, utan att det påverkar tillämpningen av nationell rätt.

3. Registreringar om personer som söks för ett rättsligt förfarande enligt artikel 34 ska raderas när
- a) den behöriga myndigheten i den registrerande medlemsstaten har fått besked om var personen befinner sig,
  - b) lagringstiden för registreringen har löpt ut i enlighet med artikel 53, eller
  - c) en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.

Om åtgärder inte kan vidtas avseende den vidarebefordrade information som avses i led a ska Sirenekontoret i den registrerande medlemsstaten informera Sirenekontoret i den verkställande medlemsstaten i syfte att lösa problemet.

Vid händelse av en träff när adressuppgifterna har överlämnats till den registrerande medlemsstaten, och en senare träff i den verkställande medlemsstaten ger samma adressuppgifter, ska träffen dokumenteras i den verkställande medlemsstaten men varken adressuppgifterna eller tilläggsinformationen ska återsändas till den registrerande medlemsstaten. I dessa fall ska den verkställande medlemsstaten upplysa den registrerande medlemsstaten om att flera träffar uppkommit och den registrerande medlemsstaten ska utföra en noggrann individuell bedömning av behovet av att behålla registreringen.

4. Registreringar om diskreta kontroller, undersökningskontroller och särskilda kontroller enligt artikel 36 ska raderas när

- a) lagringstiden för registreringen har löpt ut i enlighet med artikel 53, eller
- b) en behörig myndighet i den registrerande medlemsstaten har fattat beslut om radering av dem.

5. Radering av registreringar om föremål som ska beslagtas eller användas som bevis i brottmål enligt artikel 38 ska raderas när

- a) föremålet har beslagtogs eller motsvarande åtgärder har vidtagits och det därav följande nödvändiga utbytet av tilläggsinformation har skett mellan de berörda Sirenekontoren eller föremålet omfattas av ett annat rättsligt eller administrativt förfarande,
- b) lagringstiden för registreringen i enlighet med artikel 53 har löpt ut, eller
- c) en behörig myndighet i den registrerande medlemsstaten har fattat beslut om radering av dem.

6. Registreringar om okända efterlysta personer enligt artikel 40 ska raderas när

- a) personen har identifierats,
- b) lagringstiden för registreringen i enlighet med artikel 53 har löpt ut, eller
- c) en behörig myndighet i den registrerande medlemsstaten har fattat beslut om radering av dem.

7. När den är länkad till en registrering om en person, ska en registrering om ett föremål som förts in i enlighet med artiklarna 26, 32, 34 och 36 raderas när registreringen om personen raderas i enlighet med den här artikeln.

#### KAPITEL XV

### **Allmänna bestämmelser om databehandling**

#### Artikel 56

#### **Behandling av SIS-uppgifter**

1. Medlemsstaterna får endast behandla de uppgifter som avses i artikel 20 för de syften som anges för respektive registreringskategori i artiklarna 26, 32, 34, 36, 38 och 40.
2. Uppgifterna får endast kopieras för tekniska ändamål om sådan kopiering krävs för att de behöriga myndigheter som avses i artikel 44 ska kunna göra direkta sökningar. Denna förordning ska tillämpas på dessa kopior. En medlemsstat får inte kopiera registreringsuppgifter eller kompletterande uppgifter som förts in av en annan medlemsstat från dess N.SIS eller från CS-SIS till andra nationella dataregister.

3. Sådana tekniska kopior som avses i punkt 2 och som leder till offlinedatabaser får lagras i högst 48 timmar.

Medlemsstaterna ska föra ett uppdaterat register över dessa kopior, göra detta register tillgängligt för sina tillsynsmyndigheter och säkerställa att denna förordning, särskilt artikel 10, tillämpas på dessa kopior.

4. De nationella behöriga myndigheter som avses i artikel 44 ska ha åtkomst till uppgifter i SIS endast inom ramen för sin behörighet, och då endast för vederbörligen bemyndigad personal.

5. När det gäller de registreringar som avses i artiklarna 26, 32, 34, 36, 38 och 40 i denna förordning, ska all behandling av uppgifter i SIS för andra syften än de för vilka uppgifterna fördes in i SIS ha koppling till ett specifikt ärende och motiveras av behovet av att avvärja en överhängande och allvarlig fara för den allmänna ordningen och säkerheten, en betydande risk för den nationella säkerheten eller ett grovt brott. Förhandstillstånd från den registrerande medlemsstaten krävs för detta ändamål.

6. All användning av SIS-uppgifter som inte är förenlig med punkterna 1–5 i den här artikeln ska betraktas som missbruk enligt varje medlemsstats nationella rätt och leda till sanktioner i enlighet med artikel 73.

7. Varje medlemsstat ska till eu-LISA sända in en förteckning över sina behöriga myndigheter som är behöriga att direkt söka i uppgifter i SIS i enlighet med denna förordning, samt alla ändringar i förteckningen. I förteckningen ska för varje myndighet anges vilka uppgifter den får söka i och för vilka syften. eu-LISA ska säkerställa att förteckningen offentliggörs årligen i *Europeiska unionens officiella tidning*. eu-LISA ska på sin webbplats upprätthålla en kontinuerligt uppdaterad förteckning över de ändringar som sänts in av medlemsstaterna mellan de årliga offentliggörandena.

8. Om inga särskilda bestämmelser föreskrivs i unionsrätten ska varje medlemsstats nationella rätt gälla för uppgifter i dess N.SIS.

#### Artikel 57

### SIS-uppgifter och nationella system

1. Artikel 56.2 ska inte påverka tillämpningen av en medlemsstats rätt att i sina nationella system lagra SIS-uppgifter i samband med vilka åtgärder har vidtagits inom dess territorium. Dessa uppgifter får lagras högst tre år i de nationella systemen, om inte särskilda bestämmelser i nationell rätt tillåter att uppgifterna lagras under en längre period.

2. Artikel 56.2 ska inte påverka en medlemsstats rätt att i sina nationella system lagra uppgifterna i en registrering som den medlemsstaten har fört in.

#### Artikel 58

### Information om att en registrering inte verkställs

Om en begärd åtgärd inte kan vidtas ska den medlemsstat som har anmodats att vidta en åtgärd omedelbart informera den registrerande medlemsstaten genom att utbyta tilläggsinformation.

#### Artikel 59

### Kvaliteten på uppgifterna i SIS

1. En registrerande medlemsstat ska ansvara för att säkerställa att uppgifterna i SIS är korrekta och aktuella och att de förs in i och lagras i SIS på lagligt sätt.

