EUROPEISKA
KOMMISSIONEN

Bryssel den 21.12.2016
COM(2016) 883 final

2016/0409 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring av förordning (EU) nr 515/2014 och om upphävande av förordning (EG) nr 1986/2006, rådets beslut 2007/533/RIF och kommissionens beslut 2010/261/EU

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Under de senaste två åren har Europeiska unionen arbetat med att parallellt ta itu med de separata utmaningarna i samband med migrationshantering, integrerad förvaltning av EU:s yttre gränser och kampen mot terrorism och gränsöverskridande brottslighet. Ett effektivt informationsutbyte mellan medlemsstaterna samt mellan medlemsstaterna och relevanta EU-organ är ytterst viktigt för att bemöta dessa utmaningar på ett kraftfullt sätt och för att bygga en effektiv och verklig säkerhetsunion.

Schengens informationssystem (SIS) är det verktyg som fungerat bäst för det praktiska samarbetet mellan immigrations-, polis- och tullmyndigheterna och de rättsliga myndigheterna i EU och de Schengenassocierade länderna. Medlemsstaternas behöriga myndigheter, t.ex. poliser, gränsbevakningstjänstemän och tulltjänstemän, behöver ha åtkomst till högkvalitativ information om de personer eller föremål som de kontrollerar, med tydliga anvisningar om vad som bör göras i varje enskilt fall. Detta storskaliga informationssystem utgör själva kärnan i Schengensamarbetet och har en viktig roll i underlättandet av den fria rörligheten för personer inom Schengenområdet. Det gör det möjligt för behöriga myndigheter att lägga in och söka uppgifter om efterlysta personer, personer som kanske inte har rätt att resa in eller vistas i EU, försvunna personer – särskilt barn – och föremål som kan vara stulna, bortförda eller försvunna. SIS innehåller inte bara information om en viss person eller ett visst föremål, utan även tydliga anvisningar om vad de behöriga myndigheterna ska göra om de hittar den personen eller det föremålet.

Kommissionen utförde en övergripande utvärdering[1] av SIS 2016, tre år efter det att andra generationen av systemet togs i bruk. Denna utvärdering visade att SIS har gett verkligt goda operativa resultat. Under 2015 kontrollerade de nationella behöriga myndigheterna personer och föremål mot uppgifter som lagrats i SIS vid nästan 2,9 miljarder tillfällen och utbytte tilläggsinformation över 1,8 miljoner gånger. Trots detta bör systemets effektivitet och ändamålsenlighet stärkas ytterligare på grundval av dessa positiva erfarenheter, i enlighet med kommissionens arbetsprogram för 2017. I detta syfte lägger kommissionen fram en första serie om tre förslag för att förbättra och utvidga användningen av SIS till följd av utvärderingen, medan den samtidigt fortsätter arbetet med att göra de befintliga och framtida systemen för brottsbekämpning och gränsförvaltning mer interoperabla, utgående från det pågående arbetet i expertgruppen för informationssystem och interoperabilitet.

Dessa förslag omfattar användningen av systemet i samband med a) gränsförvaltning, b) polissamarbete och straffrättsligt samarbete, samt c) återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna. De första två förslagen utgör tillsammans den rättsliga grunden för inrättande, drift och användning av SIS. Förslaget om användning av SIS i samband med återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna kompletterar förslaget om gränsförvaltning och dess bestämmelser. Genom förslaget införs en

[1] Rapport till Europaparlamentet och rådet 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. (EUT...).

ny registreringskategori och det bidrar till genomförandet och tillsynen av direktiv 2008/115/EG[2].

På grund av att medlemsstaterna deltar i olika grad i EU:s politiska instrument på området med frihet, säkerhet och rättvisa är det nödvändigt att anta tre olika rättsliga instrument som ändå fungerar smidigt tillsammans för att möjliggöra den övergripande driften och användningen av systemet.

Parallellt inledde kommissionen i april 2016 en reflektionsprocess om ”Starkare och smartare informationssystem för gränser och säkerhet”[3] i syfte att utöka och förbättra informationshanteringen på EU-nivå. Det övergripande målet är att säkerställa att de behöriga myndigheterna systematiskt har nödvändig information från olika informationssystem till sitt förfogande. För att uppnå detta mål har kommissionen sett över den befintliga informationsstrukturen för att kartlägga informationsluckor och blinda fläckar som orsakas av brister i de befintliga systemens funktioner och av att EU:s övergripande uppgiftshanteringsstruktur är splittrad. För att stödja detta arbete har kommissionen inrättat en expertgrupp för informationssystem och interoperabilitet, vars preliminära resultat också har legat till grund för denna första serie förslag i fråga om uppgifternas kvalitet[4]. Ordförande Jean-Claude Juncker hänvisade också i sitt tal om tillståndet i unionen i september 2016 till vikten av att åtgärda de nuvarande bristerna i informationshanteringen och att förbättra interoperabiliteten och sammankopplingen mellan befintliga informationssystem.

Expertgruppen för informationssystem och interoperabilitet kommer att lägga fram sina resultat under första halvan av 2017, varpå kommissionen kommer att överväga en andra serie med förslag i mitten av 2017 för att ytterligare förbättra interoperabiliteten mellan SIS och andra it-system. Översynen av förordning (EU) nr 1077/2011[5] om Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA) är en lika viktig del av detta arbete och kommer sannolikt att leda till separata kommissionsförslag under 2017. Investeringar i informationsutbyte och informationshantering som fungerar snabbt, effektivt och med hög kvalitet samt säkerställande av interoperabiliteten mellan EU:s databaser och informationssystem är väsentliga delar av arbetet med att ta itu med aktuella säkerhetsutmaningar.

Detta förslag utgör en del av en första serie med förslag[6] för att förbättra SIS:s funktioner och dess drift och användning på området polissamarbete och straffrättsligt samarbete. Det genomför

(1) kommissionens tillkännagivande om att förbättra SIS:s mervärde för brottsbekämpande ändamål[7] för att svara på nya hot,

---

2 Europaparlamentets och rådets direktiv 2008/115/EG av den 16 december 2008 om gemensamma normer och förfaranden för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna (EUT L 348, 24.12.2008, s. 98).

3 COM(2016) 205 final, 6.4.2016.

4 Kommissionens beslut 2016/C 257/03, 17.6.2016.

5 Europaparlamentets och rådets förordning (EU) nr 1077/2011 av den 25 oktober 2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 286, 1.11.2011, s. 1).

6 Förordning (EU) 2018/xxx [in- och utresekontroller] och förordning (EU) 2018/xxx [återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna].

7 Se meddelandet *Att genomföra den europeiska säkerhetsagendan mot terrorism och bana väg för en säkerhetsunion*, COM(2016) 230 final av den 20 april 2016.

(2) en konsolidering av resultaten av det arbete med att genomföra SIS vilket har utförts under de senaste tre åren, bland annat tekniska ändringar av det centrala SIS för att utvidga några av de befintliga registreringskategorierna och införa nya funktioner,

(3) rekommendationer om tekniska och förfarandemässiga ändringar, på grundval av en övergripande utvärdering av SIS[8],

(4) begäranden om tekniska förbättringar från SIS:s slutanvändare, och

(5) de preliminära resultaten från expertgruppen för informationssystem och interoperabilitet[9]i fråga om uppgifternas kvalitet.

Sett till det faktum att detta förslag är nära kopplat till kommissionens förslag till en förordning om inrättande, drift och användning av SIS på området in- och utresekontroller är ett antal bestämmelser gemensamma för båda texterna. Dessa är till exempel åtgärder som avser genomgående användning av SIS vilka inte bara omfattar driften av det centrala systemet och de nationella systemen, utan även slutanvändarnas behov, stärkta åtgärder för driftskontinuitet, åtgärder som avser uppgifternas kvalitet, uppgiftsskydd och datasäkerhet, samt bestämmelser om övervakning, utvärdering och rapportering. Båda förslagen utvidgar också användningen av biometriska uppgifter[10].

Den befintliga rättsliga ramen för andra generationen av SIS – vad gäller dess användning i samband med polissamarbete och straffrättsligt samarbete – bygger på ett instrument som tidigare omfattades av den tredje pelaren, dvs. rådets beslut 2007/533/RIF[11], och ett instrument som tidigare omfattades av den första pelaren, dvs. förordning (EG) nr 1986/2006[12].Genom detta förslag konsolideras de befintliga instrumentens innehåll med tillägg av nya bestämmelser för att

- bättre harmonisera de nationella förfarandena för användningen av SIS, särskilt i fråga om terrorismrelaterade brott och barn som löper risk för att bli bortförda av en förälder,
- utvidga tillämpningsområdet för SIS genom införande av nya element av biometriska kännetecken till befintliga registreringar,
- införa tekniska ändringar för att förbättra säkerheten och minska den administrativa bördan genom att föreskriva obligatoriska nationella kopior och gemensamma tekniska standarder för genomförandet,
- beakta den genomgående användningen av SIS som inte bara ska omfatta de centrala och nationella systemen utan även säkerställa att slutanvändarna får alla uppgifter de behöver för att utföra sina uppgifter och att de följer alla säkerhetsbestämmelser när de behandlar SIS-uppgifter.

---

8 Rapport till Europaparlamentet och rådet 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. (EUT...).

9 Expertgrupp – ordförandens rapport av den 21 december 2016.

10 Se avsnitt 5 ”Övriga inslag” för en närmare beskrivning av de ändringar som ingår i detta förslag.

11 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).

12 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).

•Förenlighet med unionens politik på andra områden samt med befintliga och framtida rättsliga instrument

Förslaget har en nära koppling till och kompletterar unionens politik på andra områden, däribland följande:

(1) **Den inre säkerheten**, som betonades i den europeiska säkerhetsagendan[13] och kommissionens arbete i riktning mot en effektiv och verklig säkerhetsunion[14], för att förebygga, upptäcka, utreda och lagföra terroristbrott och andra grova brott genom att ge brottsbekämpande myndigheter rätt att behandla personuppgifter om personer som misstänks vara inblandade i terroristdåd eller grova brott.

(2) **Uppgiftsskydd**, i den mån detta förslag säkerställer skyddet av de grundläggande rättigheterna för de personer vars personuppgifter behandlas i SIS.

Förslaget har också en nära koppling till och kompletterar befintlig unionslagstiftning, nämligen följande:

(3) **Europeiska gräns- och kustbevakningen**, vad gäller deras åtkomst till SIS i samband med det föreslagna EU-systemet för reseuppgifter och resetillstånd (Etias)[15], och i samband med tillhandahållandet av ett tekniskt gränssnitt för åtkomst till SIS för de europeiska gräns- och kustbevakningsenheterna, enheterna med personal som arbetar med återvändande och medlemmar i stödgruppen för migrationshantering vilka, inom ramen för sitt mandat, ska ha rätt att få åtkomst till och söka uppgifter i SIS.

(4) **Europol**, i den mån detta förslag ger Europol ytterligare rätt att få åtkomst till och rätt att, inom ramen för byråns mandat, söka uppgifter i SIS.

(5) **Prüm**, i den mån de utökade möjligheterna i detta förslag att identifiera personer på grundval av fingeravtryck (samt ansiktsbilder och DNA-profiler) kompletterar de befintliga Prümbestämmelserna[16] om ömsesidig gränsöverskridande onlineåtkomst till utvalda nationella DNA-databaser och automatiska system för identifiering av fingeravtryck.

Förslaget har också en nära koppling till och kompletterar framtida unionslagstiftning, nämligen följande:

(6) **Förvaltning av de yttre gränserna.** Förslaget kompletterar den planerade nya principen i kodexen om Schengengränserna om systematiska kontroller av alla resande, även EU-medborgare, mot relevanta databaser vid inresa till och utresa från Schengenområdet, vilken inrättas som ett svar på problemet med utländska terroriststridande.

(7) **In- och utresesystemet.** Förslaget syftar till att återspegla den föreslagna användningen av en kombination av fingeravtryck och ansiktsbilder som biometriska kännetecken vid driften av in- och utresesystemet.

---

13 COM(2015) 185 final.

14 COM(2016) 230 final.

15 COM(2016) 731 final.

16 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) och 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).

(8) **Etias.** Förslaget beaktar det föreslagna Etias, som möjliggör en grundlig säkerhetskontroll, bland annat en kontroll i SIS, av tredjelandsmedborgare som avser att resa i EU.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Detta förslag använder artiklarna 82.1 d, 85.1, 87.2 a och 88.2 a i fördraget om Europeiska unionens funktionssätt som rättslig grund för bestämmelser om polissamarbete och straffrättsligt samarbete.

• Variabel geometri

Detta förslag bygger på de bestämmelser i Schengenregelverket som avser polissamarbete och straffrättsligt samarbete. Följaktligen måste konsekvenserna vad gäller olika protokoll och avtal med de associerade länderna beaktas.

Danmark: Enligt artikel 4 i protokoll nr 22 om Danmarks ställning, fogat till fördragen, ska Danmark inom sex månader efter det att rådet har beslutat om denna förordning, besluta huruvida landet ska genomföra detta förslag, som bygger på Schengenregelverket, i sin nationella lagstiftning.

Förenade kungariket: Denna förordning är bindande för Förenade kungariket i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, som är fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, och artikel 8.2 i 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[17].

Irland: Denna förordning är bindande för Irland i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, som är fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, och artikel 6.2 i rådets beslut 2002/192/EG av den 28 februari 2002 om Irlands begäran om att få delta i vissa bestämmelser i Schengenregelverket[18].

Bulgarien och Rumänien: Denna förordning utgör en rättsakt som grundas på Schengenregelverket eller som på annat sätt har samband med detta i enlighet med artikel 4.2 i 2005 års anslutningsakt. Denna förordning ska läsas jämförd med rådets beslut 2010/365/EU av den 29 juni 2010[19], varigenom de bestämmelser i Schengenregelverket som rör Schengens informationssystem med vissa begränsningar är tillämpliga på Bulgarien och Rumänien.

Cypern och Kroatien: Denna förordning utgör en rättsakt som grundas på Schengenregelverket eller som på annat sätt har samband med detta i enlighet med artikel 3.2 i 2003 års anslutningsakt respektive artikel 4.2 i 2011 års anslutningsakt.

---

17 EGT L 131, 1.6.2000, s. 43.

18 EGT L 64, 7.3.2002, s. 20.

19 Rådets beslut 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).

Associerade länder: På grundval av de avtal genom vilka Island, Norge, Schweiz och Liechtenstein associeras till genomförandet, tillämpningen och utvecklingen av Schengenregelverket blir dessa länder bundna av den föreslagna förordningen.

- **Subsidiaritetsprincipen**

Detta förslag utvecklar och bygger på det befintliga SIS, som har varit i drift sedan 1995. Den ursprungliga mellanstatliga ramen ersattes den 9 april 2013 av unionsinstrument (förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF). En fullständig subsidiaritetsprövning har utförts vid tidigare tillfällen; detta initiativ syftar till att ytterligare finslipa de befintliga bestämmelserna, ta itu med konstaterade brister och förbättra de operativa förfarandena.

Den avsevärda mängden informationsutbyte mellan medlemsstaterna genom SIS kan inte uppnås genom decentraliserade lösningar. På grund av åtgärdens omfattning, effekter och konsekvenser kan detta förslag bättre genomföras på unionsnivå.

Målen för detta förslag omfattar bland annat tekniska förbättringar för att effektivisera SIS och åtgärder för att harmonisera användningen av systemet i alla deltagande medlemsstater. På grund av målens transnationella karaktär och utmaningarna med att säkerställa ett effektivt informationsutbyte för att bekämpa ständigt föränderliga hot är EU väl lämpat att föreslå lösningar på dessa problem, som inte i tillräcklig utsträckning kan lösas av medlemsstaterna på egen hand.

Om befintliga begränsningar i SIS inte åtgärdas finns det en risk för att många möjligheter till maximerad effektivitet och mervärde på EU-nivå går förlorade, och för att blinda fläckar hindrar de behöriga myndigheternas arbete. Bristen på harmoniserade regler om radering av överflödiga registreringar i systemet kan exempelvis leda till hinder för den fria rörligheten för personer, vilken är en av unionens grundläggande principer.

- **Proportionalitetsprincipen**

I artikel 5 i fördraget om Europeiska unionen anges det att unionens åtgärder inte ska gå utöver vad som är nödvändigt för att nå målen i fördraget. EU:s åtgärder bör utformas så att målet för förslaget uppnås och så att genomförandet blir så effektivt som möjligt. Det föreslagna initiativet utgör en ändring av SIS i fråga om polissamarbete och straffrättsligt samarbete.

Förslaget bygger på principerna om inbyggt integritetsskydd. Vad gäller rätten till skydd av personuppgifter är detta förslag proportionerligt eftersom det innehåller särskilda bestämmelser om radering av registreringar och inte kräver att uppgifterna samlas in och lagras för en längre tid än vad som är absolut nödvändigt för att systemet ska kunna fungera och målen ska kunna uppnås. Med beaktande av de operativa kraven förkortas genom detta förslag lagringstiden för registreringar om föremål, som blir enhetliga med registreringar om personer (eftersom de ofta har samband med personuppgifter, såsom id-handlingar eller nummerplåtar). Polisens erfarenheter visar att stulen egendom kan återfås inom en relativt kort tidsperiod, vilket gör lagringstiden på 10 år för registreringar om föremål onödigt lång.

SIS-registreringar innehåller endast de uppgifter som krävs för att identifiera och lokalisera en person eller ett föremål och möjliggöra lämpliga operativa åtgärder. Alla övriga kompletterande uppgifter tillhandahålls via Sirenekontoren som möjliggör utbytet av tilläggsinformation.

Dessutom föreskrivs i förslaget tillämpning av alla nödvändiga skyddsåtgärder och mekanismer som krävs för ett effektivt skydd av de registrerades grundläggande rättigheter,

framför allt skyddet av deras privatliv och personuppgifter. Det innehåller också bestämmelser som särskilt utformats för att öka säkerheten för enskildas personuppgifter som finns i SIS.

Det krävs inga ytterligare förfaranden eller någon ytterligare harmonisering på EU-nivå för att systemet ska fungera. Den planerade åtgärden är proportionerlig eftersom den inte går utöver vad som är nödvändigt när det gäller åtgärder på EU-nivå för att uppnå de fastställda målen.

- **Val av instrument**

Den föreslagna omarbetningen tar formen av en förordning och kommer att ersätta rådets beslut 2007/533/RIF och samtidigt behålla mycket av innehållet i det beslutet. Beslut 2007/533/RIF antogs som ett så kallat instrument inom tredje pelaren inom ramen för det tidigare fördraget om Europeiska unionen. Sådana instrument inom tredje pelaren antogs av rådet utan Europaparlamentet som medlagstiftare. Den rättsliga grunden för detta förslag återfinns i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), eftersom pelarstrukturen upphörde att existera då Lissabonfördraget trädde i kraft den 1 december 2009. Den rättsliga grunden fordrar att det ordinarie lagstiftningsförfarandet används. Formen av en (Europaparlamentets och rådets) förordning måste väljas för att bestämmelserna ska vara bindande och direkt tillämpliga i alla medlemsstater.

Förslaget kommer att bygga på och förbättra ett befintligt centraliserat system som medlemsstaterna använder för samarbete sinsemellan, vilket kräver en gemensam struktur och bindande operativa regler. Dessutom fastställs i förslaget obligatoriska bestämmelser om åtkomst till systemet, bland annat för brottsbekämpande ändamål, vilka är enhetliga för alla medlemsstater och för Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa[20] (eu-LISA). Sedan den 9 maj 2013 ansvarar eu-LISA för den operativa förvaltningen av det centrala SIS, dvs. alla åtgärder som krävs för att säkerställa att det centrala SIS är i full drift 24 timmar om dygnet alla veckodagar. Detta förslag bygger på eu-LISA:s ansvarsuppgifter i fråga om SIS.

Dessutom fastställs i förslaget direkt tillämpliga bestämmelser som ger registrerade åtkomst till sina egna uppgifter och rättsmedel utan att detta kräver ytterligare genomförandeåtgärder.

Detta gör att en förordning är det enda möjliga rättsliga instrumentet.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning**

I enlighet med förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF utförde kommissionen tre år efter det att det centrala SIS II togs i bruk en övergripande utvärdering av systemet samt av det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstaterna.

Resultaten av utvärderingen visade på behovet av ändringar i den rättsliga grunden för SIS, för att kunna reagera bättre på nya säkerhets- och migrationsutmaningar. Detta inbegriper exempelvis ett förslag att ta itu med SIS från ett helhetsperspektiv genom att reglera slutanvändarnas användning av systemet och fastställa datasäkerhetsstandarder som även är

[20] Inrättad genom Europaparlamentets och rådets förordning (EU) nr 1077/2011 av den 25 oktober 2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 286, 1.11.2011, s. 1).

tillämpliga på slutanvändarapplikationer, att stärka systemets nytta för terrorismbekämpning genom att införa en ny åtgärd som bör vidtas, att klargöra situationen för barn som riskerar att bortföras av sina föräldrar och att utöka de biometriska kännetecken som finns tillgängliga i systemet.