2. Om en registrerande medlemsstat mottar relevanta kompletterande eller ändrade uppgifter av det slag som anges i artikel 20.3, ska den utan dröjsmål komplettera eller ändra registreringen.

3. Endast den registrerande medlemsstaten ska ha behörighet att ändra, komplettera, rätta, uppdatera eller radera de uppgifter som den har fört in i SIS.

4. Om en annan medlemsstat än den registrerande medlemsstaten har relevanta kompletterande eller ändrade uppgifter av det slag som anges i artikel 20.3, ska den utan dröjsmål, genom utbyte av tilläggsinformation, överföra dem till den registrerande medlemsstaten så att denna kan komplettera eller ändra registreringen. Om de kompletterande eller ändrade uppgifterna avser en person får de överföras endast om personens identitet har fastställts.

5. Om en annan medlemsstat än den registrerande medlemsstaten har bevis för att en uppgift kan vara felaktig i sak eller har lagrats olagligt ska den genom utbyte av tilläggsinformation informera den registrerande medlemsstaten om detta så snart som möjligt, dock senast två arbetsdagar efter det att den fått kännedom om dessa bevis. Den registrerande medlemsstaten ska kontrollera informationen och, vid behov, utan dröjsmål rätta eller radera uppgiften i fråga.

6. Om medlemsstaterna inte kan nå en uppgörelse inom två månader efter det att man fick kännedom om bevisen, i enlighet med vad som anges i punkt 5 i den här artikeln, ska den medlemsstat som inte förde in registreringen överlämna ärendet till de berörda tillsynsmyndigheterna och till Europeiska datatillsynsmannen för beslut, genom samarbete i enlighet med artikel 71.

7. Medlemsstaterna ska utbyta tilläggsinformation i de fall en person säger sig inte vara det avsedda föremålet för en registrering. Om det vid kontroll visar sig att det avsedda föremålet för en registrering inte är klaganden, ska klaganden underrättas om de åtgärder som föreskrivs i artikel 62 och om rätten till tillgång till prövning i enlighet med artikel 68.1.

#### Artikel 60

##### Säkerhetstillbud

1. Varje händelse som har eller kan få inverkan på säkerheten i SIS eller som kan orsaka skada på eller förlust av SIS-uppgifter eller tilläggsinformation ska betraktas som ett säkerhetstillbud, särskilt om systemet kan ha utsatts för dataintrång eller om uppgifternas tillgänglighet, integritet och konfidentialiteten har äventyrats eller kan ha äventyrats.

2. Säkerhetstillbud ska hanteras på ett sätt som säkerställer snabba, effektiva och välavvägda motåtgärder.

3. Utan att det påverkar anmälan av och informationen om en personuppgiftsincident enligt artikel 33 i förordning (EU) 2016/679 eller artikel 30 i direktiv (EU) 2016/680, ska medlemsstaterna, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån utan dröjsmål underrätta kommissionen, eu-LISA, den behöriga tillsynsmyndigheten och Europeiska datatillsynsmannen om säkerhetstillbud. eu-LISA ska utan dröjsmål underrätta kommissionen och Europeiska datatillsynsmannen om alla säkerhetstillbud som rör centrala SIS.

4. Information om ett säkerhetstillbud som har eller kan ha påverkat driften av SIS i en medlemsstat eller inom eu-LISA, tillgängligheten, integriteten och konfidentialiteten hos de uppgifter som förts in eller sänts av andra medlemsstater eller tilläggsinformation som utbyts, ska utan dröjsmål ges till samtliga medlemsstater och rapporteras i enlighet med den tillbudshanteringsplan som eu-LISA tillhandahåller.

5. Medlemsstaterna och eu-LISA ska samarbeta om ett säkerhetstillbud inträffar.

6. Kommissionen ska omedelbart rapportera allvarliga tillbud till Europaparlamentet och rådet. Dessa rapporter ska ges säkerhetsskyddsklassificeringen EU RESTRICTED/RESTREINT UE i enlighet med tillämpliga säkerhetsbestämmelser.

7. Om ett säkerhetstillbud orsakas av missbruk av uppgifter ska medlemsstaterna, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån säkerställa att sanktioner påförs i enlighet med artikel 73.

#### Artikel 61

##### Särskiljande av personer med snarlika kännetecken

1. Om det, när en ny registrering förs in, framkommer att det i SIS redan finns en registrering om en person med samma identitetsuppgifter ska Sirenekontoret kontakta den registrerande medlemsstaten genom utbyte av tilläggsinformation inom 12 timmar för att dubbelkontrollera om föremålet för de två registreringarna är samma person.

2. Om dubbelkontrollen visar att den som är föremål för den nya registreringen och den person som är föremål för en registrering som redan har förts in i SIS faktiskt är samma person ska Sirenekontoret tillämpa det förfarande för införande av flera registreringar som anges i artikel 23.

3. Om dubbelkontrollen visar att det rör sig om två olika personer ska Sirenekontoret godkänna begäran om att föra in den andra registreringen genom att lägga till sådana uppgifter som krävs för att undvika felidentifiering.

#### Artikel 62

##### Kompletterande uppgifter för att komma till rätta med missbruk av identitet

1. Om den person som faktiskt är avsedd som föremål för en registrering kan förväxlas med en person vars identitet har missbrukats ska den registrerande medlemsstaten, om den person vars identitet har missbrukats har gett sitt uttryckliga samtycke, lägga till uppgifter om denna i registreringen för att undvika de negativa följder som en felidentifiering kan medföra. Var och en vars identitet har missbrukats ska ha rätt att återkalla sitt samtycke avseende behandlingen av de personuppgifter som har lagts till.

2. Uppgifter om en person vars identitet har missbrukats får användas endast i följande syften:
  - a) För att göra det möjligt för den behöriga myndigheten att skilja mellan den person vars identitet har missbrukats och den person som är avsedd att vara föremålet för registreringen.
  - b) För att göra det möjligt för den person vars identitet har missbrukats att styrka sin identitet och fastställa att hans eller hennes identitet har missbrukats.
3. Vid tillämpning av denna artikel, och om den person vars identitet har missbrukats för varje uppgiftskategori har gett sitt uttryckliga samtycke, får enbart följande personuppgifter avseende den person vars identitet har missbrukats föras in och vidarebehandlas i SIS:
  - a) Efternamn.
  - b) Förnamn.
  - c) Namn vid födelsen.
  - d) Tidigare använda namn och eventuella separat införda alias.
  - e) Särskilda, objektiva, fysiska kännetecken som inte förändras.
  - f) Födelseort.
  - g) Födelsedatum.
  - h) Kön.
  - i) Fotografier och ansiktsbilder.
  - j) Fingeravtryck, handavtryck eller båda.
  - k) Samtliga medborgarskap.
  - l) Identifieringshandlingarnas kategori.
  - m) Land som utfärdat identifieringshandlingarna.
  - n) Identifieringshandlingarnas nummer.
  - o) Identifieringshandlingarnas utfärdandedatum.
  - p) Personens adress.
  - q) Personens fars namn.
  - r) Personens mors namn.
4. Kommissionen ska anta genomförandeakter för att fastställa och utveckla tekniska regler som är nödvändiga för att föra in och vidarebehandla de uppgifter som avses i punkt 3 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.
5. De uppgifter som avses i punkt 3 ska raderas samtidigt med motsvarande registrering eller innan dess på begäran av den berörda personen.
6. Endast de myndigheter som har åtkomsträtt till motsvarande registrering får ha åtkomst till de uppgifter som avses i punkt 3. Detta får ske endast för att undvika felidentifiering.

#### Artikel 63

#### Länkning mellan registreringar

1. En medlemsstat får skapa en länk mellan registreringar den för in i SIS. En sådan länk ska upprätta en förbindelse mellan två eller flera registreringar.
2. Skapandet av en länk ska inte påverka vare sig de särskilda åtgärder som ska vidtas på grundval av var och en av de länkade registreringarna eller tidsfristen för översyn av någon av de länkade registreringarna.
3. Skapandet av en länk ska inte påverka de åtkomsträttigheter som föreskrivs i denna förordning. Myndigheter som inte har åtkomsträtt till vissa registreringskategorier får inte kunna se länkar till registreringar som de inte har åtkomst till.
4. En medlemsstat ska skapa en länk mellan registreringar om det föreligger ett operativt behov.
5. Om en medlemsstat anser att en länk som en annan medlemsstat skapat mellan registreringar är oförenlig med dess nationella rätt eller dess internationella åtaganden, får den vidta nödvändiga åtgärder för att säkerställa att det inte går att få åtkomst till länken från dess territorium och att de egna myndigheterna utanför landets territorium inte kan få åtkomst till länken.

6. Kommissionen ska anta genomförandeakter för att fastställa och utveckla tekniska regler för länkning av registreringar. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 64

### Tilläggsinformationens syften och lagringstid

1. Medlemsstaterna ska på Sirenekontoret bevara en hänvisning till de beslut som ger upphov till en registrering, för att stödja utbytet av tilläggsinformation.
2. Personuppgifter som Sirenekontoret innehar till följd av informationsutbyte ska lagras endast under så lång tid som kan behövas för att uppnå de syften för vilka de tillhandahålls. De ska under alla omständigheter raderas senast ett år efter det att motsvarande registrering har raderats i SIS.
3. Punkt 2 ska inte påverka en medlemsstats rätt att i sina nationella system lagra uppgifter om en registrering som den medlemsstaten har fört in, eller om en registrering i samband med vilken en åtgärd har vidtagits på dess territorium. Hur länge sådana uppgifter får lagras i dessa system ska regleras i nationell rätt.

#### Artikel 65

### Överföring av personuppgifter till tredje man

Uppgifter som behandlats i SIS och motsvarande tilläggsinformation som utbyts i enlighet med denna förordning får inte överföras till eller göras tillgängliga för tredjeländer eller för internationella organisationer.

#### KAPITEL XVI

### Dataskydd

#### Artikel 66

### Tillämplig lagstiftning

1. Förordning (EU) 2018/1725 ska vara tillämplig på eu-LISA:s, Europeiska gräns- och kustbevakningsbyråns och Eurojusts behandling av personuppgifter inom ramen för den här förordningen. Förordning (EU) nr 2016/794 ska vara tillämplig på Europols behandling av personuppgifter inom ramen för denna förordning.
2. Direktiv (EU) 2016/680 ska vara tillämpligt när de nationella behöriga myndigheterna och enheterna behandlar personuppgifter enligt den här förordningen för att förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot och förebygga hot mot den allmänna säkerheten.
3. Förordning (EU) 2016/679 ska vara tillämplig när de nationella behöriga myndigheterna och enheterna behandlar personuppgifter enligt den här förordningen, med undantag för behandling för att förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot och förebygga hot mot den allmänna säkerheten.

#### Artikel 67

### Rätt till åtkomst, rättelse av oriktiga uppgifter och radering av olagligt lagrade uppgifter

1. De registrerade ska kunna utöva de rättigheter som fastställs i artiklarna 15, 16 och 17 i förordning (EU) 2016/679 samt artiklarna 14, 16.1 och 16.2 i direktiv (EU) 2016/680.
2. En annan medlemsstat än den registrerande medlemsstaten får till den registrerade lämna ut information om de av den registrerades personuppgifter som behandlas endast om den i förväg har gett den registrerande medlemsstaten tillfälle att meddela sin ståndpunkt. Kommunikationen mellan dessa medlemsstater ska ske genom utbytet av tilläggsinformation.
3. En medlemsstat ska besluta att endast delvis eller inte alls lämna ut information till den registrerade, i enlighet med nationell rätt, i den mån och så länge som en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med vederbörlig hänsyn till den berörda registrerades grundläggande rättigheter och berättigade intressen, för att
  - a) inte försvåra officiella eller rättsliga utredningar, undersökningar eller förfaranden,
  - b) undvika menlig inverkan på förebyggande, förhindrande, avslöjande, utredning eller lagföring av brott eller på verkställighet av straffrättsliga påföljder,



- c) skydda den allmänna säkerheten,
- d) skydda den nationella säkerheten, eller
- e) skydda andra personers rättigheter och friheter.

Medlemsstaten ska, i de fall som avses i första stycket utan onödigt dröjsmål skriftligen informera den registrerade om varje vägran eller begränsning av åtkomsten och om skälen för vägran eller begränsningen. Denna information får utelämnas om tillhandahållandet av den skulle undergräva något av skälen i första stycket a–e. Medlemsstaten ska informera den registrerade om möjligheten att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

Medlemsstaten ska dokumentera de sakliga eller rättsliga grunderna för beslutet att inte lämna ut informationen till den registrerade. Denna information ska göras tillgänglig för tillsynsmyndigheterna.

I sådana fall ska den registrerade även kunna utöva sina rättigheter genom de behöriga tillsynsmyndigheterna.

4. Efter en ansökan om åtkomst, rättelse eller radering ska medlemsstaten informera den registrerade så snart som möjligt och i alla händelser inom de tidsfrister som avses i artikel 12.3 i förordning (EU) 2016/679 om vilka åtgärder som vidtas till följd av utövandet av rättigheterna enligt den här artikeln.