Resultaten av utvärderingen visade också behovet av att göra rättsliga ändringar för att förbättra systemets tekniska funktion och för att rationalisera de nationella förfarandena. Dessa åtgärder kommer att öka systemets effektivitet och ändamålsenlighet genom att underlätta användningen och minska byråkratin. Ytterligare åtgärder har utformats för att förbättra uppgifternas kvalitet och insynen i systemet genom en tydligare beskrivning av medlemsstaternas och eu-LISA:s specifika rapporteringsuppgifter.

Resultaten av den övergripande utvärderingen (utvärderingsrapporten och det tillhörande arbetsdokumentet antogs den 21 december 2016[21]) utgör grunden för de åtgärder som ingår i detta förslag.

- **Samråd med berörda parter**

Under kommissionens utvärdering av SIS begärdes återkoppling och förslag från berörda parter, bland annat medlemmarna i SISVIS-kommittén enligt det förfarande som fastställs i artikel 67 i rådets beslut 2007/533/RIF. I kommittén ingår medlemsstaternas företrädare både för operativa Sirenefrågor (det gränsöverskridande samarbetet i fråga om SIS) och för tekniska frågor om utvecklingen och underhållet av SIS och den tillhörande Sireneapplikationen.

Som en del av utvärderingsförfarandet svarade medlemmarna på utförliga frågeformulär. Om ytterligare förtydliganden krävdes eller ämnet behövde utvecklas ytterligare skedde detta via e-postkommunikation eller riktade intervjuer. Detta fortlöpande förfarande gjorde det möjligt att ta upp frågor på ett övergripande och öppet sätt. Under 2015 och 2016 diskuterade medlemmarna i SISVIS-kommittén dessa frågor under särskilda möten och workshoppar.

Kommissionen höll också särskilda samråd med medlemsstaternas nationella dataskyddsmyndigheter och medlemmarna i samarbetsgruppen för tillsyn av SIS II i fråga om uppgiftsskydd. Medlemsstaterna delade med sig av sina erfarenheter av registrerades begäranden om åtkomst och de nationella dataskyddsmyndigheternas arbete genom att svara på ett särskilt frågeformulär. Svaren på detta frågeformulär från juni 2015 har beaktats vid utformandet av detta förslag.

Internt inrättade kommissionen en styrgrupp med företrädare från generalsekretariatet och generaldirektoraten för migration och inrikes frågor, rättsliga frågor och konsumentfrågor, personal och säkerhet samt informationsteknik. Denna styrgrupp har övervakat utvärderingsförfarandet och gett vägledning vid behov.

I resultaten av utvärderingen beaktades även den bevisning som samlats in under utvärderingsbesök på plats i medlemsstaterna där man detaljerat kontrollerade hur SIS används i praktiken. Detta inbegriper diskussioner och intervjuer med användarna, Sirenekontorets personal och nationella behöriga myndigheter.

Mot bakgrund av denna återkoppling föreskrivs i detta förslag åtgärder som ska förbättra systemets tekniska och operativa effektivitet och ändamålsenlighet.

---

[21] Rapport till Europaparlamentet och rådet 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.

- **Insamling och användning av sakkunnigutlåtanden**

Förutom samråden med berörda parter har kommissionen också begärt extern sakkunskap genom följande tre studier, vars resultat har tagits med vid utarbetandet av detta förslag:

- En teknisk bedömning av SIS (Kurt Salmon)[22]

  Vid denna bedömning konstaterades centrala problem i SIS:s funktion och framtida behov som bör beaktas, huvudsakligen orosmoment som rör maximering av driftskontinuiteten och säkerställande av att den övergripande strukturen kan anpassas till ökande kapacitetskrav.

- IKT-konsekvensbedömning av möjliga förbättringar av SIS II-arkitekturen (Kurt Salmon)[23]

  I denna studie bedömde man de löpande kostnaderna för driften av SIS på nationell nivå och utvärderade två möjliga tekniska scenarier för en förbättring av systemet. Bägge scenarierna omfattar en rad tekniska förslag med fokus på förbättringar av det centrala systemet och den övergripande strukturen.

- IKT-konsekvensbedömning av de tekniska förbättringarna av SIS II-strukturen – Slutrapport, den 10 november 2016 (Wavestone)[24]

  I denna studie bedömde man hur medlemsstaternas kostnader påverkas av tillämpningen av en nationell kopia genom en analys av tre scenarier (ett helt centraliserat system, en standardiserad N.SIS-tillämpning som eu-LISA utvecklar och tillhandahåller medlemsstaterna och en separat N.SIS-tillämpning med gemensamma tekniska standarder).

- **Konsekvensbedömning**

Kommissionen har inte genomfört någon konsekvensbedömning.

De tre oberoende bedömningar som nämns ovan (under ”Insamling och användning av sakkunnigutlåtanden”) utgjorde grunden för bedömningen av konsekvenserna av systemändringar ur ett tekniskt perspektiv. Dessutom har kommissionen slutfört två översyner av Sirenehandboken sedan 2013, dvs. sedan SIS II togs i bruk den 9 april 2013 och beslut 2007/533/RIF blev tillämpligt. Detta inbegriper en halvtidsöversyn som ledde till att den nya Sirenehandboken[25] offentliggjordes den 29 januari 2015. Kommissionen har också antagit en katalog över bästa praxis och rekommendationer[26]. Dessutom utför eu-LISA och medlemsstaterna regelbundet fortlöpande tekniska förbättringar av systemet. Det anses att dessa alternativ nu har uttömts, och att en mer omfattande ändring av den rättsliga grunden krävs. Klarhet i fråga om exempelvis tillämpningen av slutanvändarsystemen samt närmare

22 Europeiska kommissionens SLUTRAPPORT – SIS II teknisk bedömning.

23 Europeiska kommissionens SLUTRAPPORT – IKT-konsekvensbedömning av möjliga förbättringar av SIS II-arkitekturen 2016.

24 Europeiska kommissionens SLUTRAPPORT – IKT-konsekvensbedömning av de tekniska förbättringarna av SIS II-strukturen – Slutrapport, 10 november 2016 (Wavestone).

25 Kommissionens genomförandebeslut (EU) 2015/219 av den 29 januari 2015 om ändring av bilagan till genomförandebeslut 2013/115/EU om antagande av Sirenehandboken och övriga genomförandeåtgärder avseende andra generationen av Schengens informationssystem (SIS II) (EUT L 44, 18.2.2015, s. 75).

26 Kommissionens rekommendation om upprättande av en katalog över rekommendationer och bästa praxis för korrekt tillämpning av andra generationen av Schengens informationssystem (SIS II) och utbyte av kompletterande information mellan medlemsstaternas behöriga myndigheter som genomför och använder SIS II (C(2015)9169/1).

bestämmelser om radering av registreringar kan inte uppnås enbart genom att förbättra genomförandet och verkställigheten.

Dessutom har kommissionen utfört en övergripande utvärdering av SIS, som krävs enligt 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 lagt fram ett åtföljande arbetsdokument. Resultaten av den övergripande utvärderingen (utvärderingsrapporten och det tillhörande arbetsdokumentet antogs den 21 december 2016) utgör grunden för de åtgärder som ingår i detta förslag.

Den utvärderingsmekanism för Schengenregelverket som fastställs i förordning (EU) nr 1053/2013[27] möjliggör regelbundna rättsliga och operativa utvärderingar av hur SIS fungerar i medlemsstaterna. Utvärderingarna utförs gemensamt av kommissionen och medlemsstaterna. Genom denna mekanism utfärdar rådet rekommendationer till enskilda medlemsstater, baserat på de utvärderingar som utförts som en del av de fleråriga och årliga programmen. Eftersom dessa rekommendationer är individuella kan de inte ersätta rättsligt bindande bestämmelser som är tillämpliga samtidigt i alla medlemsstater som använder SIS.

SISVIS-kommittén diskuterar regelbundet praktiska operativa och tekniska frågor. Även om dessa möten är mycket viktiga för samarbetet mellan kommissionen och medlemsstaterna kan dessa diskussioner (utan lagstiftningsändringar) till exempel inte åtgärda problem som uppstår till följd av varierande nationell praxis.

De ändringar som föreslås i denna förordning har inte några betydande ekonomiska eller miljörelaterade konsekvenser. Ändringarna väntas dock ha en mycket positiv social effekt eftersom de förbättrar säkerheten genom att möjliggöra bättre identifiering av personer som använder falsk identitet, brottslingar som har begått ett grovt brott men vars identitet inte är känd samt försvunna minderåriga. Ändringarnas konsekvenser för de grundläggande rättigheterna och uppgiftsskyddet har beaktats och beskrivs mer i detalj i följande avsnitt (”Grundläggande rättigheter”).

Förslaget har utarbetats med hjälp av en omfattande mängd information som samlats in för att vägleda den övergripande utvärderingen av andra generationen av SIS, där man undersökte systemets funktion och möjliga områden för förbättringar. Dessutom utfördes en bedömning av kostnadseffekterna, för att säkerställa att den nationella struktur som valdes var den lämpligaste och mest proportionerliga.

- **Grundläggande rättigheter och uppgiftsskydd**

Detta förslag syftar till att utveckla och förbättra ett befintligt system, snarare än att skapa ett nytt, och det bygger därför på viktiga och effektiva skyddsåtgärder som redan har inrättats. Trots detta finns det potentiella konsekvenser för enskildas grundläggande rättigheter, eftersom systemet fortsättningsvis behandlar personuppgifter, och kommer att behandla ytterligare kategorier av känsliga biometriska uppgifter. Dessa har övervägts noggrant och fler skyddsåtgärder har införts för att begränsa insamlingen och vidarebehandlingen av uppgifter till vad som är strängt nödvändigt och krävs för den operativa verksamheten, och att begränsa åtkomsten till dessa uppgifter till dem som av operativa orsaker behöver den. I detta förslag fastställs tydliga tidsramar för lagring av uppgifter, bland annat förkortade lagringstider för registreringar om föremål. Det finns ett uttryckligt erkännande av och bestämmelser om

[27] 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).

personers rätt att få åtkomst till uppgifter om sig själva och begära rättelser och radering av uppgifterna i enlighet med de grundläggande rättigheterna (se avsnittet om uppgiftsskydd och säkerhet).

Dessutom stärker förslaget åtgärder som skyddar grundläggande rättigheter, eftersom det anger rättsliga krav på att en registrering ska raderas och inför en proportionalitetsbedömning om lagringstiden för en registrering förlängs. Tillförlitligare identifiering av personer kommer att bli möjlig genom användning av biometriska uppgifter om försvunna personer i behov av skydd, med säkerställande av att personuppgifter är riktiga och skyddade på lämpligt sätt. I förslaget fastställs omfattande och kraftiga skyddsåtgärder för användningen av biometriska kännetecken för att undvika att oskyldiga personer besväras.

Enligt förslaget krävs också genomgående säkerhet för systemet vilket säkerställer ett bättre skydd av de uppgifter som lagras där. Genom införandet av ett tydligt förfarande för hantering av tillbud, samt förbättrad driftskontinuitet för SIS, är detta förslag helt förenligt med Europeiska unionens stadga om de grundläggande rättigheterna[28] vad gäller rätten till skydd av personuppgifter. Utvecklingen av SIS och dess fortsatta effektivitet kommer att bidra till säkerheten för personer i samhället.

Förslaget för med sig betydande ändringar när det gäller biometriska kännetecken. Förutom fingeravtryck bör även handavtryck samlas in och lagras om de rättsliga kraven uppfylls. Fingeravtrycksloggar kopplas till alfanumeriska SIS-registreringar enligt artiklarna 26, 32, 34 och 36. I framtiden bör det vara möjligt att söka dessa finger- och handavtrycksuppgifter utifrån fingeravtryck som hittas på en brottsplats, förutsatt att brottet kan klassas som grov brottslighet eller terrorism och att det kan konstateras att fingeravtrycken med hög sannolikhet tillhör gärningsmannen. Dessutom föreskrivs i förslaget att fingeravtryck ska lagras för så kallade ”okända efterlysta personer” (villkoren beskrivs i detalj i avsnitt 5 underavsnitt "Fotografier, ansiktsbilder, finger- och handavtrycksuppgifter och DNA-profiler”). Om det råder osäkerhet om en persons identitet efter en kontroll av dennas handlingar bör de behöriga myndigheterna göra en sökning av fingeravtryck mot de fingeravtryck som finns lagrade i SIS-databasen.

Enligt förslaget krävs det att man samlar in och lagrar kompletterande uppgifter (såsom detaljer om id-handlingarna) som gör det lättare för tjänstemän på fältet att fastställa en persons identitet.

I förslaget garanteras den registrerades rätt till effektiva rättsmedel för att bestrida beslut, vilka i varje fall ska inbegripa ett effektivt rättsmedel inför domstol i enlighet med artikel 47 i stadgan om de grundläggande rättigheterna.

4. BUDGETKONSEKVENSER

SIS är ett enda informationssystem. Följaktligen bör de beräknade utgifterna för två av förslagen (det föreliggande och förslaget till förordning om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller) inte ses som två separata belopp utan som ett enda. Budgetkonsekvenserna av de ändringar som krävs för genomförandet av bägge förslagen ingår i en finansieringsöversikt för rättsakterna.

På grund av att det tredje förslaget (om återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna) har en kompletterande karaktär behandlas dess budgetkonsekvenser separat och i en fristående finansieringsöversikt som endast gäller inrättandet av denna specifika registreringskategori.

[28] Europeiska unionens stadga om de grundläggande rättigheterna (2012/C 326/02).

På grundval av en bedömning av de olika aspekterna av det arbete som krävs i samband med nätverket, det centrala SIS av eu-LISA och den nationella utvecklingen i medlemsstaterna kommer de två förslagen till förordningar att kräva ett sammanlagt belopp på 64,3 miljoner euro för perioden 2018–2020.

Detta omfattar en ökning av bandbredden för Testa-NG på grund av att nätverket enligt de båda förslagen kommer att överföra filer med fingeravtryck och ansiktsbilder vilket kräver högre genomströmning och kapacitet (9,9 miljoner euro). Det omfattar också eu-LISA:s personal- och driftskostnader (17,6 miljoner euro). eu-LISA har informerat kommissionen om att de planerar att anställa tre nya kontraktsanställda i januari 2018 så att utvecklingsfasen kan inledas i tid för att säkerställa att de uppdaterade funktionerna i SIS tas i bruk under 2020. Det här förslaget innebär tekniska ändringar av det centrala SIS för att utvidga några av de befintliga registreringskategorierna och införa nya funktioner. Dessa ändringar redovisas närmare i den bifogade finansieringsöversikten.

Dessutom har kommissionen utfört en bedömning av kostnadseffekterna för att bedöma kostnaderna för de nationella ändringar som krävs till följd av detta förslag[29]. Den beräknade kostnaden är 36,8 miljoner euro som bör fördelas genom ett engångsbelopp till medlemsstaterna. Varje medlemsstat kommer därför att få ett belopp på 1,2 miljoner euro för att uppgradera sitt nationella system i enlighet med de krav som fastställs i detta förslag, bland annat för inrättande av en partiell nationell kopia om en sådan ännu inte finns eller för ett backupsystem.

En omfördelning av återstoden av anslaget för smarta gränser inom ramen för fonden för inre säkerhet planeras för att genomföra uppgraderingarna och implementera de funktioner som planeras i de båda förslagen. Förordningen om fonden för inre säkerhet och stödet för yttre gränser[30] är det finansieringsinstrument som innehåller budgeten för genomförande av paketet för smarta gränser. Enligt artikel 5 i förordningen ska 791 miljoner euro satsas på ett program för inrättande av it-system till stöd för hanteringen av migrationsströmmar över de yttre gränserna, enligt de villkor som fastställs i artikel 15. Av de 791 miljoner euro som nämns ovan är 480 miljoner euro reserverade för utvecklingen av in- och utresesystemet och 210 miljoner euro för utvecklingen av EU-systemet för reseuppgifter och resetillstånd (Etias). Återstoden kommer att användas delvis för att täcka kostnaderna för de ändringar som planeras i de båda förslagen om SIS.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Kommissionen, medlemsstaterna och eu-LISA kommer regelbundet att se över och övervaka användningen av SIS för att säkerställa att systemet fortsätter att fungera ändamålsenligt och effektivt. Kommissionen kommer att bistås av SISVIS-kommittén vid genomförandet av de tekniska och operativa åtgärder som beskrivs i förslaget.

Dessutom inbegriper denna föreslagna förordning i artikel 71.7 och 71.8 bestämmelser om ett formellt, regelbundet översyns- och utvärderingsförfarande.

---

[29] Wavestone, IKT-konsekvensbedömning av de tekniska förbättringarna av SIS II-strukturen – Slutrapport, 10 november 2016, scenario 3 distinkt implementering av N. SIS II.

[30] Europaparlamentets och rådets förordning (EU) nr 515/2014 av den 16 april 2014 om inrättande, som en del av fonden för inre säkerhet, av ett instrument för ekonomiskt stöd för yttre gränser och visering (EUT L 150, 20.5.2014, s. 143).

Vartannat år måste eu-LISA lämna en rapport till Europaparlamentet och rådet om den tekniska funktionen – bland annat säkerheten – hos SIS, den kommunikationsinfrastruktur som stöder systemet samt det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstaterna.

Dessutom måste kommissionen vart fjärde år genomföra en övergripande utvärdering av SIS och informationsutbytet mellan medlemsstaterna och lämna den till Europaparlamentet och rådet. I utvärderingen kommer man att

- granska uppnådda resultat i förhållande till målen,
- bedöma om de ursprungliga förutsättningarna för systemet fortfarande är aktuella,
- granska hur förordningen tillämpas på det centrala systemet,
- utvärdera det centrala systemets säkerhet,
- utreda konsekvenserna för systemets framtida funktion.

eu-LISA har nu också i uppgift att tillhandahålla daglig, månatlig och årlig statistik om användningen av SIS, för att säkerställa en fortlöpande övervakning av systemet och dess funktion i förhållande till målen.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Bestämmelser som är gemensamma för det här förslaget och förslaget till en förordning om inrättande, drift och användning av SIS på området in- och utresekontroller

- Allmänna bestämmelser (artiklarna 1–3)
- Teknisk utformning och drift av SIS (artiklarna 4–14)
- eu-LISA:s ansvarsområden (artiklarna 15–18)
- Åtkomsträtt och lagringstid för registreringar (artiklarna 43, 46, 48, 50 och 51)
- Allmänna regler för uppgiftsbehandling och uppgiftsskydd (artiklarna 53–70)
- Övervakning och statistik (artikel 71)

Genomgående användning av SIS

SIS är ett oerhört välanvänt och effektivt verktyg för informationsutbyte, med över 2 miljoner slutanvändare vid behöriga myndigheter i hela Europa. Dessa förslag omfattar bestämmelser om den fullständiga genomgående driften av systemet, bland annat det centrala SIS som drivs av eu-LISA, de nationella systemen och slutanvändarapplikationerna. Förslaget beaktar inte bara de centrala och nationella systemen, utan även slutanvändarnas tekniska och operativa behov.

I artikel 9.2 fastställs att slutanvändarna måste få de uppgifter som krävs för att de ska kunna utföra sina uppgifter (i synnerhet alla de uppgifter som krävs för att identifiera den registrerade och att vidta den begärda åtgärden). Där föreskrivs också en gemensam plan för medlemsstaternas tillämpning av SIS, för att säkerställa harmonisering av alla nationella system. Enligt artikel 6 måste varje medlemsstat säkerställa oavbruten tillgång till SIS-uppgifter för slutanvändarna, för att maximera de operativa vinsterna genom att minska risken för driftstopp.

Artikel 10.3 säkerställer att säkerheten vid uppgiftsbehandling även gäller slutanvändarnas uppgiftsbehandling. Enligt artikel 14 är medlemsstaterna skyldiga att säkerställa att personal

som har åtkomst till SIS regelbundet och fortlöpande fortbildas om datasäkerhet och uppgiftsskydd.

Införandet av dessa åtgärder leder till att detta förslag omfattar SIS:s fullständiga genomgående funktion på ett mer omfattande sätt, med bestämmelser och skyldigheter för de miljontals slutanvändarna runtom i Europa. För att utnyttja SIS på effektivaste möjliga sätt bör medlemsstaterna säkerställa att deras slutanvändare varje gång de är berättigade att göra en sökning i en nationell polis- eller immigrationsdatabas parallellt även söker i SIS. På detta sätt kan SIS fylla sin funktion som den främsta kompensationsåtgärden på området utan inre gränskontroller, och medlemsstaterna kan ta itu med den gränsöverskridande dimensionen av brottslighet och brottslingarnas rörlighet på ett bättre sätt. Denna parallella sökning måste ske i överensstämmelse med artikel 4 i direktiv (EU) 2016/680[31].

Driftskontinuitet

Förslagen stärker bestämmelserna om driftskontinuitet, både på nationell nivå och för eu-LISA (artiklarna 4, 6, 7 och 15). Dessa säkerställer att SIS förblir funktionellt och åtkomligt för personal på fältet, även om det uppstår problem som påverkar systemet.

Uppgifternas kvalitet

Förslaget bibehåller principen om att den medlemsstat som äger uppgifterna även är ansvarig för att de uppgifter som läggs in i SIS är korrekta (artikel 56). Det är dock nödvändigt att föreskriva en central mekanism som förvaltas av eu-LISA och som gör det möjligt för medlemsstaterna att regelbundet se över de registreringar där de obligatoriska uppgiftsfälten kan göra att kvaliteten ifrågasätts. Därför bemyndigas eu-LISA i artikel 15 i förslaget att regelbundet tillställa medlemsstaterna rapporter om uppgifternas kvalitet. Denna verksamhet kan underlättas genom en central databas för utarbetande av statistiska rapporter och rapporter om uppgifternas kvalitet (artikel 71). Dessa förbättringar återspeglar de preliminära resultaten från expertgruppen för informationssystem och interoperabilitet.