#### Artikel 68

#### Rättsmedel

1. Utan att det påverkar tillämpningen av bestämmelserna om rättsmedel i förordning (EU) 2016/679 och i direktiv (EU) 2016/680 ska var och en kunna få sin sak prövad av en behörig myndighet, inbegripet en domstol, enligt varje medlemsstats nationella rätt, för att få åtkomst till, rätta, radera eller erhålla information eller erhålla ersättning i samband med en registrering som rör dem.
2. Utan att det påverkar tillämpningen av artikel 72 förbinder sig medlemsstaterna ömsesidigt att verkställa slutliga avgöranden som har meddelats av sådana domstolar eller myndigheter som avses i punkt 1 i den här artikeln.
3. Medlemsstaterna ska årligen rapportera till Europeiska dataskyddsstyrelsen om
  - a) hur många gånger det har begärts åtkomst hos personuppgiftsansvariga och i hur många ärenden åtkomst till uppgifterna beviljats,
  - b) hur många gånger det har begärts åtkomst hos tillsynsmyndigheten och i hur många ärenden åtkomst till uppgifterna beviljats,
  - c) hur många gånger rättelse av oriktiga uppgifter och radering av olagligt lagrade uppgifter begärts hos personuppgiftsansvariga och i hur många ärenden uppgifterna rättats eller raderats,
  - d) hur många gånger rättelse av oriktiga uppgifter eller radering av olagligt lagrade uppgifter begärts hos tillsynsmyndigheten,
  - e) hur många domstolsförfaranden som inletts,
  - f) hur många ärenden som lett till att domstolen gett den klagande rätt,
  - g) eventuella anmärkningar avseende fall av ömsesidigt erkännande av slutliga avgöranden som har meddelats av andra medlemsstaters domstolar eller myndigheter om registreringar som förts in av den registrerande medlemsstaten.

Kommissionen ska utarbeta en mall för den rapportering som avses i denna punkt.

4. Medlemsstaternas rapporter ska ingå i den gemensamma rapport som avses i artikel 71.4.

#### Artikel 69

#### Tillsyn över N.SIS

1. Medlemsstaterna ska säkerställa att de oberoende tillsynsmyndigheter som utses i varje medlemsstat, med de befogenheter som avses i kapitel VI i förordning (EU) 2016/679 eller kapitel VI i direktiv (EU) 2016/680, övervakar lagenligheten i behandlingen av personuppgifter i SIS inom deras territorium, i överföringen av uppgifterna från deras territorium och i utbytet och vidarebehandlingen av tilläggsinformation inom deras territorium.
2. Tillsynsmyndigheterna ska säkerställa att en revision av behandlingen av uppgifterna i N.SIS genomförs minst vart fjärde år i enlighet med internationella revisionsstandarder. Tillsynsmyndigheterna ska antingen genomföra revisionen själv eller begära den direkt från en oberoende dataskyddsrevisor. Den oberoende revisorn ska fortlöpande kvarstå under tillsynsmyndigheternas kontroll och ansvar.

3. Medlemsstaterna ska säkerställa att deras tillsynsmyndigheter har de resurser som krävs för att fullgöra de uppgifter som de åläggs enligt denna förordning och har tillgång till rådgivning från personer med tillräcklig kunskap om biometriska uppgifter.

#### Artikel 70

##### Tillsyn över eu-LISA

1. Europeiska datatillsynsmannen ska ansvara för att övervaka eu-LISA:s behandling av personuppgifter och för att säkerställa att den utförs i enlighet med denna förordning. De uppgifter och befogenheter som avses i artiklarna 57 och 58 i förordning (EU) 2018/1725 ska gälla i enlighet därmed.

2. Europeiska datatillsynsmannen ska genomföra en revision av eu-LISA:s behandling av personuppgifter minst vart fjärde år i enlighet med internationella revisionsstandarder. En rapport från denna revision ska sändas till Europaparlamentet, rådet, eu-LISA, kommissionen och tillsynsmyndigheterna. eu-LISA ska ges tillfälle att yttra sig innan rapporten antas.

#### Artikel 71

##### Samarbete mellan tillsynsmyndigheter och Europeiska datatillsynsmannen

1. Tillsynsmyndigheterna och Europeiska datatillsynsmannen ska inom ramen för sina respektive befogenheter aktivt samarbeta inom sina ansvarsområden och säkerställa samordnad tillsyn över SIS.

2. Tillsynsmyndigheterna och Europeiska datatillsynsmannen ska inom ramen för sina respektive befogenheter och efter behov utbyta relevant information, bistå varandra vid genomförandet av revisioner och inspektioner, utreda svårigheter när det gäller tolkningen eller tillämpningen av denna förordning och andra tillämpliga unionsrättsakter, undersöka problem som framkommer i samband med utövandet av oberoende tillsyn eller i samband med utövandet av de registrerades rättigheter, utarbeta harmoniserade förslag till gemensamma lösningar på eventuella problem och främja medvetenheten om rättigheterna i fråga om dataskydd.

3. För de ändamål som anges i punkt 2 ska tillsynsmyndigheterna och Europeiska datatillsynsmannen hålla minst två möten om året inom ramen för Europeiska dataskyddsstyrelsen. Europeiska dataskyddsstyrelsen ska stå för kostnaderna och tillhandahålla tjänster för dessa möten. En arbetsordning ska antas vid det första mötet. Ytterligare arbetsmetoder ska utvecklas gemensamt efter behov.

4. En gemensam verksamhetsrapport om samordnad tillsyn ska årligen översändas av Europeiska dataskyddsstyrelsen till Europaparlamentet, rådet och kommissionen.

#### KAPITEL XVII

##### Skadeståndsansvar och sanktioner

#### Artikel 72

##### Skadeståndsansvar

1. Utan att det påverkar rätten till ersättning och eventuellt skadeståndsansvar enligt förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725 ska följande gälla:

- Varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en otillåten behandling av personuppgifter genom användning av N.SIS eller någon annan åtgärd från en medlemsstats sida som är oförenlig med denna förordning ska ha rätt till ersättning från den senare medlemsstaten.
- Varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en åtgärd från eu-LISA:s sida som är oförenlig med denna förordning ska ha rätt till ersättning från eu-LISA.

En medlemsstat eller eu-LISA ska helt eller delvis undantas från skadeståndsansvar enligt första stycket om de bevisar att de inte är ansvariga för den händelse som orsakade skadan.

2. Om en medlemsstats underlåtenhet att fullgöra sina skyldigheter enligt denna förordning skadar SIS ska medlemsstaten vara ansvarig för denna skada, såvida inte eu-LISA eller en annan medlemsstat som deltar i SIS har underlåtit att vidta rimliga åtgärder för att förhindra skadan eller minimera dess verkningar.