Fotografier, ansiktsbilder, finger- och handavtrycksuppgifter och DNA-profiler

Möjligheten att göra sökningar med fingeravtryck för att identifiera en person fastställs redan i artikel 22 i förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF. Genom förslagen blir den här sökningen obligatorisk om personens identitet inte kan säkerställas på något annat sätt. Dessutom kommer det genom ändringar av artikel 22 och de nya artiklarna 40, 41 och 42 att bli tillåtet att utöver fingeravtryck även använda ansiktsbilder, handavtryck och DNA-profiler för att identifiera en person. För närvarande kan ansiktsbilder endast användas för att bekräfta en persons identitet efter en sökning med alfanumeriska uppgifter, snarare än att dessa skulle utgöra grunden för en sökning. Daktylografi avser det vetenskapliga studiet av fingeravtryck som en identifieringsmetod. Experter på daktylografi konstaterar att handavtryck har en unik karaktär och innehåller referenspunkter som möjliggör exakta och avgörande jämförelser, precis som fingeravtryck. Handavtryck kan användas för att fastställa en persons identitet på samma sätt som fingeravtryck. Det har i flera årtionden varit polispraxis att ta en persons handavtryck tillsammans med tio rullade och tio platta fingeravtryck. Det finns två huvudsakliga användningsområden för handavtryck, nämligen följande:

[31] 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 (EUT L 119, 4.5.2016, s. 89).

i) Identifiering, då personen med eller utan avsikt har skadat fingertopparna. Detta kan ske genom att man försöker undvika att bli identifierad eller behöva lämna sina fingeravtryck, eller genom skador som orsakats av olyckor eller tungt manuellt arbete. Under diskussionerna om de tekniska bestämmelserna för SIS Afis rapporterade Italien betydande framgångar med identifiering av irreguljära migranter som avsiktligen har skadat sina fingertoppar i ett försök att undvika att bli identifierade. De italienska myndigheterna tog handavtryck, vilket möjliggjorde identifiering.

ii) Latenta avtryck från brottsplatser. Den misstänkta lämnar ofta spår på en brottsplats vilka visar sig komma från handflatan. Det är endast genom att rutinmässigt ta handavtryck när en person är lagligen skyldig att lämna fingeravtryck som den misstänkta kan identifieras. Handavtrycket innehåller vanligen också detaljer från nedre delen av fingrarna, som sällan ingår i de rullade och platta avtryck som tas, eftersom dessa tenderar att fokuseras på fingertopparna och de övre lederna.

Användningen av ansiktsbilder för identifiering kommer att säkerställa bättre överensstämmelse mellan SIS och det föreslagna EU-systemet för in- och utresa, elektroniska spärrar och självbetjäningskiosker. Denna funktion kommer att begränsas till reguljära gränspassager.

Om fingeravtryck eller handavtryck inte finns att tillgå möjliggör artikel 22.1 b användning av DNA-profiler för försvunna personer som behöver ställas under beskydd, särskilt barn. Denna funktion kommer endast att användas om fingeravtryck saknas och kommer bara att kunna användas av behöriga användare. Denna bestämmelse möjliggör alltså användning av DNA-profiler via den försvunna personens eller det försvunna barnets föräldrar eller syskon så att de nationella myndigheterna ska kunna identifiera och lokalisera personen i fråga. Medlemsstaterna utbyter redan denna information med varandra på operativ nivå, genom utbyte av tilläggsinformation. Detta förslag utgör den rättsliga ramen för denna praxis, genom att införa den i den materiella rättsliga grunden för drift och användning av SIS och genom att fastställa tydliga förfaranden för de omständigheter under vilka sådana profiler får användas.

De föreslagna ändringarna kommer också att göra det möjligt att föra in SIS-registreringar för okända personer som är efterlysta i samband med ett brott, på grundval av fingeravtryck eller handavtryck (artiklarna 40–42). Dessa registreringar kan skapas till exempel när latenta fingeravtryck eller handavtryck upptäcks på platsen för ett grovt brott och det finns starka skäl att misstänka att fingeravtrycken tillhör brottets gärningsman. Till exempel när fingeravtryck hittas på ett vapen som användes för att begå brottet eller på något annat föremål som gärningsmannen använde då han eller hon begick brottet. Denna nya registreringskategori kompletterar de Prümbestämmelser som möjliggör sammankoppling av nationella straffrättsliga system för identifiering av fingeravtryck. Via Prümmekanismen kan en medlemsstat skicka en förfrågan för att fastställa om gärningsmannen till ett brott vars fingeravtryck har hittats är känd i någon annan medlemsstat (vanligtvis för utredningändamål). En person kan identifieras via Prümmekanismen endast om han eller hon har lämnat fingeravtryck i en annan medlemsstat i samband med brott. Förstagångsförbrytare kan alltså inte identifieras. Uppdateringarna i detta förslag, dvs. lagring av fingeravtryck från okända efterlysta personer, kommer att göra det möjligt att ladda upp fingeravtrycken från en okänd gärningsman till SIS så att personen kan identifieras som efterlyst om han eller hon påträffas i en annan medlemsstat. Användningen av denna funktion förutsätter att medlemsstaten först har sökt i alla tillgängliga nationella och internationella källor, men inte kunnat fastställa identiteten för personen i fråga. Tillräckliga skyddsåtgärder har tagits med i förslaget för att säkerställa att det i denna kategori i SIS endast lagras fingeravtryck från personer som på starka grunder misstänks ha begått ett grovt brott eller ett terroristbrott.

Följaktligen kan användning av denna nya registreringskategori endast tillåtas i fall då den okända gärningsmannen utgör en stor risk för den allmänna säkerheten, vilket motiverar jämförelse av dessa fingeravtryck med resenärers fingeravtryck, till exempel för att undvika att personen lämnar området utan inre gränskontroller.

Denna bestämmelse tillåter inte slutanvändarna att föra in fingeravtryck i denna kategori om deras koppling till gärningsmannen inte kan fastställas. Ett ytterligare villkor kommer att vara att personens identitet inte kan fastställas genom användning av någon annan nationell, europeisk eller internationell databas med lagrade fingeravtryck. När ett sådant fingeravtryck väl har lagrats i SIS kommer det att användas för att identifiera personer vars identitet inte kan fastställas på annat sätt. Om denna kontroll leder till en potentiell träff bör medlemsstaten utföra ytterligare kontroller med sina fingeravtryck, möjligen med hjälp av fingeravtrycksexperter, för att fastställa om fingeravtrycken tillhör samma person vars avtryck finns lagrade i SIS, och bör fastställa personens identitet. Förfarandena regleras i nationell lagstiftning. En identifiering som en person som registrerats som ”okänd efterlyst person” i SIS kan leda till gripande.

Åtkomst till SIS

I detta underavsnitt beskrivs de nya inslagen i fråga om åtkomsträtt till SIS med avseende på de nationella myndigheterna och EU-organ (institutionella användare).

Nationella myndigheter – immigrationsmyndigheter

För att säkerställa att SIS används på effektivaste möjliga sätt föreskrivs i förslaget åtkomst till SIS för nationella myndigheter som ansvarar för att granska villkor och fatta beslut om tredjelandsmedborgares inresa till, vistelse på och återvändande från medlemsstaternas territorium. Detta tillägg möjliggör sökning i SIS när det gäller irreguljära migranter som inte har kontrollerats vid vanliga gränskontroller. Detta förslag säkerställer en likabehandling av tredjelandsmedborgare som passerar de yttre gränserna vid reguljära gränsövergångsställen (och därför genomgår de kontroller som tillämpas på tredjelandsmedborgare) och tredjelandsmedborgare som anländer till Schengenområdet på ett irreguljärt sätt.

Dessutom säkerställer detta förslag att registreringsmyndigheterna för fordon (artikel 44), fartyg och luftfartyg kommer att ha begränsad åtkomst till systemet för att utföra sina uppgifter, förutsatt att de är statliga myndigheter. Detta kommer att göra det lättare att förhindra registrering av transportmedlen i fråga om de är stulna och söks i andra medlemsstater. Initiativet är inte något nytt för fordonsregistreringstjänsterna eftersom deras åtkomst till SIS föreskrevs redan i artikel 102a i Schengenkonventionen och i förordning (EG) nr 1986/2006[32]. Med samma logik föreskrivs i förslaget åtkomst till SIS-registreringar om fartyg och luftfartyg för de myndigheter som registrerar fartyg och luftfartyg.

Institutionella användare

Europol (artikel 46), Eurojust (artikel 47) och Europeiska gräns- och kustbevakningsbyrån – samt dess enheter, enheter med personal som arbetar med återvändande och medlemmarna i stödgruppen för migrationshantering – (artiklarna 48 och 49) har den åtkomst till SIS och SIS-uppgifter som de behöver. Lämpliga skyddsåtgärder inrättas för att säkerställa att uppgifterna i systemet skyddas ordentligt (bland annat bestämmelserna i artikel 50 om att dessa organ endast har åtkomsträtt till de uppgifter de behöver för att utföra sina uppgifter).

[32] 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).

Dessa ändringar utvidgar Europols åtkomst till SIS till att även omfatta registreringar om försvunna personer, för att säkerställa att byrån kan utnyttja systemet på bästa sätt när den utför sina uppgifter, och lägger till nya bestämmelser som säkerställer att Europeiska gräns- och kustbevakningsbyrån och dess enheter har åtkomst till systemet vid olika insatser för stöd till medlemsstaterna inom ramen för deras mandat. I samband med arbetet inom expertgruppen för informationssystem och interoperabilitet och i syfte att ytterligare stärka informationsutbytet om terrorism kommer kommissionen att bedöma om Europol automatiskt bör få ett meddelande från SIS när en registrering om terrorismrelaterad verksamhet skapas.

I enlighet med kommissionens förslag till Europaparlamentets och rådets förordning om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias)[33] kommer Etias centralenhet inom Europeiska gräns- och kustbevakningsbyrån därtill att göra sökningar i SIS via Etias för att fastställa om den tredjelandsmedborgare som ansöker om ett resetillstånd omfattas av en SIS-registrering. I detta syfte kommer Etias centralenhet också att ha full åtkomst till SIS.

Särskilda ändringar av registreringar

Artikel 26 gör det möjligt för medlemsstaterna att göra en registrering om gripande tillfälligt otillgänglig (under en pågående polisinsats eller utredning), så att den under en begränsad tid endast kan ses av Sirenekontoren och inte av tjänstemän på fältet. Denna bestämmelse gör det lättare att undvika att en konfidentiell polisinsats för gripande av en mycket efterspanad gärningsman äventyras av en polis som inte är involverad i insatsen.

Artiklarna 32 och 33 innehåller bestämmelser om registreringar om försvunna personer. Ändringar av dessa gör det möjligt att föra in förebyggande registreringar i fall där barn bedöms löpa stor risk för att bortföras av en förälder, och att kategorisera registreringar om försvunna personer på ett mer nyanserat sätt. När en förälder bortför sitt barn sker det ofta under väl planerade förhållanden, med avsikten att snabbt lämna den medlemsstat där vårdnadsarrangemangen fastställdes. Dessa ändringar åtgärdar en potentiell lucka i den nuvarande lagstiftningen där registreringar om barn endast kan föras in när de väl är försvunna. Myndigheterna i medlemsstaterna kommer att kunna ange barn som löper en särskild risk. Dessa ändringar innebär att gränsbevakningstjänstemän och tjänstemän inom brottsbekämpning görs medvetna om att det finns en stor och överhängande risk för att en förälder kan bortföra sitt barn, och de kan därför mer i detalj granska omständigheterna när ett barn i riskzonen reser, och vid behov omhänderta barnet. Tilläggsinformation, bland annat om beslutet från den behöriga rättsliga myndighet som begärde registreringen, tillhandahålls via Sirenekontoren. Sirenehandboken kommer att ändras i enlighet med detta. Denna registrering kommer att kräva att rättsliga myndigheter har utfärdat ett tillbörligt beslut om att bevilja vårdnaden till endast en av föräldrarna. Ett ytterligare villkor kommer att vara att det finns en överhängande risk för bortförande. Statusen för registreringar om försvunna barn kommer automatiskt att uppdateras för att återspegla att de uppnått vuxen ålder, när detta är tillämpligt.

Enligt artikel 34 får uppgifter om fordon läggas till registreringen om det finns tydliga tecken på att fordonet har samband med den person som söks.

I artikel 37 införs en ny form av kontroll: ”undersökningskontroll”. Denna är särskilt avsedd för att stödja åtgärder som syftar till att bekämpa terrorism och grov brottslighet. Det gör det möjligt för myndigheterna att stoppa och förhöra den berörda personen. Den är mer djupgående än den befintliga diskreta kontrollen, men involverar ingen kroppsvisitering och

[33] COM(2016) 731 final.

medför inget gripande. Den kan dock ge tillräcklig information för att besluta att ytterligare åtgärder bör vidtas. Artikel 36 ändras också för att återspegla denna nya typ av kontroll.

Detta förslag innehåller bestämmelser om SIS-registreringar om officiella blankodokument och utfärdade id-handlingar (artikel 36) och om fordon, även fartyg och luftfartyg (artiklarna 32 och 34), när dessa har samband med registreringar som förts in om personer enligt dessa artiklar. Artikel 37 ändras för att föreskriva åtgärder som bör vidtas på grundval av dessa registreringar. Syftet är enbart undersökande, eftersom myndigheterna kommer att få möjligheter att hantera situationer där flera personer använder autentiska men snarlika handlingar som de inte är lagliga innehavare till.

I artikel 38 anges en utökad förteckning över föremål för vilka registreringar kan föras in, och där tilläggs förfalskade handlingar, fordon oavsett framdrivningssystem (dvs. både elektriska och bensin/dieseldrivna osv.), förfalskade sedlar, it-utrustning och identifierbara beståndsdelar av fordon och industriell utrustning. Det innehåller inte längre registreringar om betalningsmedel eftersom dessa registreringar har varit mycket ineffektiva och knappt gett några träffar alls.

Artikel 39 ändras för att förtydliga det förfarande som ska följas när ett föremål som omfattas av en registrering har hittats, genom att fastställa att föremål måste beslagtas, i enlighet med nationell lagstiftning, utöver att den myndighet som förde in registreringen måste kontaktas.

Uppgiftsskydd och datasäkerhet

I detta förslag förtydligas vem som har ansvar för att förebygga, rapportera och hantera tillbud som kan påverka säkerheten eller integriteten hos SIS-infrastrukturen, SIS-uppgifterna eller tilläggsinformationen (artiklarna 10, 16 och 57).

Artikel 12 innehåller bestämmelser om loggning och sökning i loggar av registreringshistorik.

Artikel 12 innehåller också bestämmelser om automatiska skanningssökningar av motorfordons nummerplåtar med automatiska nummerplåtsavläsningssystem, vilka förpliktar medlemsstaterna att föra en logg över dessa sökningar i enlighet med nationell lagstiftning.

Genom artikel 15.3 bibehålls artikel 15.3 i rådets beslut 2007/533/RIF och föreskrivs att kommissionen fortfarande ansvarar för avtalsfrågor i samband med kommunikationsinfrastrukturen, bland annat uppgifter som gäller genomförandet av budgeten samt förvärv och förnyande. Dessa uppgifter kommer att överföras till eu-LISA genom den andra serien förslag om SIS i juni 2017.

Genom artikel 21 utvidgas kravet att överväga om ett fall är tillräckligt adekvat, relevant och viktigt till att även omfatta beslut om huruvida giltighetstiden för en registrering bör förlängas. Ett nytillskott i den här artikeln är också kravet på att medlemsstaterna under alla omständigheter skapar en registrering enligt artiklarna 34, 36 och 38 (efter tillämplighet) om de personer eller relaterade föremål vars verksamhet omfattas av artiklarna 1, 2, 3 och 4 i rådets rambeslut 2002/475/RIF om bekämpande av terrorism.

Kategorier av uppgifter och uppgiftsbehandling

Genom detta förslag utvidgas de typer av information (artikel 20) som kan lagras om personer som omfattas av en registrering till att även inbegripa

- uppgifter om personen är involverad i någon verksamhet som omfattas av artiklarna 1, 2, 3 och 4 i rådets rambeslut 2002/475/RIF,
- andra personliga kommentarer, syftet med registreringen,
- uppgifter om personens nationella registreringsnummer och registreringsort,

- kategorisering av typen av försvinnande (endast registreringar om försvunna personer enligt artikel 32),
- uppgifter om en persons id- eller resehandlingar,
- färgkopia av personens id- eller resehandlingar,
- DNA-profiler (endast om fingeravtryck som lämpar sig för identifiering inte är tillgängliga).

I artikel 59 utökas förteckningen över de personuppgifter som får läggas in och behandlas i SIS i syfte att komma till rätta med missbruk av identitet. Dessa uppgifter kan endast läggas in med medgivande från den person vars identitet har missbrukats. Dessa kommer nu även att omfatta

- ansiktsbilder,
- handavtryck,
- uppgifter om identitetshandlingar,
- offrets adress,
- namn på offrets far och mor.

I artikel 20 föreskrivs mer detaljerad information i registreringarna. Den inbegriper uppgifter om de registrerades id-handlingar och gör det möjligt att kategorisera försvunna barn enligt deras försvinnande, såsom ensamkommande barn, barn som blivit bortförda av en förälder, barn som rymt osv. Detta är väsentligt för att slutanvändarna utan dröjsmål ska kunna vidta de åtgärder som krävs för att skydda barnen. Den utökade informationen gör det lättare att identifiera den berörda personen och lättare för slutanvändarna att fatta ett mer välgrundat beslut. För att skydda de slutanvändare som utför kontrollerna kommer SIS också att visa om den person för vilken en registrering har förts in omfattas av någon av de kategorier som avses i artiklarna 1, 2, 3 och 4 i rådets rambeslut 2002/475/RIF om bekämpande av terrorism[34].

Förslaget klargör att medlemsstaterna inte får kopiera uppgifter som lagts in av en annan medlemsstat till andra nationella dataregister (artikel 53).

Lagring

Den längsta tillåtna lagringstiden för registreringar om personer förlängs till fem år, förutom för registreringar om diskreta eller särskilda kontroller eller undersökningskontroller, vars lagringstid förblir ett år. Medlemsstaterna kan alltid fastställa kortare giltighetstider. Den förlängda maximala giltighetstiden följer nationell praxis att förlänga giltighetstiden om en registrering ännu inte har uppfyllt sitt ändamål och personen i fråga fortfarande är efterlyst. Dessutom var det nödvändigt att samordna SIS med den lagringstid som föreskrivs i andra instrument, såsom återvändandedirektivet och Eurodac. För transparens och tydlighet är det nödvändigt att föreskriva samma lagringstid för registreringar om personer, förutom registreringar som skapats för diskreta eller särskilda kontroller eller undersökningskontroller. Förlängningen av lagringstiden äventyrar inte de registrerades intressen eftersom en registrering inte kan sparas längre än vad som är nödvändigt för dess ändamål. Bestämmelser om radering av registreringar fastställs uttryckligen i artikel 52. I artikel 51 fastställs

[34] Rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3).

tidsramarna för översyn av registreringar, i synnerhet en förkortad lagringstid för registreringar om föremål. Eftersom det inte finns några operativa behov av att bibehålla den längre perioden för föremål har den nu förkortats till fem år så att den överensstämmer med lagringstiden för registreringar om personer. Lagringstiden för utfärdade handlingar och blankodokument är dock fortfarande 10 år, eftersom giltighetstiden för sådana handlingar är 10 år.

Radering

I artikel 52 anges de omständigheter under vilka registreringar måste raderas, för att bättre harmonisera den nationella praxisen på detta område. I artikel 51 anges särskilda bestämmelser för personal vid Sirenekontoren att proaktivt radera registreringar som inte längre behövs om inget svar inkommer från de behöriga myndigheterna.

Registrerades rätt att få åtkomst till uppgifter, rätta oriktiga uppgifter och radera olagligt lagrade uppgifter

De närmare bestämmelserna om registrerades rättigheter förblir oförändrade eftersom de befintliga bestämmelserna redan säkerställer en hög skyddsnivå och är i linje med förordning (EU) 2016/679[35] och direktiv 2016/680[36]. Utöver detta fastställs i artikel 63 de omständigheter under vilka medlemsstaterna får besluta att inte överlämna information till de registrerade. Detta måste ske av ett av de skäl som anges i denna artikel, och det måste vara en proportionerlig och nödvändig åtgärd som är förenlig med nationell lagstiftning.

Utbyte av uppgifter om förkomna, stulna, ogiltigförklarade eller bortförda handlingar med Interpol

Genom artikel 63 bibehålls artikel 55 i rådets beslut 2007/533/RIF i sin helhet, eftersom bättre interoperabilitet mellan dokumentsektionen i SIS och Interpols databas om stulna och förkomna handlingar kommer att behandlas i expertgruppens meddelande och i den andra serien förslag om SIS i juni 2017.

Statistik

För att få en överblick av hur rättsmedel fungerar i praktiken föreskrivs i artikel 66 ett standardiserat statistiskt system med årliga rapporter om antalet

- ansökningar om åtkomst från de registrerade,
- begäranden om rättelse av oriktiga uppgifter och radering av olagligt lagrade uppgifter,
- ärenden prövade i domstol,
- ärenden där domstolen gav sökanden rätt, och
- uppgifter om ärenden med ömsesidigt erkännande av slutliga avgöranden som meddelats av en domstol eller myndighet i andra medlemsstater om registreringar som skapats av den registrerande staten.

---

35 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 dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

36 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 (EUT L 119, 4.5.2016, s. 89).

Övervakning och statistik

I artikel 71 anges de arrangemang som måste göras för att säkerställa korrekt övervakning av SIS och dess funktion i förhållande till dess mål. För att göra detta får eu-LISA till uppgift att tillhandahålla daglig, månatlig och årlig statistik om hur systemet används.

Artikel 71.5 kräver att eu-LISA tillställer medlemsstaterna, kommissionen, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån de statistiska rapporter som den utarbetar och tillåter kommissionen att begära ytterligare statistiska rapporter och rapporter om uppgifternas kvalitet med avseende på SIS och Sirenekommunikation.

I artikel 71.6 föreskrivs skapande och underhåll av en central databas för uppgifter, som en del av eu-LISA:s arbete med att övervaka hur SIS fungerar. Detta kommer att göra det möjligt för behörig personal från medlemsstaterna, kommissionen, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån att få åtkomst till de uppgifter som anges i artikel 71.3 för att utarbeta den statistik som krävs.

2016/0409 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring av förordning (EU) nr 515/2014 och om upphävande av förordning (EG) nr 1986/2006, rådets beslut 2007/533/RIF 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 led 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, och

av följande skäl:

(1) Schengens informationssystem (SIS) är ett grundläggande verktyg för tillämpningen av bestämmelserna i Schengenregelverket, såsom det införlivats i Europeiska unionens ramar. SIS är en av de centrala kompensationsåtgärder som bidrar till att upprätthålla en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i Europeiska unionen genom att stödja det operativa samarbetet mellan gränsbevakningstjänstemän, polis- och tullmyndigheter samt andra brottsbekämpande och rättsliga myndigheter i straffrättsliga frågor.

(2) SIS inrättades 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 gradvist avskaffande av kontroller vid de gemensamma gränserna[37] (Schengenkonventionen). Kommissionen fick i uppdrag att utveckla andra generationen av SIS (SIS II) genom rådets förordning (EG) nr 2424/2001[38] och rådets beslut 2001/886/RIF[39] och systemet inrättades genom förordning (EG) nr 1987/2006[40]

---

37 EGT L 239, 22.9.2000, s. 19. Konventionen ändrad genom Europaparlamentets och rådets förordning (EG) nr 1160/2005 (EUT L 191, 22.7.2005, s. 18).

38 EGT L 328, 13.12.2001, s. 4.

39 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).

40 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).

samt rådets beslut 2007/533/RIF[41]. SIS II ersatte det SIS som inrättades genom Schengenkonventionen.

(3) Tre år efter det att SIS II togs i bruk utförde kommissionen en utvärdering av systemet i enlighet med artiklarna 24.5, 43.5 och 50.5 i förordning (EG) nr 1987/2006 och artiklarna 59 och 65.5 i beslut 2007/533/RIF. Utvärderingsrapporten och det tillhörande arbetsdokumentet antogs den 21 december 2016[42]. Denna förordning bör, i tillämpliga fall, återspegla rekommendationerna i dessa dokument.

(4) Denna förordning utgör den rättsliga grund som krävs för styrning av SIS avseende aspekter som omfattas av kapitlen 4 och 5 i avdelning V i fördraget om Europeiska unionens funktionssätt. Europaparlamentets och rådets förordning (EU) 2018/... om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller[43] utgör den rättsliga grund som krävs för styrning av SIS avseende aspekter som omfattas av kapitel 2 i avdelning V i fördraget om Europeiska unionens funktionssätt.

(5) Det faktum att den rättsliga grund som krävs för styrning av SIS består av separata instrument påverkar inte principen att SIS är ett enda informationssystem som bör fungera som ett enda system. Vissa av bestämmelserna i dessa instrument bör därför vara identiska.

(6) Det är nödvändigt att ange målen för SIS, dess tekniska utformning och finansiering, fastställa bestämmelser om den genomgående driften och användningen av systemet samt bestämma ansvarsfördelningen, vilka typer av uppgifter som ska läggas in i systemet och ändamålen med att uppgifterna ska läggas in samt kriterier för sådant inläggande, vilka myndigheter som ska ha åtkomst till uppgifterna, hur biometriska kännetecken ska användas samt närmare bestämmelser om behandling av uppgifter.

(7) SIS omfattar ett centralt system (det centrala SIS) och nationella system med en fullständig eller partiell kopia av SIS-databasen. Med tanke på att SIS är det viktigaste instrumentet för informationsutbyte i Europa är det nödvändigt att säkerställa att det fungerar utan avbrott både på central och på nationell nivå. Därför bör varje medlemsstat upprätta en fullständig eller partiell kopia av SIS-databasen, och inrätta ett eget backupsystem.

(8) Det är nödvändigt att upprätthålla en handbok med närmare bestämmelser om utbytet av den tilläggsinformation som krävs för åtgärder påkallade av registreringen. Nationella myndigheter i varje medlemsstat (Sirenekontoren) bör säkerställa utbytet av denna information.

(9) För att upprätthålla ett effektivt utbyte av tilläggsinformation om den åtgärd som enligt registreringen ska vidtas är det lämpligt att stärka Sirenekontorens verksamhet genom att specificera kraven på tillgängliga resurser, fortbildning för användare och svarstiderna för förfrågningar från andra Sirenekontor.

---

41 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).

42 Rapport till Europaparlamentet och rådet 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. (EUT...).

43 Förordning (EU) 2018/…

(10) Den operativa förvaltningen av de centrala delarna av SIS sköts av Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa[44] (nedan kallad *byrån*). För att byrån ska kunna avdela de finansiella resurser och personalresurser som behövs för alla aspekter av den operativa förvaltningen av det centrala SIS bör dess uppgifter fastställas i detalj i denna förordning, i synnerhet när det gäller de tekniska aspekterna av utbytet av tilläggsinformation.

(11) Utan att det påverkar medlemsstaternas ansvar för att de uppgifter som läggs in i SIS är korrekta bör byrån ges ansvaret för att förbättra uppgifternas kvalitet genom att införa ett centralt kvalitetskontrollverktyg, och för att regelbundet tillställa medlemsstaterna rapporter.

(12) I syfte att möjliggöra bättre övervakning av användningen av SIS för att analysera tendenser i fråga om brott bör byrån kunna utveckla en avancerad kapacitet för statistisk rapportering till medlemsstaterna, kommissionen, Europol och Europeiska gräns- och kustbevakningsbyrån utan att äventyra dataintegriteten. Därför bör en central statistikdatabas inrättas. Den statistik som framställs bör inte innehålla personuppgifter.

(13) SIS bör innehålla ytterligare uppgiftskategorier för att göra det möjligt för slutanvändarna att utan dröjsmål fatta välgrundade beslut utifrån en registrering. I syfte att underlätta identifieringen av personer och att upptäcka om flera identiteter används bör de uppgiftskategorier som avser personer därför inbegripa en hänvisning till id-handlingen eller personnumret och om möjligt en kopia av denna handling.

(14) I SIS bör man inte lagra några uppgifter som används för sökning, med undantag av loggar för att kontrollera att sökningen är laglig, övervaka att uppgifterna behandlas på ett lagligt sätt, utföra egenkontroll och säkerställa att N.SIS fungerar på ett korrekt sätt, samt för dataintegritet och datasäkerhet.

(15) SIS bör möjliggöra behandling av biometriska uppgifter för att bidra till tillförlitlig identifiering av berörda personer. SIS bör också möjliggöra behandling av uppgifter om personer vars identitet missbrukats (för att undvika problem orsakade av felidentifiering) men det bör fastställas särskilda skyddsåtgärder för detta, särskilt den berörda personens medgivande och en sträng begränsning av de ändamål för vilka sådana uppgifter lagligen får behandlas.

(16) Medlemsstaterna bör göra de nödvändiga tekniska arrangemangen så att en slutanvändare som gör en berättigad sökning i en nationell polis- eller immigrationsdatabas varje gång parallellt även söker i SIS, i enlighet med artikel 4 i Europaparlamentets och rådets direktiv (EU) 2016/680[45]. Detta bör säkerställa att SIS fungerar som den främsta kompensationsåtgärden på området utan inre gränskontroller och bättre beaktar den gränsöverskridande dimensionen av brottslighet och brottslingarnas rörlighet.

(17) I denna förordning bör det fastställas villkor för användning av finger- och handavtrycksuppgifter och ansiktsbilder för identifiering. Användningen av

---

44 Inrättad genom Europaparlamentets och rådets förordning (EU) nr 1077/2011 av den 25 oktober 2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 286, 1.11.2011, s. 1).

45 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).

ansiktsbilder för identifiering i SIS bör också bidra till att säkerställa enhetlighet vid de gränskontrollförfaranden där identifiering och identitetskontroll krävs genom användning av fingeravtryck och ansiktsbilder. Sökning med finger- och handavtrycksuppgifter bör vara obligatorisk om det råder något som helst tvivel om en persons identitet. Ansiktsbilder bör användas för identifiering endast i samband med vanliga gränskontroller i självbetjäningskiosker och elektroniska spärrar.

(18) 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[46]. Prümmekanismen möjliggör sammankoppling av nationella system för identifiering av fingeravtryck så att en medlemsstat kan skicka en förfrågan för att fastställa om gärningsmannen till ett brott vars fingeravtryck har hittats är känd i någon annan medlemsstat. Genom Prümmekanismen kan man kontrollera om den person som fingeravtrycken tillhör är känd vid en viss tidpunkt, men om gärningsmannen blir känd i någon medlemsstat efteråt kommer denna alltså inte nödvändigtvis att gripas. Fingeravtryckssökningen i SIS möjliggör ett aktivt sökande efter gärningsmannen. Därför bör det vara möjligt att ladda upp en okänd gärningsmans fingeravtryck i SIS, förutsatt att det med stor sannolikhet kan fastställas att den person som fingeravtrycken tillhör har begått ett grovt brott eller en terroristhandling. Detta gäller speciellt om fingeravtrycken hittas på ett vapen eller något annat föremål som har använts för brottet. Blotta förekomsten av fingeravtryck på brottsplatsen bör inte anses tyda på en stor sannolikhet att fingeravtrycken tillhör gärningsmannen. En ytterligare förutsättning för skapandet av en sådan registrering bör vara att gärningsmannens identitet inte kan fastställas via några andra nationella, europeiska eller internationella databaser. Om en sådan fingeravtryckssökning leder till en potentiell träff bör medlemsstaten utföra ytterligare kontroller med sina fingeravtryck, möjligen med hjälp av fingeravtrycksexperter, för att fastställa om fingeravtrycken tillhör den person vars avtryck finns lagrade i SIS och bör fastställa personens identitet. Förfarandena bör regleras i nationell lagstiftning. En identifiering av en person som registrerats som ”okänd efterlyst person” i SIS kan bidra till utredningen på ett betydande sätt och kan leda till gripande, förutsatt att alla villkor för ett gripande är uppfyllda.

(19) Det bör vara tillåtet att kontrollera fingeravtryck som hittas på en brottsplats mot fingeravtryck som lagrats i SIS om det med stor sannolikhet kan fastställas att de tillhör den person som begått det grova brottet eller terroristbrottet. Grov brottslighet bör definieras som de brott som anges i rådets rambeslut 2002/584/RIF[47] och terroristbrott som de brott enligt nationell lagstiftning som avses i rådets rambeslut 2002/475/RIF[48].

(20) Det bör vara möjligt att lägga till en DNA-profil i fall där inga finger- och handavtrycksuppgifter finns att tillgå, och den bör endast vara tillgänglig för behöriga

---

46 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) och 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).

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

48 Rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3).

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 föräldrars och syskons DNA-profiler för identifiering. DNA-uppgifterna bör inte innehålla några hänvisningar till ras.

(21) 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 som behövs för överlämnande- och utlämningsförfaranden. De uppgifter som avses i artikel 8 i rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna[49] bör i synnerhet behandlas i SIS. Av operativa orsaker 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 inte vara tillfälligt otillgängliga längre än 48 timmar.

(22) Det bör vara möjligt att i SIS lägga till en översättning av de kompletterande uppgifter som läggs in för överlämnande enligt den europeiska arresteringsordern och för utlämning.

(23) SIS bör innehålla registreringar om försvunna personer för att säkerställa deras säkerhet eller förebygga hot mot den allmänna säkerheten. Införandet av en registrering i SIS för barn som löper risk för bortförande (dvs. för att förhindra framtida skador som ännu inte har skett, t.ex. för barn som löper risk för att bortföras av en förälder) bör vara begränsat, och det är därför lämpligt att införa stränga och lämpliga skyddsåtgärder. När det gäller barn bör dessa registreringar och motsvarande förfaranden tjäna barnets bästa med beaktande av artikel 24 i Europeiska unionens stadga om de grundläggande rättigheterna och Förenta nationernas konvention om barnets rättigheter av den 20 november 1989.

(24) En ny åtgärd bör införas för fall av misstänkt terrorism och grov brottslighet för att göra det möjligt att stoppa och förhöra en person som misstänks ha begått ett grovt brott eller en person som det finns orsaker att misstänka kommer att begå ett grovt brott, så att den registrerande medlemsstaten ska få så noggranna uppgifter som möjligt. Denna nya åtgärd bör inte innebära att personen vare sig kroppsvisiteras eller grips. Den bör dock ge tillräckligt mycket information för att besluta om ytterligare åtgärder. Grova brott bör vara de brott som förtecknas i rådets rambeslut 2002/584/RIF.

(25) SIS bör innehålla nya kategorier för föremål med högt värde, såsom elektronisk och teknisk utrustning som kan identifieras och sökas med ett unikt nummer.

(26) 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 det gäller registreringar 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

[49] Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (EGT L 190, 18.7.2002, s. 1).

registrering med flaggning bör fattas endast på grundval av de skäl för vägran som anges i rambeslutet.

(27) 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.

(28) Medlemsstaterna bör ha möjlighet att länka samman olika registreringar i SIS. Det faktum att en medlemsstat länkar samman två eller flera registreringar bör inte påverka den åtgärd som ska vidtas, lagringstiden eller åtkomsträtten till registreringarna.

(29) Registreringar bör inte bevaras i SIS längre än vad som är nödvändigt för att uppnå det ändamål för vilket de fördes in. För att minska den administrativa bördan för de olika myndigheter som för olika ändamål behandlar uppgifter om personer är det lämpligt att anpassa lagringstiden för registreringar om personer till de lagringstider som planeras för återvändande och olagliga vistelser. Dessutom förlänger medlemsstaterna regelbundet giltighetstiden för registreringar om personer om den begärda åtgärden inte kunde vidtas inom den ursprungliga tidsfristen. Därför bör lagringstiden för registreringar om personer vara högst fem år. Den allmänna principen bör vara att registreringar om personer automatiskt raderas från SIS efter en period på fem år, förutom när det gäller registreringar som förts in för diskreta och särskilda kontroller samt undersökningskontroller. Dessa bör raderas efter ett år. Registreringar om föremål som har lagts in för diskreta kontroller, undersökningskontroller eller särskilda kontroller bör automatiskt raderas från SIS efter ett år, eftersom de alltid är kopplade till personer. Registreringar om föremål som ska beslagtas eller användas som bevis i brottmål bör automatiskt raderas från SIS efter fem år, eftersom sannolikheten att hitta dem efter en sådan period är mycket låg och deras ekonomiska värde har minskat markant. Registreringar om utfärdade id-handlingar och blankodokument bör behållas i 10 år, eftersom giltighetstiden för sådana handlingar är 10 år från det att de utfärdats. Beslut om att behålla registreringar om personer bör grundas på en övergripande individuell bedömning. Medlemsstaterna bör se över registreringar om personer inom översynsperioden och föra statistik över antalet registreringar om personer för vilka lagringstiden har förlängts.

(30) Inläggande av och förlängning av giltighetstiden för en registrering i SIS bör vara föremål för nödvändiga proportionalitetskrav, med bedömning av om ett visst fall är tillräckligt adekvat, relevant och viktigt för att en registrering ska föras in i SIS. De brott som avses i artiklarna 1, 2, 3 och 4 i rådets rambeslut 2002/475/RIF om bekämpande av terrorism[50] utgör ett mycket allvarligt hot mot den allmänna säkerheten och livsintegriteten för individer och för samhället, och dessa brott är extremt svåra att förhindra, upptäcka och utreda inom ett område utan inre gränskontroller där potentiella förbrytare kan röra sig fritt. Om en person eller ett föremål söks i samband med dessa brott är det alltid nödvändigt att skapa en motsvarande registrering i SIS om personer som söks för ett straffrättsligt förfarande, om personer eller föremål som är föremål för diskreta kontroller, undersökningskontroller och särskilda kontroller samt om föremål som ska beslagtas, eftersom ingen annan åtgärd skulle vara lika effektiv för detta ändamål.

[50] Rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3).

(31) Det är nödvändigt att ge klarhet om radering av registreringar. En registrering bör inte lagras längre än vad som är nödvändigt för att uppnå det ändamål för vilket den lagts in. Eftersom medlemsstaterna har olika praxis när det gäller att fastställa hur länge en registrering är ändamålsenlig är det lämpligt att ange närmare kriterier för varje registreringskategori för att kunna avgöra när den bör raderas ur SIS.

(32) 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 vara föremål för ett enhetligt förfarande för rapportering av tillbud.

(33) De uppgifter som behandlas i SIS i enlighet med denna förordning bör inte överföras eller göras tillgängliga för tredjeländer eller för internationella organisationer. Samarbetet mellan Europeiska unionen och Interpol bör emellertid stärkas genom främjande av effektivt utbyte av passuppgifter. I de fall då personuppgifter överförs från SIS till Interpol bör det sörjas för lämpligt skydd för personuppgifterna och skyddet bör fastställas i ett avtal, där det föreskrivs strikta skyddsåtgärder och villkor.

(34) Det är lämpligt att bevilja åtkomst till SIS för myndigheter som ansvarar för registrering av fordon, fartyg och luftfartyg för att de ska kunna kontrollera om transportmedlet redan söks i en medlemsstat för beslagtagande eller kontroll. Direktåtkomst bör beviljas statliga myndigheter. Denna åtkomst bör begränsas till registreringar om respektive transportmedel och deras registreringsbevis eller nummerplåt. Följaktligen bör bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 1986/2006[51] införlivas i denna förordning och den förordningen bör upphävas.

(35) De nationella bestämmelser som införlivar direktiv (EU) 2016/680 bör tillämpas när de behöriga nationella myndigheterna behandlar uppgifter för att förebygga, utreda och upptäcka grova brott eller terroristbrott, eller att lagföra brott och verkställa straffrättsliga påföljder, inbegripet skyddsåtgärder för att förebygga hot mot den allmänna säkerheten. Bestämmelserna i Europaparlamentets och rådets förordning (EU) 2016/679[52] och direktiv (EU) 2016/680 bör specificeras ytterligare i denna förordning i tillämpliga fall.

(36) Förordning (EU) 2016/679 bör tillämpas på de nationella myndigheternas behandling av personuppgifter enligt denna förordning i de fall då direktiv (EU) 2016/680 inte är tillämpligt. Europaparlamentets och rådets förordning (EG) nr 45/2001[53] bör tillämpas på unionsinstitutionernas och unionsorganens behandling av personuppgifter när de fullgör sina skyldigheter enligt denna förordning.

(37) Bestämmelserna i direktiv (EU) 2016/680, förordning (EU) 2016/679 och förordning (EG) nr 45/2001 bör specificeras ytterligare i denna förordning i tillämpliga fall. När

---

[51] 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).

[52] 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 dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

[53] 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).

det gäller Europols behandling av personuppgifter tillämpas förordning (EU) 2016/794 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europolförordningen)[54].

(38) Bestämmelserna i beslut 2002/187/RIF av den 28 februari 2002[55] om inrättande av Eurojust för att stärka kampen mot grov brottslighet tillämpas i fråga om uppgiftsskydd på Eurojusts behandling av uppgifter i SIS, inbegripet befogenheterna för den gemensamma tillsynsmyndighet som inrättats genom det beslutet för övervakning av Eurojusts verksamhet och dess ansvar för eventuell olaglig behandling av personuppgifter. I fall där en sökning som Eurojust utför i SIS visar att det finns en registrering som förts in av en medlemsstat kan Eurojust inte vidta de åtgärder som begärs. Därför bör Eurojust meddela den berörda medlemsstaten så att den kan följa upp ärendet.

(39) När det gäller sekretess bör relevanta bestämmelser i tjänsteföreskrifterna för tjänstemän i Europeiska unionen och anställningsvillkoren för övriga anställda i Europeiska unionen tillämpas på tjänstemän och övriga anställda vars arbete har samband med SIS.

(40) Såväl medlemsstaterna som byrån bör upprätthålla säkerhetsplaner för att underlätta genomförandet av säkerhetsskyldigheterna och bör samarbeta med varandra så att de behandlar säkerhetsfrågor ur ett gemensamt perspektiv.