3. Skadeståndsanspråk mot en medlemsstat för sådan skada som avses i punkterna 1 och 2 ska regleras i den medlemsstatens nationella rätt. Skadeståndsanspråk mot eu-LISA för sådan skada som avses i punkterna 1 och 2 ska omfattas av de villkor som fastställs i fördragen.

### Artikel 73

#### Sanktioner

Medlemsstaterna ska säkerställa att missbruk av SIS-uppgifter eller behandling av sådana uppgifter eller utbyte av tilläggsinformation i strid med denna förordning är belagt med sanktioner i enlighet med nationell rätt.

Sanktionerna ska vara effektiva, proportionella och avskräckande.

### KAPITEL XVIII

#### Slutbestämmelser

### Artikel 74

#### Övervakning och statistik

1. eu-LISA ska säkerställa att det finns rutiner för att övervaka hur SIS fungerar i förhållande till mål i fråga om produktivitet, kostnadseffektivitet, säkerhet och tjänsternas kvalitet.
2. eu-LISA ska, för tekniskt underhåll, för rapportering, för rapportering om uppgifters kvalitet och för statistik, ha tillgång till nödvändiga upplysningar om den databehandling som sker i det centrala SIS.
3. eu-LISA ska utarbeta daglig, månatlig och årlig statistik som visar antalet loggningsnoteringar per registreringskategori, både per medlemsstat och aggregerat. eu-LISA ska också tillhandahålla årliga rapporter om antalet träffar per registreringskategori, hur många gånger SIS använts för sökningar och hur många gånger SIS använts för att föra in, uppdatera eller radera registreringar, både per medlemsstat och aggregerat. Den statistik som utarbetas får inte innehålla några personuppgifter. Den årliga statistiska rapporten ska offentliggöras.
4. Medlemsstaterna, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån ska tillstålla eu-LISA och kommissionen den information som de behöver för att utarbeta de rapporter som avses i punkterna 3, 6, 8 och 9.
5. Denna information ska omfatta separat statistik om antalet sökningar som utförs av de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon och de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis eller säkerställa trafikledning för fartyg, även fartygsmotorer, och luftfartyg, inklusive flygmotorer, samt skjutvapen, eller på dessas vägnar. Statistiken ska också visa antalet träffar per registreringskategori.
6. eu-LISA ska tillstålla Europaparlamentet, rådet, medlemsstaterna, kommissionen, Europol, Eurojust, Europeiska gräns- och kustbevakningsbyrån och Europeiska datatillsynsmannen alla statistiska rapporter den har utarbetat.

För att övervaka genomförandet av unionsrättsakter, även tillämpningen av förordning (EU) nr 1053/2013, får kommissionen begära att eu-LISA, antingen regelbundet eller för särskilda ändamål, tillhandahåller ytterligare specifika statistiska rapporter om hur SIS fungerar och används och om utbytet av tilläggsinformation.

Europeiska gräns- och kustbevakningsbyrån får begära att eu-LISA, antingen regelbundet eller för särskilda ändamål, tillhandahåller ytterligare specifika statistiska rapporter för att genomföra de risk- och sårbarhetsanalyser som avses i artiklarna 11 och 13 i förordning (EU) 2016/1624.

7. Vid tillämpning av artikel 15.4 och punkterna 3, 4 och 6 i den här artikeln ska eu-LISA inrätta, implementera och i sina tekniska lokaler hysa en central databas med de uppgifter som avses i artikel 15.4 och i punkt 3 i den här artikeln vilka inte möjliggör identifiering av enskilda personer men vilka gör det möjligt för kommissionen och de byråer som anges i punkt 6 i den här artikeln att få skräddarsydd rapportering och statistik. eu-LISA ska på begäran ge medlemsstaterna och kommissionen samt Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån, i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter, säker åtkomst till den centrala databasen via kommunikationsinfrastrukturen. eu-LISA ska genomföra åtkomstkontroll och specifika användarprofiler för att säkerställa att åtkomst till den centrala databasen sker enbart för rapporterings- och statistikändamål.

8. Två år efter den dag då denna förordning börjar tillämpas i enlighet med artikel 79.5 första stycket och därefter vartannat år ska eu-LISA till Europaparlamentet och rådet överlämna en rapport om hur det centrala SIS och kommunikationsinfrastrukturen fungerat tekniskt, inklusive deras säkerhet, om Afis och om det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstaterna. Så snart den relevanta tekniken är i bruk ska rapporten även innehålla en utvärdering av användningen av ansiktsbilder för identifiering av personer.

9. Tre år efter den dag då denna förordning börjar tillämpas i enlighet med artikel 79.5 och därefter vart fjärde år ska kommissionen utföra en övergripande utvärdering av det centrala SIS och det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstaterna. Denna övergripande utvärdering ska innehålla en granskning av uppnådda resultat i relation till målen och en bedömning av huruvida de förutsättningar som ligger till grund för systemet fortfarande är giltiga, tillämpningen av denna förordning när det gäller det centrala SIS, säkerheten i det centrala SIS och om några slutsatser kan dras beträffande den framtida verksamheten. Utvärderingsrapporten ska även omfatta en bedömning av Afis samt de informationskampanjer om SIS som utförs av kommissionen i enlighet med artikel 19.

Kommissionen ska överlämna utvärderingsrapporten till Europaparlamentet och rådet.

10. Kommissionen ska anta genomförandeakter för att fastställa närmare bestämmelser om driften av den centrala databas som avses i punkt 7 i den här artikeln och bestämmelser om dataskydd och datasäkerhet som är tillämpliga på den databasen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 76.2.

#### Artikel 75

##### Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Den befogenhet att anta delegerade akter som avses i artiklarna 38.3 och 43.4 ska ges till kommissionen tills vidare från och med den 27 december 2018.
3. Den delegering av befogenhet som avses i artiklarna 38.3 och 43.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Innan kommissionen antar en delegerad akt, ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artiklarna 38.3 eller 43.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

#### Artikel 76

##### Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

#### Artikel 77

##### Ändringar av beslut 2007/533/RIF

Beslut 2007/533/RIF ska ändras på följande sätt:

1. Artikel 6 ska ersättas med följande:

”Artikel 6

##### Nationella system

1. Varje medlemsstat ska ansvara för att inrätta, driva, underhålla och vidareutveckla sitt N.SIS II och ansluta det till NI-SIS.
2. Varje medlemsstat ska ansvara för att säkerställa oavbruten tillgång till SIS II-uppgifter för slutanvändare.”

2. Artikel 11 ska ersättas med följande:

"Artikel 11

**Konfidentialitet – Medlemsstater**

1. Varje medlemsstat ska i enlighet med den nationella lagstiftningen tillämpa sina regler om tystnadsplikt eller motsvarande konfidentialitetskrav på alla personer eller organ som arbetar med SIS II-uppgifter och tilläggsinformation. Denna skyldighet ska gälla även efter det att dessa personer lämnar sin tjänst eller anställning och efter det att organets verksamhet upphört.

2. Om en medlemsstat samarbetar med externa entreprenörer i samband med SIS II-relaterade uppgifter, ska den noga övervaka entreprenörens verksamhet för att säkerställa att alla bestämmelser i detta beslut följs, särskilt i fråga om säkerhet, konfidentialitet och dataskydd.

3. Den operativa förvaltningen av N.SIS II eller av tekniska kopior får inte anförtros privata företag eller privata organisationer."

3. Artikel 15 ska ändras på följande sätt:

- a) Följande punkt ska införas:

"3a. Förvaltningsmyndigheten ska utveckla och underhålla en mekanism och förfaranden för kvalitetskontroll av uppgifterna i CS-SIS. Den ska regelbundet rapportera till medlemsstaterna i detta avseende.

Förvaltningsmyndigheten ska regelbundet rapportera till kommissionen om problem som uppstått och vilka medlemsstater som berörs.

Kommissionen ska regelbundet rapportera till Europaparlamentet och rådet om problem som uppstått i fråga om uppgifternas kvalitet."

- b) Punkt 8 ska ersättas med följande:

"8. Den operativa förvaltningen av det centrala SIS II ska omfatta alla de uppgifter som krävs för att det centrala SIS II ska kunna fungera dygnet runt alla dagar i veckan i enlighet med detta beslut, särskilt det underhåll och den tekniska utveckling som krävs för att systemet ska kunna fungera smidigt. Dessa uppgifter ska även omfatta samordning och förvaltning av samt stöd till tester för det centrala SIS II och N.SIS II som säkerställer att det centrala SIS II och N.SIS II fungerar i enlighet med kraven på teknisk överensstämmelse i artikel 9."

4. I artikel 17 ska följande punkter läggas till:

"3. Om förvaltningsmyndigheten samarbetar med externa entreprenörer i samband med SIS II-relaterade uppgifter, ska den noga övervaka entreprenörens verksamhet för att säkerställa efterlevnaden av samtliga bestämmelser i detta beslut, särskilt i fråga om säkerhet, konfidentialitet och dataskydd.

4. Den operativa förvaltningen av CS-SIS får inte anförtros privata företag eller privata organisationer."

5. I artikel 21 ska följande stycke läggas till:

"Om en person eller ett föremål söks i samband med en registrering med anknytning till ett terroristbrott ska ärendet anses vara tillräckligt adekvat, relevant och viktigt för att motivera en registrering i SIS II. Av skäl som rör allmän eller nationell säkerhet kan medlemsstaterna i undantagsfall avstå från att föra in en registrering, när denna sannolikt skulle försvåra officiella eller rättsliga utredningar, undersökningar eller förfaranden."

6. Artikel 22 ska ersättas med följande:

"Artikel 22

**Särskilda bestämmelser om införande av, kontroll eller sökning med fotografier och fingeravtryck**

1. Fotografier och fingeravtryck får föras in endast efter en särskild kvalitetskontroll i syfte att fastställa att minimistandarder för uppgifternas kvalitet är uppfyllda. Specificeringen av den särskilda kvalitetskontrollen ska fastställas i enlighet med förfarandet i artikel 67.

2. Om fotografier och fingeravtrycksuppgifter finns tillgängliga i en registrering i SIS II ska sådana fotografier och fingeravtrycksuppgifter användas för att bekräfta identiteten på en person som har lokaliserats efter en alfanumerisk sökning i SIS II.

3. En sökning i fingeravtrycksuppgifter för att identifiera en person får göras i samtliga fall. En sökning i fingeravtrycksuppgifter ska dock göras för att identifiera en person om det inte går att fastställa personens identitet på annat sätt ska. Det centrala SIS II ska därför innehålla ett automatiskt fingeravtrycksidentifieringssystem (Afis).

4. En sökning i fingeravtrycksuppgifter i SIS II avseende registreringar som förts in i enlighet med artiklarna 26, 32 och 36 får också göras med hjälp av fullständiga eller ofullständiga uppsättningar fingeravtryck som upptäckts på platsen för ett grovt brott eller terroristbrott som utreds, om det med stor sannolikhet kan fastställas att dessa uppsättningar avtryck tillhör en gärningsman och förutsatt att sökningen görs samtidigt i medlemsstaternas relevanta nationella fingeravtrycksdatabaser.”

7. Artikel 41 ska ersättas med följande:

”Artikel 41

#### **Europols åtkomst till uppgifter i SIS II**

1. Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol), som inrättats genom Europaparlamentets och rådets förordning (EU) 2016/794 (\*), ska, där så krävs för att Europol ska fullgöra sitt uppdrag, ha rätt att få åtkomst till och söka i uppgifter i SIS II. Europol får även utbyta och begära ytterligare tilläggsinformation i enlighet med bestämmelserna i Sirenehandboken.

2. Om en sökning som Europol utför visar att det finns en registrering i SIS II ska Europol informera den registrerande medlemsstaten genom att utbyta tilläggsinformation via kommunikationsinfrastrukturen och i enlighet med bestämmelserna i Sirenehandboken. Fram till dess att Europol har möjlighet att använda funktionerna för utbyte av tilläggsinformation ska Europol informera de registrerande medlemsstaterna genom de kanaler som fastställs i förordning (EU) 2016/794.

3. Europol får behandla den tilläggsinformation som har erhållits från medlemsstater för att jämföra den med sina databaser och projekt för operativa analyser i syfte att kartlägga kopplingar eller andra relevanta samband mellan uppgifter och för de analyser av strategisk eller tematisk karaktär och för de operativa analyser som avses i artikel 18.2 a, b och c i förordning (EU) 2016/794. All Europols eventuella behandling av tilläggsinformation vid tillämpning av denna artikel ska ske i överensstämmelse med den förordningen.

4. Europols användning av uppgifter som erhållits genom en sökning i SIS II eller genom behandling av tilläggsinformation kräver tillstånd från den registrerande medlemsstaten. Om medlemsstaten tillåter användning av uppgifterna ska Europols behandling av dem regleras av förordning (EU) 2016/794. Europol får endast meddela sådana uppgifter till tredjeländer eller utomstående instanser med den registrerande medlemsstatens tillstånd och med fullständig efterlevnad av unionsrätten om dataskydd.