(41) De nationella oberoende tillsynsmyndigheterna bör övervaka att medlemsstaternas behandling av personuppgifter sker på ett lagligt sätt enligt denna förordning. Man bör fastställa den registrerades rätt till åtkomst till, rättelse och radering av sina personuppgifter som finns lagrade i SIS och påföljande rättsmedel inför nationella domstolar samt det ömsesidiga erkännandet av domar. Därför är det lämpligt att kräva årlig statistik från medlemsstaterna.

(42) Tillsynsmyndigheterna bör säkerställa att en revision av behandlingen av uppgifter i N.SIS genomförs minst vart fjärde år i enlighet med internationella revisionsstandarder. Antingen bör revisionen utföras av tillsynsmyndigheterna, eller så bör de nationella tillsynsmyndigheterna begära revisionen direkt från en oberoende uppgiftsskyddsrevisor. Den oberoende revisorn bör kvarstå under den nationella tillsynsmyndighetens eller tillsynsmyndigheternas kontroll och ansvar, och dessa bör därför själv begära revisionen och ange en tydligt fastställd avsikt, omfattning och metod för revisionen samt vägledning och tillsyn avseende den och slutresultatet.

(43) I förordning (EU) 2016/794 (Europolförordningen) fastställs att Europol stöder och stärker medlemsstaternas behöriga myndigheters insatser och deras samarbete vad gäller bekämpning av terrorism och grov brottslighet, samt tillhandahåller analyser och hotbildsbedömningar. Utvidgningen av Europols åtkomsträtt till SIS-registreringar om försvunna personer bör ytterligare förbättra Europols förmåga att ge nationella brottsbekämpande myndigheter omfattande operativa och analytiska produkter om människohandel och sexuellt utnyttjande av barn, även online. Detta skulle bidra till bättre förebyggande av dessa brott, skydd av potentiella offer och till utredningen om

---

[54] 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, 25.5.2016, s. 53).

[55] Rådets beslut 2002/187/RIF av den 28 februari 2002 om inrättande av Eurojust för att stärka kampen mot grov brottslighet (EGT L 63, 6.3.2002, s. 1).

gärningsmännen. Europeiska it-brottscentrumet vid Europol skulle också gynnas av Europols nya åtkomst till SIS-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. Dessutom bör Europeiska centrumet för bekämpning av människosmuggling vid Europol på grund av sin viktiga strategiska roll med att förhindra underlättande av irreguljär migration få åtkomst till registreringar om personer som nekas inresa eller vistelse inom en medlemsstats territorium antingen på grundval av brott eller bristande efterlevnad med villkoren för visering och uppehållstillstånd.

(44) För att överbrygga klyftan i utbytet av information om terrorism, i synnerhet om utländska terroristtridande – där övervakningen av deras rörlighet är avgörande – bör medlemsstaterna dela information om terrorismrelaterad verksamhet med Europol parallellt med att de för in en registrering i SIS, samt om träffar och relaterad information. Detta bör ge det europeiska centrumet mot terrorism vid Europol möjlighet att kontrollera om det finns några ytterligare kontextuella uppgifter tillgängliga i Europols databaser och att leverera högkvalitativa analyser som bidrar till att störa terroristnätverk och, om möjligt, förhindra deras attacker.

(45) Det är också nödvändigt att fastställa klara bestämmelser för Europol om behandling och nedladdning av SIS-uppgifter för att möjliggöra en så omfattande användning av SIS som möjligt, förutsatt att standarder om uppgiftsskydd respekteras enligt 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 så att den kan följa upp ärendet.

(46) I Europaparlamentets och rådets förordning (EU) 2016/1624[56] föreskrivs att värdmedlemsstaten vid tillämpning av den förordningen bör tillåta medlemmar i de europeiska gräns- och kustbevakningsenheterna eller i enheter med personal som arbetar med återvändande vilka utplaceras av Europeiska gräns- och kustbevakningsbyrån att göra sådana sökningar i europeiska databaser som är nödvändiga för att uppfylla operativa mål som anges i den operativa planen för gränskontroller, gränsbevakning och återvändande. Andra berörda unionsbyråer – särskilt Europeiska stödkontoret för asylfrågor och Europol – får också utplacera experter som inte är anställda vid de unionsbyråerna för att dessa ska delta i stödgrupper för migrationshantering. Målet med utplaceringen av de europeiska gräns- och kustbevakningsenheterna, enheterna som arbetar med återvändande och stödgruppen för migrationshantering är att ge tekniskt och operativt stöd till begärande medlemsstater, särskilt de som står inför oproportionerligt stora migrationsutmaningar. För att det ska gå att genomföra de arbetsuppgifter som tilldelats de europeiska gräns- och kustbevakningsenheterna, enheterna som arbetar med återvändande och stödgruppen för migrationshantering krävs åtkomst till SIS via ett tekniskt gränssnitt som kopplar Europeiska gräns- och kustbevakningsbyrån till det centrala SIS. I fall där en sökning som enheterna utför i SIS visar att det finns en registrering som förts in av en medlemsstat kan medlemmen av enheten eller personalen inte vidta de åtgärder

[56] 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).

som begärs, om personen inte getts befogenhet att göra detta av värdmedlemsstaten. Därför bör enheten meddela den berörda medlemsstaten så att den kan följa upp ärendet.

(47) I enlighet med kommissionens förslag till Europaparlamentets och rådets förordning om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias)[57] kommer Etias centralenhet inom Europeiska gräns- och kustbevakningsbyrån att kontrollera SIS via Etias för att göra en bedömning av ansökningar om resetillstånd som bland annat kräver att man fastställer om den tredjelandsmedborgare som ansöker om ett resetillstånd omfattas av en SIS-registrering. I detta syfte bör Etias centralenhet inom Europeiska gräns- och kustbevakningsbyrån också ha åtkomst till SIS i den utsträckning som behövs för att den ska kunna utföra sitt mandat, dvs. alla registreringskategorier om personer och registreringar om blankodokument och utfärdade id-handlingar.

(48) Vissa aspekter av SIS kan inte täckas på ett uttömmande sätt av bestämmelserna i denna förordning på grund av deras tekniska beskaffenhet, detaljnivå och behov av regelbunden uppdatering. Hit hör bland annat tekniska bestämmelser för att lägga in, uppdatera, radera och söka uppgifter, uppgifternas kvalitet och bestämmelser om sökning med biometriska kännetecken, bestämmelser om överensstämmelse och prioritering av registreringar, tillägg av flaggning, länkar mellan registreringar, fastställande av nya kategorier av föremål inom kategorin teknisk och elektronisk utrustning, fastställande av giltighetstiden för registreringar inom den längsta tillåtna tidsfristen och utbyte av tilläggsinformation. Genomförandebefogenheterna för dessa aspekter bör därför tilldelas kommissionen. Tekniska föreskrifter för sökning i registreringar bör ta hänsyn till att de nationella tillämpningarna ska fungera smidigt.

(49) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med förordning (EU) nr 182/2011[58]. Förfarandet för antagande av genomförandeåtgärderna bör vara det samma för denna förordning och för förordning (EU) 2018/xxx (in- och utresekontroller).

(50) För att säkerställa öppenhet bör byrån vartannat år utarbeta en rapport om den tekniska funktionen för det centrala SIS och kommunikationsinfrastrukturen, inklusive säkerheten i denna, och om utbytet av tilläggsinformation. Kommissionen bör lägga fram en övergripande utvärdering vart fjärde år.

(51) Eftersom målen för denna förordning, nämligen att inrätta och reglera ett gemensamt informationssystem och utbytet av relaterad tilläggsinformation, genom själva sin beskaffenhet inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och de därför bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

(52) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna. Denna förordning syftar i synnerhet till att säkerställa en trygg miljö för alla personer

[57] COM(2016) 731 final.

[58] 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).

som vistas på Europeiska unionens territorium och ett särskilt skydd för barn som kan vara offer för människohandel eller har bortförts av sina föräldrar, med full respekt för skyddet av personuppgifter.

(53) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, 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 lagstiftning.

(54) Förenade kungariket deltar i denna förordning i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, som är fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, och artikel 8.2 i 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[59].

(55) Irland deltar i denna förordning i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, som är fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, och artikel 6.2 i rådets beslut 2002/192/EG av den 28 februari 2002 om Irlands begäran om att få delta i vissa bestämmelser i Schengenregelverket[60].

(56) 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[61], en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.G i rådets beslut 1999/437/EG[62] om vissa tillämpningsföreskrifter för det avtalet.

(57) 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, 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 4.1 i rådets beslut 2004/849/EG[63] och 2004/860/EG[64].

---

59 EGT L 131, 1.6.2000, s. 43.

60 EGT L 64, 7.3.2002, s. 20.

61 EGT L 176, 10.7.1999, s. 36.

62 EGT L 176, 10.7.1999, s. 31.

63 Rådets beslut 2004/849/EG av den 25 oktober 2004 om undertecknande på Europeiska unionens vägnar och provisorisk tillämpning av vissa bestämmelser av avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 368, 15.12.2004, s. 26).

64 Rådets beslut 2004/860/EG av den 25 oktober 2004 om undertecknande på Europeiska gemenskapens vägnar och provisorisk tillämpning av vissa bestämmelser av avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 370, 17.12.2004, s. 78).

(58) När det gäller Liechtenstein utgör denna förordning, i enlighet med 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[65], 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[66] och artikel 3 i rådets beslut 2011/350/EU[67].

(59) 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 om tillämpningen av de bestämmelser i Schengenregelverket som rör Schengens informationssystem i Republiken Bulgarien och Rumänien[68].

(60) När det gäller Cypern och 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 3.2 i 2003 års anslutningsakt respektive artikel 4.2 i 2011 års anslutningsakt.

(61) 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.

(62) De beräknade kostnaderna för uppgraderingen av de nationella SIS-systemen och för genomförandet av de nya funktioner som planeras i denna förordning är lägre än det återstående beloppet i budgetrubriken för smarta gränser i Europaparlamentets och rådets förordning (EU) nr 515/2014[69]. Därför bör man genom denna förordning omfördela det beloppet, som anslagits för utveckling av it-system som stöd för hanteringen av migrationsströmmar över de yttre gränserna i enlighet med artikel 5.5 b i förordning (EU) nr 515/2014.

---

65 EUT L 160, 18.6.2011, s. 21.

66 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).

67 Rådets beslut 2011/350/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, om avskaffande av kontroller vid de inre gränserna och om personers rörlighet (EUT L 160, 18.6.2011, s. 19).

68 EUT L 166, 1.7.2010, s. 17.

69 Europaparlamentets och rådets förordning (EU) nr 515/2014 av den 16 april 2014 om inrättande, som en del av fonden för inre säkerhet, av ett instrument för ekonomiskt stöd för yttre gränser och visering (EUT L 150, 20.5.2014, s. 143).

(63) Rådets beslut 2007/533/RIF och kommissionens beslut 2010/261/EU[70] bör därför upphävas.

(64) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den …

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1
Allmänt syfte med SIS

Syftet med SIS ska vara att med hjälp av information som delas via systemet säkerställa hög säkerhet inom området med frihet, säkerhet och rättvisa i unionen, bland annat bevarande av allmän säkerhet och allmän ordning och skydd av säkerheten på medlemsstaternas territorier, samt att tillämpa bestämmelserna om fri rörlighet för personer på medlemsstaternas territorier enligt tredje delen, avdelning V, kapitlen 4 och 5 i fördraget om Europeiska unionens funktionssätt.

Artikel 2
Tillämpningsområde

1. I denna förordning fastställs villkor och förfaranden för inläggande och behandling i SIS av registreringar 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 SIS:s tekniska utformning, om ansvarsområden för medlemsstaterna och för Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, om allmän uppgiftsbehandling, om berörda personers rättigheter samt om skadeståndsansvar.

Artikel 3
Definitioner

1. I denna förordning gäller följande definitioner:

   (a) *registrering*: en sammanställning av uppgifter, däribland sådana biometriska kännetecken som avses i artiklarna 22 och 40, som lagts in i SIS och som de behöriga myndigheterna kan använda för att identifiera en person eller ett föremål med tanke på en viss åtgärd som ska vidtas.

   (b) *tilläggsinformation*: information som inte ingår i registreringsuppgifterna i SIS, men som avser SIS-registreringar och som ska utbytas

[70] 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).

(1) för att medlemsstaterna ska kunna samråda med eller underrätta varandra när de lägger in en registrering,

(2) för att lämpliga åtgärder ska kunna vidtas vid träff,

(3) när den åtgärd som krävs inte kan vidtas,

(4) när SIS-uppgifternas kvalitet hanteras,

(5) när registreringarnas överensstämmelse och prioritet hanteras,

(6) när åtkomsträtten hanteras.

(c) *kompletterande uppgifter*: sådana uppgifter i SIS som rör SIS-registreringar och som ska vara omedelbart tillgängliga för de behöriga myndigheterna när en person, om vilken uppgifter har lagts in i SIS, lokaliseras till följd av en sökning i systemet.

(d) *personuppgifter*: alla uppgifter om en identifierad eller identifierbar fysisk person (*den registrerade*).

(e) *en identifierbar fysisk person*: en person som direkt eller indirekt kan identifieras, särskilt med hjälp av sådana kännetecken som namn, id-nummer, lokaliseringsuppgift, onlineidentifierare eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

(f) *behandling av personuppgifter*: varje åtgärd eller serie av åtgärder som vidtas med personuppgifter eller uppsättningar av personuppgifter, vare sig det sker automatiserat eller inte, till exempel insamling, loggning, organisering, strukturering, lagring, bearbetning eller ändring, hämtning, läsning, användning, utlämnande genom översändande, spridning eller tillhandahållande på annat sätt, sammanställning eller samkörning, begränsning, radering eller förstöring.

(g) *träff*: uppkommer i SIS när

(1) en användare gör en sökning,

(2) sökningen visar en registrering som lagts in i SIS av en annan medlemsstat,

(3) uppgifterna i registreringen i SIS motsvarar sökuppgifterna, och

(4) ytterligare åtgärder begärs.

(h) *flaggning*: nationellt uppskov av giltigheten för en registrering, vilken kan fogas till registreringar om gripande, registreringar om försvunna personer och registreringar om diskreta kontroller, undersökningskontroller och särskilda kontroller, om en medlemsstat anser att verkställandet av en registrering är oförenligt med dess nationella lagstiftning, internationella skyldigheter eller viktiga nationella intressen. Om en registrering försetts med flaggning ska den åtgärd som begärts på grundval av registreringen inte vidtas på denna medlemsstats territorium.

(i) *registrerande medlemsstat*: den medlemsstat som har lagt in registreringen i SIS.

(j) *verkställande medlemsstat*: den medlemsstat som vidtar eller har vidtagit de begärda åtgärderna till följd av en träff.

(k) *slutanvändare*: behöriga myndigheter som söker direkt i CS-SIS, N.SIS eller en teknisk kopia.

(l) *finger- och handavtrycksuppgifter*: 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.

(m) *grov brottslighet*: sådana brott som avses i artikel 2.1 och 2.2 i rambeslut 2002/584/RIF av den 13 juni 2002[71].

(n) *terroristbrott*: sådana brott enligt nationell lagstiftning som avses i artiklarna 1–4 i rambeslut 2002/475/RIF av den 13 juni 2002[72].

Artikel 4
Teknisk utformning och drift av SIS

1. SIS ska bestå av följande delar:

(a) Ett centralt system (*det centrala SIS*) bestående av

– en teknisk stödfunktion (*CS-SIS*) som innehåller SIS-databasen, och

– ett enhetligt nationellt gränssnitt (*NI-SIS*).

(b) Ett nationellt system (*N.SIS*) i var och en av medlemsstaterna, bestående av de nationella datasystem som kommunicerar med det centrala SIS. Ett N.SIS ska innehålla en datafil (*nationell kopia*) med en fullständig eller partiell kopia av SIS-databasen, samt ett backupsystem för N.SIS. N.SIS och backupsystemet får användas samtidigt för att säkerställa oavbruten tillgång för slutanvändarna.

(c) En kommunikationsinfrastruktur mellan CS-SIS och NI-SIS (*kommunikationsinfrastruktur*) som tillhandahåller ett krypterat virtuellt nätverk ägnat åt SIS-uppgifter och utbytet av uppgifter mellan Sirenekontoren enligt artikel 7.2.

2. SIS-uppgifter ska läggas in, uppdateras, raderas och sökas i de olika N.SIS-systemen. En partiell eller fullständig nationell kopia ska finnas att tillgå för automatisk sökning i kopian på varje medlemsstats territorium. Den partiella nationella kopian ska innehålla åtminstone de uppgifter som avses i artikel 20.2 vad gäller föremål och de uppgifter som avses i artikel 20.3 a–v i denna förordning vad gäller registreringar om personer. Det ska inte vara möjligt att söka i datafilerna i andra medlemsstaters N.SIS.

3. CS-SIS ska användas för teknisk tillsyn och administration och ha ett backupsystem som kan säkerställa alla funktioner i CS-SIS om huvudsystemet skulle sluta fungera. CS-SIS och dess backupsystem ska vara belägna i de två tekniska anläggningarna vid Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, vilken inrättades genom förordning (EU) nr 1077/2011[73]

---

[71] Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (EGT L 190, 18.7.2002, s. 1).

[72] Rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3).

[73] Inrättad genom Europaparlamentets och rådets förordning (EU) nr 1077/2011 av den 25 oktober 2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 286, 1.11.2011, s. 1).

(nedan kallad *byrån*). CS-SIS eller dess backupsystem kan innehålla en ytterligare kopia av SIS-databasen och får användas samtidigt i aktiv drift, förutsatt att vardera har kapacitet att behandla alla transaktioner som rör SIS-registreringar.

4. CS-SIS ska tillhandahålla de tjänster som krävs för att kunna lägga in och behandla SIS-uppgifter, även sökningar i SIS-databasen. CS-SIS ska

   a) tillhandahålla uppdatering online av de nationella kopiorna,

   b) säkerställa synkronisering och enhetlighet mellan de nationella kopiorna och SIS-databasen,

   c) hantera initialisering och återställande av de nationella kopiorna,

   d) säkra oavbruten tillgång.

Artikel 5
Kostnader

1. Kostnaderna för drift, underhåll och vidareutveckling av det centrala SIS och kommunikationsinfrastrukturen ska belasta Europeiska unionens allmänna budget.

2. Dessa kostnader ska innefatta sådant arbete med CS-SIS som görs för att säkerställa tillhandahållande av de tjänster som avses i artikel 4.4.

3. 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 den fortlöpande driften av N.SIS, dess anslutning till NI-SIS och oavbruten tillgång till SIS-uppgifter för slutanvändarna.

Artikel 7
N.SIS-byrå och Sirenekontor

1. Varje medlemsstat ska utse en myndighet (*N.SIS-byrån*) som ska ha det centrala ansvaret för landets 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 bestämmelserna i denna förordning följs. Myndigheten ska ansvara för att säkerställa att alla funktioner i SIS är vederbörligen tillgängliga för slutanvändarna.

   Varje medlemsstat ska översända sina registreringar via N.SIS-byrån.

2. Varje medlemsstat ska utse en myndighet (*Sirenekontoret*) som ska säkerställa utbyte av och tillgång till tilläggsinformation i enlighet med Sirenehandboken, såsom anges i artikel 8.

Sirenekontoren ska också samordna kvalitetskontrollen av de uppgifter som läggs in i SIS. För dessa ändamål ska de ha tillgång till de uppgifter som behandlas i SIS.

3. Medlemsstaterna ska underrätta byrån om sin N.SIS II-byrå och om sitt Sirenekontor. Byrån ska offentliggöra en förteckning över dem tillsammans med den förteckning som avses i artikel 53.8.

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 utbyte av tilläggsinformation. Om kommunikationsinfrastrukturen inte är tillgänglig får medlemsstaterna använda annan tillfredsställande säker teknik för att utbyta tilläggsinformation.

2. Tilläggsinformationen ska bara användas för det ändamål för vilket den överförts i enlighet med artikel 61, om inte förhandstillstånd har inhämtats från den registrerande medlemsstaten.

3. Sirenekontoren ska utföra sina uppgifter snabbt och effektivt, i synnerhet genom att besvara begäran så snart som möjligt och senast 12 timmar efter det att begäran mottagits.

4. Närmare bestämmelser om utbytet av tilläggsinformation ska antas genom genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2, i form av en handbok kallad *Sirenehandboken*.

Artikel 9
Teknisk och funktionell överensstämmelse

1. När en medlemsstat inrättar sitt N.SIS ska den följa de gemensamma standarder, protokoll och tekniska förfaranden som har fastställts för att säkerställa att dess N.SIS är kompatibelt med CS-SIS för snabb och effektiv dataöverföring. Dessa gemensamma standarder, protokoll och tekniska förfaranden ska antas genom genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

2. Medlemsstaterna ska med hjälp av de tjänster som tillhandahålls av CS-SIS säkerställa att uppgifter som lagrats i den nationella kopian genom de automatiska uppdateringar som avses i artikel 4.4 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. Slutanvändarna ska få de uppgifter de behöver för att utföra sina uppgifter, i synnerhet alla de uppgifter som krävs för att identifiera den registrerade och vidta begärda åtgärder.