5. Europol,

- a) får, utan att det påverkar tillämpningen av punkterna 4 och 6, inte sammankoppla några delar av SIS II med, eller överföra de uppgifter i SIS II till vilka Europol har åtkomst till, något system för insamling och behandling av uppgifter drivet av eller vid Europol, eller ladda ned eller på annat sätt kopiera några delar av SIS II,
- b) ska, utan hinder av vad som sägs i artikel 31.1 i förordning (EU) 2016/794, radera tilläggsinformation som innehåller personuppgifter senast ett år efter det att motsvarande registrering raderats. Genom undantag får Europol, i de fall där Europol har information i sina databaser eller projekt för operativa analyser om ett ärende med koppling till tilläggsinformationen, för att kunna utföra sina arbetsuppgifter undantagsvis fortsätta att lagra tilläggsinformationen där så är nödvändigt. Europol ska informera den registrerande och den verkställande medlemsstaten om den fortsatta lagringen av sådan tilläggsinformation och lämna en motivering till detta,
- c) ska begränsa åtkomsten till uppgifter i SIS II, inklusive tilläggsinformation, till personal som har särskild behörighet vid Europol som behöver åtkomst till sådana uppgifter för att kunna utföra sina uppgifter,
- d) ska vidta och tillämpa åtgärder för att säkerställa säkerhet, konfidentialitet och egenkontroll i enlighet med artiklarna 10, 11 och 13,
- e) ska säkerställa att dess personal som har behörighet att behandla SIS II-uppgifter får lämplig utbildning och information i enlighet med artikel 14, och
- f) ska, utan att det påverkar tillämpningen av förordning (EU) 2016/794, låta Europeiska datatillsynsmannen övervaka och se över hur Europol utövat rätten att få åtkomst till och söka i uppgifter i SIS II samt hur utbytet och behandlingen av tilläggsinformation hanterats.

6. Europol får endast kopiera uppgifter från SIS II för tekniska ändamål om sådan kopiering krävs för att vederbörligen bemyndigad personal vid Europol ska kunna göra direkta sökningar. Dessa kopior ska omfattas av detta beslut. Den tekniska kopian får endast användas för lagring av SIS II-uppgifter medan man söker i uppgifterna. När sökningen i uppgifterna är slutförd ska de raderas. Sådan användning ska inte anses vara en olaglig nedladdning eller kopiering av SIS II-uppgifter. Europol får inte kopiera registreringsuppgifter eller kompletterande uppgifter införda av medlemsstaterna eller uppgifter från CS-SIS II till andra Europolsystem.

7. Europol ska i enlighet med bestämmelserna i artikel 12 föra loggar över all åtkomst till och sökning i SIS II för att kontrollera om databehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa en lämplig nivå för datasäkerhet och dataintegritet. Sådana loggar och sådan dokumentation ska inte anses vara en olaglig nedladdning eller kopiering av någon del av SIS II.

8. Medlemsstaterna ska informera Europol genom att utbyta tilläggsinformation om alla träffar på registreringar med anknytning till terroristbrott. Undantagsvis får medlemsstaterna avstå från att informera Europol om detta skulle äventyra pågående utredningar eller en enskild persons säkerhet, eller strida mot den registrerande medlemsstatens väsentliga säkerhetsintressen.

9. Punkt 8 ska tillämpas från och med den dag då Europol kan ta emot tilläggsinformation i enlighet med punkt 1.

(\*) Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).”

8. Följande artikel ska införas:

”Artikel 42a

**Åtkomst till uppgifter i SIS II för de europeiska gräns- och kustbevakningsenheterna, enheterna med personal som arbetar med återvändande och medlemmarna i stödgrupperna för migrationshantering**

1. I enlighet med artikel 40.8 i Europaparlamentets och rådets förordning (EU) 2016/1624 (\*) ska medlemmarna i de enheter och grupper som avses i artikel 2.8 och 2.9 i den förordningen, inom ramen för sitt mandat och under förutsättning att de är behöriga att göra kontroller i enlighet med artikel 40.1 i det här beslutet och har fått den utbildning som krävs i enlighet med artikel 14 i det här beslutet, ha rätt att få åtkomst till och söka i uppgifter i SIS II i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter och i den mån det krävs enligt den operativa planen för en särskild insats. Åtkomst till uppgifter i SIS II får inte beviljas någon annan medlem i enheten eller gruppen.

2. Medlemmar i de enheter och grupper som avses i punkt 1 ska utöva denna rätt att ha åtkomst till och söka i uppgifter i SIS II i enlighet med punkt 1 genom ett tekniskt gränssnitt. Det tekniska gränssnittet ska inrättas och underhållas av Europeiska gräns- och kustbevakningsbyrån och ska möjliggöra direktkoppling till det centrala SIS II.

3. Om en sökning som utförs av en medlem i de enheter och grupper som avses i punkt 1 i den här artikeln visar att det finns en registrering i SIS II, ska den registrerande medlemsstaten informeras. I enlighet med artikel 40 i förordning (EU) 2016/1624 får medlemmarna i enheterna eller grupperna endast vidta åtgärder utifrån en registrering i SIS II i enlighet med anvisningar från och, som en allmän regel, endast i närvaro av gränsbevakningstjänstemän eller personal som arbetar med återvändande i den värdmedlemsstat där de är verksamma. Värdmedlemsstaten får ge medlemmar i enheterna eller grupperna tillstånd att agera för dess räkning.

4. Europeiska gräns- och kustbevakningsbyrån ska föra loggar över all åtkomst till och sökning i SIS II i enlighet med bestämmelserna i artikel 12 för att kontrollera om databehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa en lämplig nivå för datasäkerhet och dataintegritet.

5. Europeiska gräns- och kustbevakningsbyrån ska anta och tillämpa åtgärder för att säkerställa säkerhet, konfidentialitet och egenkontroll i enlighet med artiklarna 10, 11 och 13, och säkerställa att de enheter och grupper som avses i punkt 1 i den här artikeln tillämpar dessa åtgärder.

6. Ingenting i denna artikel ska tolkas som att det påverkar bestämmelserna i förordning (EU) 2016/1624 beträffande dataskydd eller skadeståndsansvar för Europeiska gräns- och kustbevakningsbyrån om den behandlar uppgifter på ett otillåtet eller felaktigt sätt.