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 med hjälp av beredskapsplaner för att skydda 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, ändring eller 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) säkerställa att personer som är behöriga att använda ett automatiskt databehandlingssystem har åtkomst endast till de uppgifter som ingår i deras befogenheter och endast med hjälp av individuella och unika användaridentiteter och skyddade åtkomstmetoder (åtkomstkontroll),

   (g) säkerställa att alla myndigheter med åtkomst till SIS eller tillträde till uppgiftsbehandlingsanläggningar skapar profiler som beskriver uppgifter och ansvar för personer som har befogenhet att läsa, lägga in, uppdatera, radera och söka uppgifter och på begäran utan dröjsmål ger de nationella tillsynsmyndigheter som avses i artikel 66 tillgång till dessa profiler (personalprofiler),

   (h) säkerställa möjligheten att kontrollera och fastställa till vilka organ personuppgifter får överföras via datakommunikationsutrustning (kommunikationskontroll),

   (i) säkerställa möjlighet till efterföljande kontroll och granskning av vilka personuppgifter som matats in i ett automatiskt databehandlingssystem samt när, av vem och för vilket ändamål uppgifterna har matats in (inmatningskontroll),

   (j) 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),

   (k) övervaka att de säkerhetsåtgärder som avses i denna punkt är ändamålsenliga och vidta nödvändiga organisatoriska åtgärder i fråga om intern övervakning (egenrevision).

2. Medlemsstaterna ska vidta åtgärder av samma slag som i punkt 1 när det gäller säkerheten vid behandling och utbyte av tilläggsinformation, bland annat genom att säkra Sirenekontorets lokaler.

3. Medlemsstaterna ska vidta åtgärder av samma slag som i punkt 1 när det gäller säkerheten vid behandling av SIS-uppgifterna av de myndigheter som avses i artikel 43.

Artikel 11
Sekretess – Medlemsstaterna

Varje medlemsstat ska i enlighet med den nationella lagstiftningen tillämpa sina regler om tystnadsplikt eller motsvarande sekretesskrav på alla personer och organ som arbetar med SIS-uppgifter och tilläggsinformation. Reglerna ska gälla även efter det att personerna lämnat sin tjänst eller anställning eller efter det att organets verksamhet upphört.

Artikel 12
Loggar på nationell nivå

1. Medlemsstaterna ska säkerställa att all åtkomst till och alla utbyten av personuppgifter med CS-SIS loggas i landets N.SIS för att möjliggöra kontroll av om sökningen är laglig, övervaka att uppgiftsbehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa att N.SIS fungerar tillfredsställande och att uppgifternas integritet och säkerhet tryggas.

2. Loggarna ska i synnerhet visa registreringshistoriken, dag och tidpunkt för behandlingen, vilken typ av uppgifter som användes för sökningen, en hänvisning till de uppgifter som överfördes och namn på den behöriga myndighet och den person som är ansvarig för uppgiftsbehandlingen.

3. Om sökningen görs med finger- och handavtrycksuppgifter eller ansiktsbilder i enlighet med artiklarna 40, 41 och 42 ska loggarna i synnerhet visa vilken typ av uppgifter som användes för sökningen, en hänvisning till den typ av uppgifter som överfördes och namn på den behöriga myndighet och den person som är ansvarig för uppgiftsbehandlingen.

4. Loggarna får användas endast för de ändamål som anges i punkt 1 och ska raderas tidigast ett år och senast tre år efter det att de skapades.

5. Loggarna får sparas längre om de behövs för kontroller som redan pågår.

6. De behöriga nationella myndigheter som har till uppgift att kontrollera om sökningen är laglig, övervaka att uppgiftsbehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa att N.SIS fungerar tillfredsställande och att uppgifternas integritet och säkerhet tryggas, ska inom gränserna för sin behörighet på begäran ha åtkomst till dessa loggar, så att de kan fullgöra sina uppgifter.

7. Då medlemsstaterna utför automatiska skanningssökningar av motorfordons nummerplåtar med automatiska nummerplåtsavläsningssystem ska de föra en logg över sökningarna i enlighet med nationell lagstiftning. Innehållet i denna logg ska fastställas genom genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2. Om en positiv träff görs mot uppgifter som lagras i SIS eller en nationell eller teknisk kopia av SIS-uppgifter ska en fullständig sökning utföras i SIS för att bekräfta att träffen verkligen är positiv. Bestämmelserna i punkt 1–6 i denna artikel ska tillämpas på denna fullständiga sökning.

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 den nationella tillsynsmyndigheten.

Artikel 14
Personalutbildning

Innan personalen vid de myndigheter som har åtkomsträtt till SIS får behandla uppgifter i SIS och regelbundet efter det att åtkomst till SIS beviljats, ska personalen utbildas på lämpligt sätt om datasäkerhet, uppgiftsskydd och förfaranden för uppgiftsbehandling enligt Sirenehandboken. Personalen ska informeras om relevanta brott och påföljder.

KAPITEL III

BYRÅNS ANSVARSOMRÅDEN

Artikel 15
Operativ förvaltning

1. Byrån ska ansvara för den operativa förvaltningen av det centrala SIS. Byrån ska i samarbete med medlemsstaterna och med förbehåll för en kostnads-nyttoanalys säkerställa att bästa tillgängliga teknik alltid används för det centrala SIS.
2. I fråga om kommunikationsinfrastrukturen ska byrån även ansvara för
   (a) övervakning,
   (b) säkerhet,
   (c) samordning av förbindelserna mellan medlemsstaterna och leverantören.
3. Kommissionen ska ansvara för alla andra uppgifter avseende kommunikationsinfrastrukturen, särskilt
   (a) genomförande av budgeten,
   (b) förvärv och förnyande,
   (c) avtalsfrågor.
4. Byrån ska ansvara för följande uppgifter avseende Sirenekontoren och kommunikationen mellan Sirenekontoren:
   (a) Samordning och hantering av tester.
   (b) Underhåll och uppdatering av tekniska specifikationer för utbytet av tilläggsinformation mellan Sirenekontoren och kommunikationsinfrastrukturen samt hantering av effekterna av tekniska förändringar som påverkar både SIS och utbytet av tilläggsinformation mellan Sirenekontoren.
5. Byrån ska utveckla och underhålla en mekanism och förfaranden för kvalitetskontroll av uppgifterna i CS-SIS, och ska regelbundet rapportera till medlemsstaterna. Byrån ska regelbundet rapportera till kommissionen om problem som uppstått och vilka

medlemsstater som berörs. Mekanismen, förfarandena och efterlevnaden av kvalitetskraven på uppgifterna ska fastställas genom genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

6. Den operativa förvaltningen av det centrala SIS ska omfatta alla uppgifter som krävs för att det centrala SIS ska kunna fungera dygnet runt alla dagar i veckan, särskilt det underhåll och den tekniska utveckling som krävs för att systemet ska kunna fungera smidigt. Dessa uppgifter omfattar även tester för att säkerställa att det centrala SIS och de nationella systemen fungerar i enlighet med de tekniska och funktionsmässiga kraven i enlighet med artikel 9 i denna förordning.

Artikel 16
Säkerhet

1. Byrån 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 med hjälp av beredskapsplaner för att skydda 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, ändring eller 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) säkerställa att personer som är behöriga att använda ett automatiskt databehandlingssystem endast med hjälp av individuella och unika användaridentiteter och skyddade åtkomstmetoder har åtkomst till endast de uppgifter som ingår i deras befogenheter (åtkomstkontroll),

   (g) skapa profiler som beskriver uppgifter och ansvar för personer som har rätt att få åtkomst till uppgifterna eller tillträde till uppgiftsbehandlingsanläggningarna och på begäran utan dröjsmål ge den europeiska datatillsynsman som avses i artikel 64 tillgång till dessa profiler (personalprofiler),

   (h) säkerställa möjligheten att kontrollera och fastställa till vilka organ personuppgifter får överföras via datakommunikationsutrustning (kommunikationskontroll),

   (i) säkerställa möjlighet till efterföljande kontroll och granskning av vilka personuppgifter som matats in i ett automatiskt databehandlingssystem samt när och av vem uppgifterna har matats in (inmatningskontroll),

   (j) 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),

(k) 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).

2. Byrån ska vidta åtgärder av samma slag som i punkt 1 när det gäller säkerheten vid behandling och utbyte av tilläggsinformation via kommunikationsinfrastrukturen.

Artikel 17
Sekretess – Byrån

1. Utan att det påverkar tillämpningen av artikel 17 i tjänsteföreskrifterna för tjänstemän i Europeiska unionen och anställningsvillkoren för övriga anställda i Europeiska unionen ska byrån tillämpa lämpliga regler om tystnadsplikt eller motsvarande sekretesskrav som är jämförbara med de som anges i artikel 11 i den här förordningen på all personal som arbetar med SIS-uppgifter. Reglerna ska gälla även efter det att personerna lämnat sin tjänst eller anställning eller efter det att verksamheten upphört.

2. Byrån ska vidta åtgärder av samma slag som i punkt 1 när det gäller sekretess vid utbyte av tilläggsinformation via kommunikationsinfrastrukturen.

Artikel 18
Loggar på central nivå

1. Byrån 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 överföringen, vilken typ av uppgifter som användes för sökningarna, en hänvisning till den typ av uppgifter som överfördes och namn på den behöriga myndighet som är ansvarig för uppgiftsbehandlingen.

3. Om sökningen görs med finger- och handavtrycksuppgifter eller ansiktsbilder i enlighet med artiklarna 40, 41 och 42 ska loggarna i synnerhet visa vilken typ av uppgifter som användes för sökningen, en hänvisning till den typ av uppgifter som överfördes och namn på den behöriga myndighet och den person som är ansvarig för uppgiftsbehandlingen.

4. Loggarna får endast användas för de ändamål som avses i punkt 1 och ska raderas tidigast ett år och senast tre år efter det att de skapades. De loggar som omfattar registreringshistorik ska raderas ett till tre år efter det att registreringarna raderats.

5. Loggar får sparas längre om de behövs för kontroller som redan pågår.

6. De behöriga myndigheter som har till uppgift att kontrollera om sökningen är laglig, övervaka att uppgiftsbehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa att CS-SIS fungerar tillfredsställande och att uppgifternas integritet och säkerhet tryggas, ska inom gränserna för sin behörighet på begäran ha åtkomst till dessa loggar, så att de kan fullgöra sina uppgifter.

KAPITEL IV

INFORMATION TILL ALLMÄNHETEN

Artikel 19
Informationskampanjer om SIS

Kommissionen ska i samarbete med de nationella tillsynsmyndigheterna och Europeiska datatillsynsmannen regelbundet genomföra informationskampanjer för att upplysa allmänheten om målen med SIS, vilka uppgifter som lagras, vilka myndigheter som har åtkomst till SIS och om de registrerades rättigheter. Medlemsstaterna ska i samarbete med sina nationella tillsynsmyndigheter utforma och genomföra de nödvändiga strategierna för att ge sina medborgare 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 kategorier av uppgifter som lämnas av var och en av medlemsstaterna, så som krävs för de ändamål som fastställs i artiklarna 26, 32, 34, 36 och 38.

2. Uppgiftskategorierna ska vara följande:

   (a) Uppgifter om personer som omfattas av en registrering.

   (b) Uppgifter om de föremål som avses i artiklarna 32, 36 och 38.

3. Uppgifter om personer som omfattas av en registrering får endast avse följande:

   (a) Samtliga efternamn.

   (b) Samtliga 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) Medborgarskap.

   (j) Huruvida personen är beväpnad, våldsam, har rymt eller deltar i en verksamhet som avses i artiklarna 1, 2, 3 och 4 i rådets rambeslut 2002/475/RIF om bekämpande av terrorism,

   (k) Orsak till registreringen.

(l) Myndighet som har fört in registreringen.

(m) Hänvisning till det beslut som gett upphov till registreringen.

(n) Begärd åtgärd.

(o) Länk(ar) till andra registreringar som förts in i SIS enligt artikel 53.

(p) Typ av brott som ligger till grund för registreringen.

(q) Personens registreringsnummer i ett nationellt register.

(r) Kategorisering av typen av försvinnande (endast för registreringar om försvunna personer enligt artikel 32).

(s) Id-handlingens kategori.

(t) Det land som utfärdat id-handlingen.

(u) Id-handlingens nummer.

(v) Id-handlingens utfärdandedatum.

(w) Fotografier och ansiktsbilder.

(x) Relevanta DNA-profiler om artikel 22.1 b i denna förordning är tillämplig.

(y) Finger- och handavtrycksuppgifter.

(z) En färgkopia av id-handlingen.

4. De tekniska föreskrifter som behövs för att lägga in, uppdatera, radera eller söka de uppgifter som avses i punkterna 2 och 3 ska fastställas och utvecklas genom genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

5. De tekniska föreskrifter som behövs för att söka de uppgifter som avses i punkt 3 ska fastställas och utvecklas i enlighet med det granskningsförfarande som avses i artikel 72.2. De tekniska föreskrifterna ska vara snarlika för sökningar i CS-SIS, nationella kopior och de tekniska kopior som avses i artikel 53.2, och de ska bygga på de gemensamma standarder som fastställts och utvecklats genom genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

Artikel 21
Proportionalitetsprincipen

1. Innan en registrering förs in och när registreringens giltighetstid förlängs ska medlemsstaterna pröva om ärendet är tillräcklig adekvat, relevant och viktigt för att motivera registrering i SIS.

2. Om en person eller ett föremål söks av en medlemsstat i samband med ett brott som omfattas av artiklarna 1–4 i rådets rambeslut 2002/475/RIF om bekämpande av terrorism, ska medlemsstaten under alla omständigheter skapa motsvarande registrering enligt antingen artikel 34, 36 eller 38 efter vad som är tillämpligt.

Artikel 22

Särskilda bestämmelser för införande av fotografier, ansiktsbilder, finger- och handavtrycksuppgifter och DNA-profiler

1. Inläggande i SIS av de uppgifter som avses i artikel 20.3 w, x och y ska ske enligt följande villkor:

   (a) Fotografier, ansiktsbilder, finger- och handavtrycksuppgifter och DNA-profiler ska läggas in endast efter en kvalitetskontroll för att konstatera att minimistandarder för uppgifternas kvalitet uppfylls.

   (b) En DNA-profil får endast läggas till de registreringar som anges i artikel 32.2 a och c, och enbart om det inte finns några fotografier, ansiktsbilder eller finger- och handavtrycksuppgifter som lämpar sig för identifiering. DNA-profiler från personer som är släktingar i rakt upp- eller nedstigande led eller syskon till den registrerade personen får läggas till registreringen förutsatt att de berörda personerna ger sitt uttryckliga medgivande. Personens ras ska inte ingå i DNA-profilen.

2. Kvalitetsstandarder ska fastställas för lagring av de uppgifter som avses i punkt 1 a i den här artikeln och i artikel 40. Närmare detaljer om dessa standarder ska fastställas genom genomförandeåtgärder och uppdateras i enlighet med det granskningsförfarande som avses i artikel 72.2.

Artikel 23

Krav för att en registrering ska få läggas in

1. En registrering om en person får inte läggas in utan de uppgifter som avses i artikel 20.3 a, g, k, m, n och, i tillämpliga fall, p, förutom i de situationer som avses i artikel 40.

2. Alla andra uppgifter som avses i artikel 20.3 ska också läggas in om de är tillgängliga.

Artikel 24

Allmänna bestämmelser om flaggning

1. Om en medlemsstat anser att verkställandet av en registrering som lagts in i enlighet med artiklarna 26, 32 och 36 är oförenlig med dess nationella lagstiftning, internationella förpliktelser eller viktiga nationella intressen, kan den därefter 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 åtgärder ska vidtas, ska den verkställande medlemsstaten pröva om den flaggning som lagts till på dess begäran kan raderas. 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 flagga som förhindrar gripandet av en person endast läggas till en registrering om gripande för överlämnande om den rättsliga myndighet som enligt nationell lag 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.

2. På begäran av en rättslig myndighet som enligt nationell lag är behörig kan, på grundval av en allmän instruktion eller i särskilda fall, emellertid en registrering om gripande för överlämnande även förses med en flagga om det är uppenbart att verkställandet av den europeiska arresteringsordern ska vägras.

KAPITEL VI

REGISTRERINGAR OM PERSONER SOM ÄR EFTERLYSTA FÖR GRIPANDE FÖR ÖVERLÄMNANDE ELLER UTLÄMNING

Artikel 26

Syfte och villkor för införande av registreringar

1. Uppgifter om personer som är efterlysta för att gripas och överlämnas på grundval av en europeisk arresteringsorder eller som är efterlysta för att gripas och utlämnas ska läggas in på begäran av den rättsliga myndigheten i den registrerande medlemsstaten.

2. Uppgifter om personer som är efterlysta för att gripas och överlämnas ska också läggas in på grundval av arresteringsorder som utfärdats i enlighet med avtal som, på grundval av artikel 37 i fördraget om Europeiska unionen, ingåtts mellan Europeiska 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 artikel 37 i fördraget om Europeiska unionen, ingåtts mellan Europeiska unionen och tredjeländer om överlämnande av personer på grundval av en arresteringsorder och som medger att en sådan arresteringsorder översänds via SIS.

4. Den registrerande medlemsstaten kan, under pågående spaningsinsatser och med tillstånd från den behöriga rättsliga myndigheten i den registrerande medlemsstaten, tillfälligt göra en befintlig registrering om gripande som förts in enligt artikel 26 i denna förordning otillgänglig för sökningar så att registreringen inte ska kunna sökas av slutanvändaren och endast vara åtkomlig för Sirenekontoren. Denna funktion ska användas under en period på högst 48 timmar. Om det är operativt nödvändigt kan den dock förlängas med ytterligare perioder på 48 timmar. Medlemsstaterna ska föra statistik över antalet registreringar för vilka denna funktion har använts.

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 lägga in en kopia av originalet av den europeiska arresteringsordern i SIS.

2. Den registrerande medlemsstaten kan också bifoga en kopia av en översättning av den europeiska arresteringsordern på ett eller flera av Europeiska unionens institutioners officiella språk.

Artikel 28

Tilläggsinformation om personer som är efterlysta för att gripas och överlämnas

Den medlemsstat som har lagt in en registrering i SIS 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 medlemsstat som lade in registreringen i SIS för utlämningsändamål ska lämna följande uppgifter till de övriga medlemsstaterna, 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 brottets begåtts, inbegripet tidpunkt, plats och i vilken grad den registrerade personen varit delaktig i gärningen.

   (e) Så långt möjligt, brottspåföljd.

   (f) Annan information som är användbar eller nödvändig för verkställande av registreringen.

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

Artikel 30

Konvertering av registreringar om personer som är efterlysta för att gripas och överlämnas eller utlämnas

Om ett gripande inte kan verkställas antingen på grund av att den anmodade medlemsstaten vägrar 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 anmodade medlemsstaten betrakta registreringen som en registrering vars syfte är att meddela var den berörda personen befinner sig.

Artikel 31

Verkställande av åtgärder på grundval av en registrering om en person som är efterlyst för att gripas och överlämnas eller utlämnas

1. En registrering som lagts in i SIS i enlighet med artikel 26 ska tillsammans med de kompletterande uppgifter som avses i artikel 27 utgöra, och ha samma verkan som,

en europeisk arresteringsorder som utfärdats i enlighet med rambeslut 2002/584/RIF när detta rambeslut är tillämpligt.

2. När rambeslut 2002/584/RIF inte är tillämpligt ska en registrering som lagts 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

Artikel 32
Syfte och villkor för införande av registreringar

1. Uppgifter om försvunna personer eller andra personer som behöver ställas under beskydd eller vars vistelseort måste fastställas ska läggas in i SIS på begäran av den behöriga myndigheten i den medlemsstat som för in registreringen.

2. Registreringar får läggas in om följande kategorier försvunna personer:

   (a) Försvunna personer som behöver ställas under beskydd

      i) med hänsyn till deras egen säkerhet,

      ii) för att förebygga hot.

   (b) Försvunna personer som inte behöver ställas under beskydd.

   (c) Barn som löper risk att bortföras i enlighet med punkt 4.

3. Punkt 2 a ska särskilt tillämpas på barn och på personer som ska omhändertas efter ett beslut av behörig myndighet.

4. En sådan registrering om ett barn som avses i punkt 2 c ska läggas in på begäran av den behöriga rättsliga myndighet i den medlemsstat som har jurisdiktion i frågor om föräldraansvar enligt rådets förordning nr 2201/2003[74] om det föreligger en konkret och uppenbar risk att barnet omgående och olagligt kan avlägsnas från den medlemsstat där den behöriga myndigheten är belägen. I medlemsstater som är parter i Haagkonventionen av den 19 oktober 1996 om behörighet, tillämplig lag, erkännande, verkställighet och samarbete i frågor om föräldraansvar och åtgärder till skydd för barn och där rådets förordning nr 2201/2003 inte är tillämplig, tillämpas bestämmelserna i Haagkonventionen.

5. Medlemsstaterna ska säkerställa att de uppgifter som läggs in i SIS anger till vilken av kategorierna i punkt 2 den försvunna personen hör. Medlemsstaterna ska dessutom säkerställa att de uppgifter som läggs in i SIS anger vilken typ av försvinnande eller sårbarhet som föreligger. Bestämmelserna om kategorisering av ärendetyp och inläggande av sådana uppgifter ska fastställas och utvecklas med hjälp

[74] Rådets förordning (EG) nr 2201/2003 av den 27 november 2003 om domstols behörighet och om erkännande och verkställighet av domar i äktenskapsmål och mål om föräldraansvar samt om upphävande av förordning (EG) nr 1347/2000 (EUT L 338, 23.12.2003, s. 1).

av genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

6. Fyra månader innan ett barn som omfattas av en registrering enligt denna artikel når vuxen ålder ska CS-SIS automatiskt underrätta den registrerande medlemsstaten att grunden för begäran och den åtgärd som ska vidtas antingen måste uppdateras eller att registreringen måste raderas.

7. Om det finns tydliga tecken på att fordon, fartyg eller luftfartyg har koppling till en person som omfattas av en registrering enligt punkt 2 får registreringar om dessa fordon, fartyg och luftfartyg föras in för att lokalisera personen. I de fallen ska registreringen om den försvunna personen och registreringen om föremålet länkas i enlighet med artikel 60. De tekniska föreskrifter som behövs för att lägga in, uppdatera, radera och söka de uppgifter som avses i denna punkt ska fastställas och utvecklas med hjälp av genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

Artikel 33
Verkställande av åtgärder på grundval av en registrering

1. När en person som avses i artikel 32 lokaliseras ska de behöriga myndigheterna, med förbehåll för vad som sägs i punkt 2, underrätta den medlemsstat som fört in registreringen om var personen befinner sig. När det gäller försvunna barn eller barn som behöver ställas under beskydd ska den verkställande medlemsstaten omedelbart samråda med den registrerande medlemsstaten för att utan dröjsmål komma överens om vilka åtgärder som ska vidtas för att skydda barnets bästa. De behöriga myndigheterna får i de fall som anges i artikel 32.2 a och c föra personen till en säker plats för att förhindra denna från att fortsätta sin resa, om så föreskrivs i nationell lag.

2. Uppgifter om en försvunnen myndig person som har lokaliserats får inte vidarebefordras utan dennas medgivande, 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 lägga in uppgifter 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 fordon, fartyg eller luftfartyg har koppling till en person som omfattas av en registrering enligt punkt 1 får registreringar om dessa fordon, fartyg och luftfartyg föras in för att lokalisera personen. I sådana fall ska registreringarna om personen och registreringen om föremålet länkas i enlighet med artikel 60. De tekniska föreskrifter som behövs för att lägga in, uppdatera, radera och söka de uppgifter som avses i denna punkt ska fastställas och utvecklas med hjälp av genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

Artikel 35
Verkställande av åtgärder på grundval av en registrering

De begärda uppgifterna ska lämnas till den ansökande medlemsstaten 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. I överensstämmelse med nationell lagstiftning i den medlemsstat som för in registreringen ska uppgifter läggas in om personer eller fordon, fartyg, luftfartyg och containrar för diskret kontroll, undersökningskontroll eller särskild kontroll i enlighet med artikel 37.4.

2. Registreringen får föras in för att lagföra brott, verkställa en straffrättslig påföljd och förebygga hot mot den allmänna säkerheten

   (a) om det finns tydliga tecken på att en person avser att begå, eller redan begår, ett grovt brott, i synnerhet de brott som anges i artikel 2.2 i rambeslut 2002/584/RIF,

   (b) om de uppgifter som avses i artikel 37.1 är nödvändiga för att verkställa en straffrättslig påföljd för en person som dömts för ett grovt brott, i synnerhet de brott som anges i artikel 2.2 i rambeslut 2002/584/RIF, eller

   (c) om en allmän bedömning av en person, särskilt på grundval av redan begångna brott, leder till misstanke om att denna även i framtiden kan komma att begå grova brott, i synnerhet de brott som anges i artikel 2.2 i rambeslut 2002/584/RIF.

3. På begäran av de myndigheter som ansvarar för den nationella säkerheten kan en registrering dessutom föras in i enlighet med nationell lagstiftning, om det finns konkreta tecken på att de uppgifter som avses i artikel 37.1 är nödvändiga för att avvärja det allvarliga hot den berörda personen utgör eller andra allvarliga hot mot statens inre eller yttre säkerhet. Den medlemsstat som för in registreringen i enlighet

med denna punkt ska informera de övriga medlemsstaterna om detta. Varje medlemsstat ska besluta till vilka myndigheter informationen ska överlämnas.

4. Om det finns tydliga tecken på att fordon, fartyg, luftfartyg och containrar har samband med de grova brott som avses i punkt 2 eller de allvarliga hot som avses i punkt 3 kan registreringar föras in om dessa fordon, fartyg, luftfartyg och containrar.

5. Om det finns tydliga tecken på att officiella blankodokument eller utfärdade id-handlingar har samband med de grova brott som avses i punkt 2 eller de allvarliga hot som avses i punkt 3 kan registreringar föras in om dessa handlingar, oavsett vem id-handlingen eventuellt har tillhört ursprungligen. De tekniska föreskrifter som behövs för att lägga in, uppdatera, radera och söka de uppgifter som avses i denna punkt ska fastställas och utvecklas med hjälp av genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

Artikel 37
Verkställande av åtgärder på grundval av en registrering

1. I syfte att utföra diskreta kontroller, undersökningskontroller eller särskilda kontroller ska samtliga eller vissa av nedanstående uppgifter insamlas och översändas till den myndighet som fört in registreringen när gränskontroller, polis- och tullkontroller eller annan brottsbekämpande verksamhet utförs inom medlemsstaten:

   (a) Lokalisering av personer, fordon, fartyg, luftfartyg, containrar, officiella blankodokument eller utfärdade id-handlingar vilka omfattas av en registrering.

   (b) Plats, tid och orsak för kontrollen.

   (c) Resväg och målet för resan.

   (d) Personer i den berörda personens sällskap 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 de berörda personerna.

   (e) Avslöjad identitet och personlig beskrivning av den person som använder det officiella blankodokument eller de utfärdade id-handlingar som är föremål för registreringen.

   (f) Fordon, fartyg, luftfartyg eller container som använts.

   (g) Medförda föremål, även resehandlingar.

   (h) De omständigheter under vilka personen eller fordonet, fartyget, luftfartyget, containern, det officiella blankodokumentet eller de utfärdade id-handlingarna lokaliserades.

2. Den information som avses i punkt 1 ska lämnas genom utbyte av tilläggsinformation.

3. Beroende på de operativa förhållandena och i enlighet med nationell lagstiftning ska en diskret kontroll bestå av en rutinkontroll av en person eller ett föremål i syfte att samla in så många av de uppgifter i punkt 1 som möjligt utan att äventyra den diskreta kontrollen.

4. Beroende på de operativa förhållandena och i enlighet med nationell lagstiftning ska en undersökningskontroll bestå av en mer ingående kontroll och en utfrågning av

personen. Om en medlemsstats nationella lagstiftning inte tillåter undersökningskontroller ska kontrollerna i den medlemsstaten ersättas med diskreta kontroller.

5. Inom ramen för särskilda kontroller får personer kroppsvisiteras och fordon, fartyg, luftfartyg, containrar och medförda föremål genomsökas i enlighet med nationell lagstiftning för de ändamål som anges i artikel 36. Kroppsvisitering och genomsökning ska ske i enlighet med nationell lagstiftning. Om en medlemsstats nationella lagstiftning inte tillåter särskilda kontroller ska kontrollerna i den medlemsstaten ersättas med undersökningskontroller.

KAPITEL X

REGISTRERINGAR OM FÖREMÅL SOM SKA BESLAGTAS ELLER ANVÄNDAS SOM BEVIS I BROTTMÅL

Artikel 38
Syfte och villkor för införande av registreringar

1. Uppgifter om föremål som söks för att antingen beslagtas för brottsbekämpande ändamål eller användas som bevis i brottmål ska läggas in i SIS.

2. Följande kategorier av lätt identifierbara föremål ska registreras:

   (a) Motorfordon, enligt definitionen i nationell lagstiftning, oavsett framdrivningssystem.

   (b) Släpvagnar med en tjänstevikt överstigande 750 kg.

   (c) Husvagnar.

   (d) Industriell utrustning.

   (e) Fartyg.

   (f) Fartygsmotorer.

   (g) Containrar.

   (h) Luftfartyg.

   (i) Skjutvapen.

   (j) Stulna, bortförda eller försvunna officiella blankodokument.

   (k) Utfärdade identitetshandlingar, till exempel pass, ID-kort, körkort, uppehållstillstånd och resehandlingar, vilka är stulna, bortförda, försvunna, ogiltiga eller som ger intryck av att vara sådana handlingar men är förfalskade.

   (l) Fordonsregistreringsbevis och nummerplåtar som är stulna, bortförda, försvunna, ogiltiga eller ger intryck av att vara sådana bevis eller nummerplåtar men är förfalskade.

   (m) Sedlar (registrerade sedlar) och förfalskade sedlar.

   (n) Teknisk utrustning, it-produkter och andra lätt identifierbara föremål av högt värde.

   (o) Identifierbara beståndsdelar av motorfordon.

   (p) Identifierbara beståndsdelar av industriell utrustning.

3. Definitionen av nya underkategorier av föremål i punkt 2 n och de tekniska föreskrifter som är nödvändiga för att lägga in, uppdatera, radera och söka de uppgifter som avses i punkt 2 ska fastställas och utvecklas med hjälp av genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

Artikel 39
Verkställande av åtgärder på grundval av en registrering

1. Om en sökning visar att det finns en registrering för ett lokaliserat föremål ska den myndighet som har noterat sambandet mellan de två uppgifterna i enlighet med nationell lagstiftning beslagta föremålet och kontakta den myndighet som fört in registreringen för att komma överens om vilka åtgärder som ska vidtas. För detta ändamål kan även personuppgifter översändas i enlighet med denna förordning.
2. Den information som avses i punkt 1 ska lämnas genom utbyte av tilläggsinformation.
3. Den medlemsstat som lokaliserade föremålet ska vidta de begärda åtgärderna i enlighet med nationell lagstiftning.

KAPITEL XI

REGISTRERINGAR OM OKÄNDA EFTERLYSTA PERSONER FÖR IDENTIFIERING I ENLIGHET MED NATIONELL LAGSTIFTNING SAMT SÖKNING MED BIOMETRISKA UPPGIFTER

Artikel 40
Registreringar om okända personer som är efterlysta för gripande enligt nationell lagstiftning

Finger- och handavtrycksuppgifter kan läggas in i SIS utan koppling till personer som omfattas av registreringarna. Dessa finger- och handavtrycksuppgifter ska antingen vara fullständiga eller ofullständiga uppsättningar fingeravtryck eller handavtryck som upptäckts på platsen för ett brott som utreds, för grova brott och terroristbrott, och det ska kunna fastställas att de med hög sannolikhet tillhör gärningsmannen. Finger- och handavtrycksuppgifterna i denna kategori ska lagras som ”okänd misstänkt eller efterlyst person”, förutsatt att de behöriga myndigheterna inte kan fastställa personens identitet med hjälp av någon annan nationell, europeisk eller internationell databas.

Artikel 41
Verkställande av åtgärder på grundval av en registrering

Vid en träff eller en potentiell matchning med de uppgifter som lagrats enligt artikel 40 ska personens identitet fastställas i enlighet med nationell lagstiftning, tillsammans med en kontroll av att de finger- och handavtrycksuppgifter som lagrats i SIS tillhör den personen. Medlemsstaterna ska kommunicera genom att använda tilläggsinformation för att underlätta att ärendet utreds snabbt.

Artikel 42

Särskilda bestämmelser om kontroll eller sökning med fotografier, ansiktsbilder, finger- och handavtrycksuppgifter och DNA-profiler

1. Fotografier, ansiktsbilder, finger- och handavtrycksuppgifter och DNA-profiler ska hämtas från SIS för att kontrollera identiteten på en person som har lokaliserats efter en alfanumerisk sökning i SIS.

2. Finger- och handavtrycksuppgifter får också användas för identifiering. Finger- och handavtrycksuppgifter i SIS ska användas för identifiering om det inte går att fastställa en persons identitet på annat sätt.

3. Finger- och handavtrycksuppgifter som lagras i SIS avseende registreringar som förts in enligt artiklarna 26, 34.1 b och d och 36 får också sökas med hjälp av fullständiga eller ofullständiga uppsättningar fingeravtryck eller handavtryck som hittats på en brottsplats under en utredning, och det kan fastställas att de mycket sannolikt tillhör gärningsmannen, förutsatt att de behöriga myndigheterna inte kan fastställa personens identitet med hjälp av någon annan nationell, europeisk eller internationell databas.

4. Fotografier och ansiktsbilder får användas för identifiering av personer så fort detta blir tekniskt möjligt, förutsatt att man säkerställer att identifieringen är mycket tillförlitlig. Identifiering med hjälp av fotografier eller ansiktsbilder ska endast användas vid reguljära gränsövergångsställen där självbetjäningssystem och automatiska gränskontrollsystem används.

KAPITEL XII

ÅTKOMSTRÄTT OCH REGISTRERINGARNAS LAGRINGSTID

Artikel 43

Myndigheter med åtkomsträtt till registreringar

1. Åtkomst till uppgifter i SIS och rätt att söka sådana uppgifter direkt eller i en kopia av SIS-uppgifter ska förbehållas myndigheter med ansvar för

   (a) gränskontroller, i enlighet med Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodexen om Schengengränserna),

   (b) polisens och tullens kontroller inom den berörda medlemsstaten och de utsedda myndigheternas samordning av sådana kontroller,

   (c) annan brottsbekämpande verksamhet som bedrivs för att förebygga, upptäcka och utreda brott inom den berörda medlemsstaten,

   (d) granskning av villkoren och beslutsfattande i samband med tredjelandsmedborgares inresa och vistelse på medlemsstaternas territorium, även gällande uppehållstillstånd och viseringar för längre vistelse, och i samband med återvändande av tredjelandsmedborgare.

2. Rätten till åtkomst till uppgifter som har lagts in i SIS och rätten att söka 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, när de utför sina

uppgifter i enlighet med nationell lagstiftning, samt av deras samordningsmyndigheter.

3. Rätten till åtkomst till uppgifter som har lagts in i SIS och rätten att söka sådana uppgifter direkt får utövas av de myndigheter som är behöriga att utföra de uppgifter som anges i punkt 1 c vid utförandet av dessa uppgifter. Dessa myndigheters åtkomst ska regleras i varje medlemsstats lagstiftning.

4. De myndigheter som anges i denna artikel ska tas med i den förteckning som avses i artikel 53.8.

Artikel 44
Fordonsregistreringsmyndigheter

1. De enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon, vilka avses i rådets direktiv 1999/37/EG[75], ska ha åtkomst till följande uppgifter som har lagts in i SIS i enlighet med artikel 38.2 a, b, c och l i denna förordning endast för att kontrollera om de fordon som anmäls för registrering är stulna, bortförda eller försvunna, eller söks som bevis i straffrättsliga förfaranden:

   (a) Uppgifter om motorfordon, enligt definitionen i nationell lagstiftning, oavsett framdrivningssystem.

   (b) Uppgifter om släpvagnar med tjänstevikt på mer än 750 kg och husvagnar.

   (c) Uppgifter som avser stulna, bortförda, försvunna eller ogiltiga registreringsbevis och nummerplåtar för fordon.

   Åtkomst till dessa uppgifter för de enheter som ansvarar för att utfärda registreringsbevis för fordon ska regleras i den medlemsstatens nationella lagstiftning.

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 inte är statliga enheter ska de endast ha indirekt åtkomst till uppgifter i SIS via en myndighet som avses i artikel 43 i denna förordning. 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 iaktta alla begränsningar av användningen av de uppgifter som förmedlats av myndigheten.

4. Artikel 39 i denna förordning ska inte vara tillämplig på åtkomst av det slag som avses i den här artikeln. All förmedling från de enheter som avses i punkt 1 till polis eller andra rättsliga myndigheter av uppgifter som framkommit vid en sökning i SIS och som leder till misstanke om brott ska regleras i nationell lagstiftning.

Artikel 45
Registreringsmyndigheter för fartyg och luftfartyg

1. De enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis eller säkerställa trafikledning för fartyg, även fartygsmotorer, och luftfartyg ska ha

[75] Rådets direktiv 1999/37/EG av den 29 april 1999 om registreringsbevis för fordon (EGT L 138, 1.6.1999, s. 57).

åtkomst till följande uppgifter som lagts in i SIS i enlighet med artikel 38.2 i denna förordning endast för att kontrollera om fartyg, även fartygsmotorer, luftfartyg eller containrar som anmäls för registrering eller görs föremål för trafikledning är stulna, bortförda eller försvunna, eller söks som bevis i straffrättsliga förfaranden:

(a) Uppgifter om fartyg.

(b) Uppgifter om fartygsmotorer.

(c) Uppgifter om luftfartyg.

Om inte annat följer av punkt 2 ska dessa enheters åtkomst till de aktuella uppgifterna regleras i medlemsstaternas lagstiftning. Åtkomst till de uppgifter som förtecknas i led a–c 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 inte är statliga enheter ska de endast ha indirekt åtkomst till uppgifter i SIS via en myndighet som avses i artikel 43 i denna förordning. 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 iaktta alla begränsningar av användningen av de uppgifter som förmedlats av myndigheten.

4. Artikel 39 i denna förordning ska inte vara tillämplig på åtkomst av det slag som avses i den här artikeln. All förmedling från de enheter som avses i punkt 1 till polis eller andra rättsliga myndigheter av uppgifter som framkommit vid en sökning i SIS och som leder till misstanke om brott ska regleras i nationell lagstiftning.

Artikel 46
Europols åtkomst till SIS-uppgifter

1. Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) ska inom ramen för sitt mandat ha rätt att få åtkomst till och söka uppgifter i SIS.

2. Om en sökning som Europol utför visar att det finns en registrering i SIS ska Europol via de kanaler som fastställs i förordning (EU) 2016/794 informera den registrerande medlemsstaten.

3. Användning av uppgifter från sökningar i SIS kräver tillstånd från den berörda medlemsstaten. Om medlemsstaten tillåter användning av uppgifterna, ska Europol behandla dem i enlighet med förordning (EU) 2016/794. Europol får överlämna sådana uppgifter till tredjeländer eller utomstående instanser endast med den berörda medlemsstatens tillstånd.

4. Europol får begära ytterligare upplysningar från den berörda medlemsstaten i enlighet med förordning (EU) 2016/794.

5. Europol ska

(a) utan att det påverkar tillämpningen av punkterna 3, 4 och 6, inte sammankoppla några delar av SIS eller överföra de uppgifter i SIS till vilka byrån har åtkomst till något datasystem för insamling och behandling av uppgifter drivet av eller vid Europol, eller ladda ned eller på annat sätt kopiera några delar av SIS,

(b) begränsa åtkomsten till uppgifter i SIS till personal vid Europol med särskild behörighet,

(c) vidta och tillämpa de åtgärder som avses i artiklarna 10 och 11,

(d) låta Europeiska datatillsynsmannen se över hur Europol utövat rätten att få åtkomst till och söka uppgifter i SIS.

6. Uppgifterna får kopieras endast för tekniska ändamål och i den mån sådan kopiering krävs för att behörig personal vid Europol ska kunna göra direkta sökningar. Dessa kopior ska omfattas av bestämmelserna i denna förordning. Den tekniska kopian ska användas för lagring av SIS-uppgifter medan man söker i uppgifterna. När sökningen av uppgifterna är slutförd ska de raderas. Sådan användning ska inte anses vara en olaglig nedladdning eller kopiering av SIS-uppgifter. Europol får inte kopiera uppgifter om registreringar eller kompletterande uppgifter införda av medlemsstaterna eller uppgifter från CS-SIS till andra Europolsystem.

7. Alla kopior som avses i punkt 6 och som leder till offlinedatabaser får sparas i högst 48 timmar. Denna period kan förlängas i nödsituationer till dess att nödsituationen har upphört. Europol ska rapportera alla sådana förlängningar till Europeiska datatillsynsmannen.

8. Europol får ta emot och behandla tilläggsinformation om motsvarande SIS-registreringar, förutsatt att bestämmelserna om uppgiftsbehandling i punkterna 2–7 tillämpas när så är lämpligt.

9. Europol bör föra loggar över all åtkomst till och sökning i SIS, för att kontrollera om uppgiftsbehandlingen sker på ett lagligt sätt, utföra egenkontroll samt säkerställa en lämplig nivå för uppgifternas säkerhet och integritet. Sådana loggar och sådan dokumentation ska inte anses vara en olaglig nedladdning eller kopiering av någon del av SIS.

Artikel 47
Eurojusts åtkomst till SIS-uppgifter

1. De nationella medlemmarna i Eurojust och deras biträdande medlemmar ska inom sitt mandat ha rätt att få åtkomst till och söka uppgifter som har lagts in i SIS inom 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 han eller hon informera den registrerande medlemsstaten.

3. Ingenting i denna artikel ska tolkas så att det påverkar bestämmelserna i beslut 2002/187/RIF beträffande uppgiftsskydd och ansvaret för otillåten eller felaktig behandling av sådana uppgifter av nationella medlemmar i Eurojust eller deras biträdande medlemmar, eller så att det påverkar befogenheterna för den gemensamma tillsynsmyndighet som inrättats genom det beslutet.