7. Utan att det påverkar tillämpningen av punkt 2 får inga delar av SIS II sammankopplas med något system för insamling och behandling av uppgifter som drivs av de enheter eller grupper som avses i punkt 1 eller av Europeiska gräns- och kustbevakningsbyrån; inte heller får de uppgifter i SIS II som dessa enheter och grupper har åtkomst till överföras till ett sådant system. Ingen del av SIS II får laddas ned eller kopieras. Loggning av åtkomst och sökningar ska inte anses vara en olaglig nedladdning eller kopiering av SIS II-uppgifter.

8. Europeiska gräns- och kustbevakningsbyrån ska tillåta att Europeiska datatillsynsmannen övervakar och ser över den verksamhet som bedrivs av de enheter och grupper som avses i denna artikel när de utövar sin rätt till åtkomst och sökning i uppgifter i SIS II. Detta påverkar inte tillämpningen av ytterligare bestämmelser i Europaparlamentets och rådets förordning (EU) 2018/1725 (\*\*).

(\*) Europaparlamentets och rådets förordning (EU) 2016/1624 av den 14 september 2016 om en europeisk gräns- och kustbevakning och om ändring av Europaparlamentets och rådets förordning (EU) 2016/399 och upphävande av Europaparlamentets och rådets förordning (EG) nr 863/2007, rådets förordning (EG) nr 2007/2004 och rådets beslut 2005/267/EG (EUT L 251, 16.9.2016, s. 1).

(\*\*) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut 1247/2002/EG (EUT L 295, 21.11.2018, s. 39)."

#### Artikel 78

### Upphävande

Förordning (EG) nr 1986/2006 och beslut 2007/533/RIF och 2010/261/EU ska upphöra att gälla den dag då den här förordningen börjar tillämpas enligt artikel 79.5 första stycket.

Hänvisningar till den upphävda förordning (EG) nr 1986/2006 och det upphävda beslut 2007/533/RIF ska anses som hänvisningar till den här förordningen och läsas i enlighet med jämförelsetabellen i bilagan.

#### Artikel 79

### Ikraftträdande, idrifttagning och tillämpning

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Senast den 28 december 2021 ska kommissionen anta ett beslut som fastställer det datum då SIS tas i drift i enlighet med denna förordning, efter en kontroll av att följande villkor har uppfyllts:

- a) De genomförandeakter som är nödvändiga för tillämpningen av denna förordning har antagits.
- b) Medlemsstaterna har underrättat kommissionen om att de har vidtagit de tekniska åtgärder och antagit den lagstiftning som behövs för att de ska kunna behandla SIS-uppgifter och utbyta tilläggsinformation i enlighet med denna förordning.
- c) eu-LISA har underrättat kommissionen om att alla tester avseende CS-SIS och samspelet mellan CS-SIS och N.SIS har slutförts med gott resultat.

3. Kommissionen ska noga övervaka hur de villkor som anges i punkt 2 gradvis uppfylls och ska informera Europaparlamentet och rådet om resultatet av den kontroll som avses i den punkten.

4. Senast den 28 december 2019 och därefter varje år, till dess att det kommissionsbeslut som avses i punkt 2 har fattats, ska kommissionen överlämna en rapport till Europaparlamentet och rådet om det aktuella läget i förberedelserna inför ett fullständigt genomförande av denna förordning. Denna rapport ska även innehålla detaljerad information om de kostnader som uppkommit och information om eventuella risker som kan påverka de totala kostnaderna.

5. Denna förordning ska tillämpas från och med den dag som fastställs i enlighet med punkt 2.

Genom undantag från första stycket ska

- a) artiklarna 4.4, 5, 8.4, 9.1, 9.5, 12.8, 15.7, 19, 20.4, 20.5, 26.6, 32.9, 34.3, 36.6, 38.3, 38.4, 42.5, 43.4, 54.5, 62.4, 63.6, 74.7, 74.10, 75, 76 och 77.1–77.5 samt punkterna 3 och 4 i den här artikeln tillämpas från och med dagen för denna förordnings ikraftträdande,



- b) artikel 77.7 och 77.8 tillämpas från och med den 28 december 2019,
  - c) artikel 77.6 tillämpas från och med den 28 december 2020.
6. Det kommissionsbeslut som avses i punkt 2 ska offentliggöras i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i medlemsstaterna i enlighet med fördragen.

Utfärdad i Bryssel den 28 november 2018.

*På Europaparlamentets vägnar*

A. TAJANI

*Ordförande*

*På rådets vägnar*

K. EDTSTADLER

*Ordförande*

---

## BILAGA

## JÄMFÖRELSETABELL

Beslut 2007/533/RIF	Denna förordning
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	Artiklarna 42 och 43
Artikel 23	Artikel 22
—	Artikel 23
Artikel 24	Artikel 24
Artikel 25	Artikel 25
Artikel 26	Artikel 26
Artikel 27	Artikel 27
Artikel 28	Artikel 28
Artikel 29	Artikel 29
Artikel 30	Artikel 30
Artikel 31	Artikel 31
Artikel 32	Artikel 32
Artikel 33	Artikel 33
Artikel 34	Artikel 34
Artikel 35	Artikel 35
Artikel 36	Artikel 36
Artikel 37	Artikel 37
Artikel 38	Artikel 38
Artikel 39	Artikel 39
—	Artikel 40
—	Artikel 41

Beslut 2007/533/RIF	Denna förordning
Artikel 40	Artikel 44
—	Artikel 45
—	Artikel 46
—	Artikel 47
Artikel 41	Artikel 48
Artikel 42	Artikel 49
—	Artikel 51
Artikel 42a	Artikel 50
Artikel 43	Artikel 52
Artikel 44	Artikel 53
Artikel 45	Artikel 54
—	Artikel 55
Artikel 46	Artikel 56
Artikel 47	Artikel 57
Artikel 48	Artikel 58
Artikel 49	Artikel 59
—	Artikel 60
Artikel 50	Artikel 61
Artikel 51	Artikel 62
Artikel 52	Artikel 63
Artikel 53	Artikel 64
Artikel 54	Artikel 65
Artikel 55	—
Artikel 56	—
Artikel 57	Artikel 66
Artikel 58	Artikel 67
Artikel 59	Artikel 68
Artikel 60	Artikel 69
Artikel 61	Artikel 70
Artikel 62	Artikel 71
Artikel 63	—
Artikel 64	Artikel 72
Artikel 65	Artikel 73
Artikel 66	Artikel 74
—	Artikel 75
Artikel 67	Artikel 76
Artikel 68	—
—	Artikel 77
Artikel 69	—
—	Artikel 78
Artikel 70	—
Artikel 71	Artikel 79
Förordning (EG) nr 1986/2006	Denna förordning
Artiklarna 1, 2 och 3	Artikel 45