4. Varje åtkomst och varje sökning som utförs av en nationell medlem i Eurojust eller en biträdande medlem ska loggas i enlighet med bestämmelserna i artikel 12 och varje användning av de uppgifter som de fått åtkomst till ska loggas.

5. Ingen del av SIS ska sammankopplas till något annat datasystem för insamling och behandling av uppgifter drivet av eller vid Eurojust, ej heller ska de uppgifter i SIS som de nationella medlemmarna eller deras biträdande medlemmar har åtkomst till överföras till ett sådant datasystem. Ingen del av SIS ska laddas ned. Loggning av

åtkomst och sökningar ska inte anses vara en olaglig nedladdning eller kopiering av SIS-uppgifter.

6. Åtkomst till uppgifter som lagts in i SIS ska begränsas till nationella medlemmar i Eurojust och deras biträdande medlemmar och ska inte beviljas personalen vid Eurojust.

7. Åtgärder för att säkerställa säkerhet och sekretess enligt artiklarna 10 och 11 ska vidtas och tillämpas.

Artikel 48

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

1. I enlighet med artikel 40.8 i förordning (EU) 2016/1624 ska medlemmar i de europeiska gräns- och kustbevakningsenheterna, i enheter som arbetar med återvändande samt i stödgrupperna för migrationshantering, inom ramen för sitt mandat, ha rätt att få åtkomst till och söka uppgifter som har lagts in i SIS inom deras mandat.

2. Medlemmarna i de europeiska gräns- och kustbevakningsenheterna, i enheter som arbetar med återvändande samt i stödgrupperna för migrationshantering ska ha åtkomst till och söka uppgifter i SIS i enlighet med punkt 1 via det tekniska gränssnitt som inrättats och underhålls av Europeiska gräns- och kustbevakningsbyrån i enlighet med artikel 49.1.

3. Om en sökning som utförs av en medlem i de europeiska gräns- och kustbevakningsenheterna, i enheter som arbetar med återvändande eller i stödgrupperna för migrationshantering 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 endast vidta åtgärder utifrån en registrering i SIS i enlighet med anvisningar från och, i 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 tillstånd att agera för dess räkning.

4. Varje åtkomst och varje sökning som utförs av en av medlemmarna i de europeiska gräns- och kustbevakningsenheterna, i enheter som arbetar med återvändande eller i stödgrupperna för migrationshantering ska loggas i enlighet med artikel 12 och all användning av de uppgifter som de fått åtkomst till ska loggas.

5. Åtkomst till uppgifter i SIS ska begränsas till en medlem i de europeiska gräns- och kustbevakningsenheterna, enheter som arbetar med återvändande eller stödgruppen för migrationshantering och ska inte beviljas någon annan medlem i enheten eller gruppen.

6. Åtgärder för att säkerställa säkerhet och sekretess enligt artiklarna 10 och 11 ska vidtas och tillämpas.

Artikel 49

Europeiska gräns- och kustbevakningsbyråns åtkomst till SIS-uppgifter

1. För tillämpning av artikel 48.1 och punkt 2 i denna artikel ska Europeiska gräns- och kustbevakningsbyrån inrätta och underhålla ett tekniskt gränssnitt som möjliggör direktkoppling till det centrala SIS.

2. Europeiska gräns- och kustbevakningsbyrån ska, för att kunna utföra sina uppgifter enligt förordningen om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias), ha rätt att få åtkomst till och söka uppgifter som lagts in i SIS i enlighet med artiklarna 26, 32, 34, 36 och 38.2 j och k.

3. Om en kontroll som Europeiska gräns- och kustbevakningsbyrån utför visar att det finns en registrering i SIS ska det förfarande som anges i artikel 22 i förordningen om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) tillämpas.

4. Ingenting i denna artikel ska tolkas så att det påverkar bestämmelserna i förordning (EU) 2016/1624 beträffande uppgiftsskydd och skadeståndsansvaret om personal vid Europeiska gräns- och kustbevakningsbyrån behandlar uppgifter på ett otillåtet eller felaktigt sätt.

5. Varje åtkomst och varje sökning som utförs av Europeiska gräns- och kustbevakningsbyrån ska loggas i enlighet med bestämmelserna i artikel 12 och varje användning av de uppgifter som den fått åtkomst till ska registreras.

6. Förutom när detta är nödvändigt för tillämpningen av förordningen om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) ska inga delar av SIS vara anslutna till något datasystem för insamling och behandling av uppgifter drivet av eller vid Europeiska gräns- och kustbevakningsbyrån, ej heller ska de SIS-uppgifter som Europeiska gräns- och kustbevakningsbyrån har åtkomst till överföras till ett sådant system. Ingen del av SIS ska laddas ned. Loggning av åtkomst och sökningar ska inte anses vara en nedladdning eller kopiering av SIS-uppgifter.

7. Åtgärder för att säkerställa säkerhet och sekretess enligt artiklarna 10 och 11 ska vidtas och tillämpas av Europeiska gräns- och kustbevakningsbyrån.

Artikel 50
Åtkomsträttens omfattning

Slutanvändarna, däribland Europol, de nationella medlemmarna i Eurojust och deras biträdande medlemmar samt Europeiska gräns- och kustbevakningsbyrån, får endast ha åtkomst till de uppgifter som krävs för att de ska kunna fullgöra sina uppgifter.

Artikel 51
Registreringarnas lagringstid

1. Registreringar som lagts in i SIS enligt denna förordning får inte lagras längre än vad som är nödvändigt för att uppnå de ändamål för vilka de lades in.

2. En medlemsstat som fört in en registrering i SIS ska inom fem år efter inläggandet se över om det är nödvändigt att behålla registreringen. Registreringar som förts in enligt artikel 36 i denna förordning ska sparas i högst ett år.

3. Registreringar om officiella blankodokument och utfärdade id-handlingar vilka lagts in i enlighet med artikel 38 ska sparas i högst tio år. Kortare lagringstider för kategorier av registreringar om föremål får fastställas genom genomförandeåtgärder som antas i enlighet med det granskningsförfarande som avses i artikel 72.2.

4. I förekommande fall ska varje medlemsstat bestämma kortare tidsfrister för denna översyn i enlighet med sin nationella lagstiftning.

5. Om det står klart för personal vid Sirenekontoret, som ansvarar för samordning och kontroll av uppgifternas kvalitet, att en registrering om en person har uppnått sitt

syfte och bör raderas från SIS, ska personalen meddela den myndighet som skapade registreringen för att göra den uppmärksam på saken. Myndigheten ska inom 30 kalenderdagar från det att den mottagit detta meddelande tillkännage att registreringen har raderats eller ska raderas, eller uppge orsakerna till att behålla registreringen. Om 30-dagarsperioden löper ut utan svar ska personalen vid Sirenekontoret radera registreringen. Sirenekontoren ska rapportera eventuella återkommande problem på detta område till sin nationella tillsynsmyndighet.

6. Den medlemsstat som fört in registreringen får inom tidsfristen för översynen efter en övergripande individuell bedömning, som ska dokumenteras, besluta att registreringen ska behållas om detta visar sig nödvändigt för de ändamål för vilka den förts in. I ett sådant fall ska punkt 2 tillämpas även på förlängningen. CS-SIS ska meddelas varje förlängning av registreringens lagringstid.

7. Registreringarna ska raderas automatiskt när tidsfristen för översyn i punkt 2 har löpt ut, om inte den medlemsstat som har fört in registreringen har meddelat CS-SIS att registreringens lagringstid förlängts enligt punkt 6. CS-SIS ska fyra månader i förväg automatiskt informera medlemsstaterna om planerad radering av uppgifter i systemet.

8. Medlemsstaterna ska föra statistik över det antal registreringar vars lagringstid förlängts enligt punkt 6.

KAPITEL XIII

RADERING AV REGISTRERINGAR

Artikel 52
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 kan också raderas om det rättsliga avgörande som registreringen grundades på har återkallats av den behöriga rättsliga myndigheten i enlighet med nationell lagstiftning.

2. Registreringar om försvunna personer ska raderas enligt följande regler:

   (a) När det gäller försvunna barn enligt artikel 32 ska en registrering raderas när

   – ärendet är avslutat, till exempel om barnet har återbördats eller de behöriga myndigheterna i den verkställande medlemsstaten har fattat beslut om vårdnaden av barnet,

   – lagringstiden för registreringen har löpt ut i enlighet med artikel 51,

   – en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom, eller

   – barnet har återfunnits.

   (b) När det gäller försvunna vuxna enligt artikel 32 då inga skyddsåtgärder har begärts ska en registrering raderas när

– den berörda åtgärden har genomförts (den verkställande medlemsstaten har fastställt var personen befinner sig),

– lagringstiden för registreringen har löpt ut i enlighet med artikel 51, eller

– en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.

(c) När det gäller försvunna vuxna då skyddsåtgärder har begärts enligt artikel 32 ska en registrering raderas när

– den berörda åtgärden har genomförts (personen har fått skydd),

– lagringstiden för registreringen har löpt ut i enlighet med artikel 51, eller

– en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.

Om en person har frihetsberövats till följd av ett beslut av en behörig myndighet får en registrering lagras tills dess att personen har återvänt, i enlighet med nationell lagstiftning.

3. Registreringar om försvunna personer som söks för ett rättsligt förfarande ska raderas enligt följande regler:

När det gäller registreringar om personer som söks för ett rättsligt förfarande enligt artikel 34 ska en registrering raderas när

(a) den behöriga myndigheten i den registrerande medlemsstaten har fått besked om var personen befinner sig. Om åtgärder inte kan vidtas avseende den vidarebefordrade informationen ska Sirenekontoret i den registrerande medlemsstaten informera Sirenekontoret i den verkställande medlemsstaten för att lösa problemet,

(b) lagringstiden för registreringen har löpt ut i enlighet med artikel 51, eller

(c) en behörig myndighet i den registrerande medlemsstaten har fattat beslut därom.

Om en av medlemsstaterna har fått en träff och adressuppgifterna har överlämnats till den registrerande medlemsstaten, och en senare träff i den medlemsstaten ger samma adressuppgifter, ska träffen loggas 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 överväga behovet av att behålla registreringen.

4. Registreringar om diskreta kontroller, undersökningskontroller och särskilda kontroller ska raderas enligt följande regler:

När det gäller registreringar om diskreta kontroller, undersökningskontroller och särskilda kontroller enligt artikel 36 ska en registrering raderas när

(a) lagringstiden för registreringen har löpt ut i enlighet med artikel 51,

(b) en behörig myndighet i den registrerande medlemsstaten har fattat beslut om radering.

5. Registreringar om föremål som ska beslagtas eller användas som bevis i brottmål ska raderas enligt följande regler:

När det gäller radering av registreringar om föremål som ska beslagtas eller användas som bevis i brottmål enligt artikel 38 ska en registrering raderas när

(a) föremålet har beslagtagits eller motsvarande åtgärder har vidtagits och det därav följande nödvändiga utbytet av tilläggsinformation har skett mellan Sirenekontoren eller föremålet omfattas av ett annat rättsligt eller administrativt förfarande,

(b) lagringstiden för registreringen har löpt ut, eller

(c) en behörig myndighet i den registrerande medlemsstaten har fattat beslut om radering.

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

7. (a) personen har identifierats, eller

8. (b) lagringstiden för registreringen har löpt ut.

KAPITEL XIV

ALLMÄNNA REGLER FÖR UPPGIFTSBEHANDLING

Artikel 53
Behandling av SIS-uppgifter

1. Medlemsstaterna får behandla de uppgifter som avses i artikel 20 endast för de ändamål som anges för respektive registreringskategori i artiklarna 26, 32, 34, 36, 38 och 40.

2. Uppgifterna får kopieras endast för tekniska ändamål och i den mån sådan kopiering krävs för att de myndigheter som avses i artikel 43 ska kunna utföra en direkt sökning. Dessa kopior ska omfattas av bestämmelserna i denna förordning. En medlemsstat får inte kopiera uppgifter om registreringar eller kompletterande uppgifter som lagts in av en annan medlemsstat från sitt N.SIS eller från CS-SIS till andra nationella dataregister.

3. Kopior av teknisk karaktär enligt punkt 2, vilka leder till offlinedatabaser, får lagras i högst 48 timmar. Denna period kan förlängas i nödsituationer till dess att nödsituationen har upphört.

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

5. Åtkomst till uppgifter ska endast beviljas behörig personal vid de nationella myndigheter som avses i artikel 43 inom gränserna för deras behörighet.

6. 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 dessa registreringar för andra ändamål än de för vilka uppgifterna lades in i SIS länkas till ett specifikt fall och motiveras av behovet av att avvärja en överhängande allvarlig fara för den allmänna ordningen och säkerheten, en betydande risk för den nationella säkerheten eller ett

grovt brott. Den medlemsstat som fört in registreringen ska i förväg ge sitt tillstånd till detta.

7. All användning av uppgifter som inte är förenlig med punkterna 1–6 ska betraktas som missbruk enligt varje medlemsstats nationella lagstiftning.

8. Varje medlemsstat ska till byrån sända in en förteckning över sina behöriga myndigheter som har tillstånd att direkt söka uppgifter i SIS enligt denna förordning, samt alla ändringar i förteckningen. I förteckningen ska för varje myndighet anges vilka uppgifter den får söka och för vilka ändamål. Byrån ska säkerställa årligt offentliggörande av förteckningen i *Europeiska unionens officiella tidning*.

9. Om inga särskilda bestämmelser föreskrivs i unionslagstiftningen, ska varje medlemsstats nationella lagstiftning gälla för de uppgifter den lägger in i sitt N.SIS.

Artikel 54
Uppgifter i SIS och nationella informationssystem

1. Artikel 53.2 ska inte påverka en medlemsstats rätt att i sina nationella system lagra SIS-uppgifter rörande åtgärder som har vidtagits inom dess territorium. Dessa uppgifter får lagras högst tre år i de nationella systemen, om inte särskilda bestämmelser i nationell lagstiftning tillåter att uppgifterna lagras under en längre period.

2. Artikel 53.2 ska inte påverka en medlemsstats rätt att i sina nationella system lagra uppgifterna i en registrering som medlemsstaten själv har fört in i SIS.

Artikel 55
Information om att registrering inte verkställs

Om en begärd åtgärd inte kan vidtas, ska den anmodade medlemsstaten omedelbart informera den registrerande medlemsstaten.

Artikel 56
SIS-uppgifternas kvalitet

1. En medlemsstat som för in en registrering ska ansvara för att säkerställa att uppgifterna är riktiga, aktuella och läggs in i SIS lagligen.

2. Endast den medlemsstat som för in en registrering ska ha tillstånd att ändra, komplettera, rätta, uppdatera eller radera de uppgifter som den har lagt in.

3. Om en annan medlemsstat än den registrerande medlemsstaten har bevis för att en uppgift är 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 tio dagar 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.

4. Om medlemsstaterna inte kan enas inom två månader efter det att man fick kännedom om bevisen, enligt punkt 3, ska den medlemsstat som inte förde in registreringen överlämna ärendet till de berörda nationella tillsynsmyndigheterna för beslut.

5. Medlemsstaterna ska utbyta tilläggsinformation om en person hävdar att han eller hon inte är den person som efterlysts genom en registrering. Om det vid kontroll visar sig att det faktiskt rör sig om två olika personer, ska klaganden underrättas om de åtgärder som fastställs i artikel 59.

6. Om en person redan omfattas av en registrering i SIS ska den medlemsstat som lägger in ytterligare en registrering komma överens om inläggandet med den medlemsstat som lade in den första registreringen. Överenskommelse ska nås genom utbyte av tilläggsinformation.

Artikel 57
Säkerhetstillbud

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

2. Säkerhetstillbud ska hanteras på ett sätt som säkerställer en snabb, effektiv och välavvägd reaktion.

3. Medlemsstaterna ska underrätta kommissionen, byrån och de nationella tillsynsmyndigheterna om säkerhetstillbud. Byrån ska underrätta kommissionen och Europeiska datatillsynsmannen om säkerhetstillbud.

4. Information om ett säkerhetstillbud som har eller kan ha påverkat driften av SIS i en medlemsstat eller inom byrån, eller tillgängligheten, integriteten och konfidentialiteten hos de uppgifter som lagts in eller sänts av andra medlemsstater ska ges till medlemsstaterna och rapporteras i enlighet med den tillbudshanteringsplan som byrån tillhandahåller.

Artikel 58
Särskiljande av personer med snarlika kännetecken

Om det, när en ny registrering läggs in, framkommer att det i SIS redan finns en person med samma identitetsuppgifter ska följande förfarande tillämpas:

(a) Sirenekontoret ska kontakta den ansökande myndigheten för att klarlägga om det rör sig om samma person.

(b) Om kontrollen visar att den person som omfattas av den nya registreringen och den person som redan är registrerad i SIS faktiskt är en och samma person, ska Sirenekontoret tillämpa det förfarande för inläggande av flera registreringar som anges i artikel 56.6. Om kontrollen visar att det rör sig om två olika personer, ska Sirenekontoret godkänna begäran om att lägga in den andra registreringen genom att tillfoga sådan information som krävs för att undvika felidentifiering.

Artikel 59
Kompletterande uppgifter för att komma till rätta med missbruk av identitet

1. Om den person som faktiskt avses i en registrering kan förväxlas med en person vars identitet har missbrukats, ska den registrerande medlemsstaten, om den sistnämnda personen har lämnat sitt uttryckliga medgivande, tillfoga uppgifter om denna i

registreringen för att undvika de negativa följder som en felidentifiering kan medföra.

2. Uppgifter om en person vars identitet har missbrukats får användas endast för följande ändamål:

   (a) För att göra det möjligt för den behöriga myndigheten att skilja mellan den person vars identitet har missbrukats och den person som faktiskt avses i registreringen.

   (b) För att göra det möjligt för den person vars identitet har missbrukats att styrka sin identitet och fastställa att den har blivit missbrukad.

3. Vid tillämpningen av denna artikel får enbart följande personuppgifter läggas in och vidarebehandlas i SIS:

   (a) Samtliga efternamn.

   (b) Samtliga förnamn.

   (c) Namn vid födelsen.

   (d) Tidigare använda namn och alias, eventuellt inlagda separat.

   (e) Särskilda, objektiva, fysiska kännetecken som inte förändras.

   (f) Födelseort.

   (g) Födelsedatum.

   (h) Kön.

   (i) Fotografier och ansiktsbilder.

   (j) Fingeravtryck.

   (k) Medborgarskap.

   (l) Id-handlingens kategori.

   (m) Det land som utfärdat id-handlingen.

   (n) Id-handlingens nummer.

   (o) Id-handlingens utfärdandedatum.

   (p) Offrets adress.

   (q) Offrets fars namn.

   (r) Offrets mors namn.

4. De tekniska föreskrifter som behövs för att lägga in och vidarebehandla de uppgifter som avses i punkt 3 ska fastställas genom genomförandeåtgärder som fastställs och utvecklas i enlighet med det granskningsförfarande som avses i artikel 72.2.

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 rätt att få åtkomst till motsvarande registrering ska få se de uppgifter som avses i punkt 3. Detta får ske endast för att undvika felidentifiering.

Artikel 60
Länkning mellan registreringar

1. En medlemsstat får skapa en länk mellan de registreringar den lägger 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 någon av de länkade registreringarnas lagringstid.

3. Skapandet av en länk ska inte påverka de åtkomsträttigheter som anges i denna förordning. Myndigheter som inte har åtkomst 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 finner att en länk som en annan medlemsstat skapat mellan registreringar är oförenlig med dess nationella lagstiftning eller 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. Tekniska föreskrifter om länkning av registreringar ska fastställas och utvecklas i enlighet med det granskningsförfarande som avses i artikel 72.2.

Artikel 61
Tilläggsinformationens ändamål 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 registrerats hos Sirenekontoret till följd av informationsutbyte ska lagras endast under så lång tid som kan behövas för att uppnå de ändamål för vilka de tillhandahölls. 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 systemet ska fastställas i den nationella lagstiftningen.

Artikel 62
Överföring av personuppgifter till tredje man

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

Artikel 63

Utbyte med Interpol av uppgifter om stulna, bortförda, borttappade eller ogiltigförklarade pass

1. Trots vad som föreskrivs i artikel 62 får uppgifter som lagts in i SIS om stulna, bortförda, borttappade eller ogiltigförklarade pass vilka avser passnummer, utfärdande land och dokumenttyp utbytas med medlemmar i Interpol, genom att en länk upprättas mellan SIS och Interpols databas för stulna eller saknade resehandlingar, under förutsättning att ett avtal har ingåtts mellan Interpol och Europeiska unionen. I avtalet ska det föreskrivas att överföringen av uppgifter som lagts in av en medlemsstat ska godkännas av den medlemsstaten.

2. I det avtal som avses i punkt 1 ska det föreskrivas att de uppgifter som delas ska vara tillgängliga enbart för medlemmar i Interpol från länder som säkerställer en tillräcklig skyddsnivå för personuppgifter. Innan detta avtal sluts ska rådet höra kommissionen om lämplig skyddsnivå för personuppgifter och respekt för grundläggande rättigheter och friheter med avseende på automatisk behandling av personuppgifter vid Interpol och de länder som har delegerade medlemmar i Interpol.

3. I det avtal som avses i punkt 1 kan det även föreskrivas åtkomst för medlemsstaterna till uppgifter från Interpols databas om stulna eller saknade resehandlingar genom SIS, i enlighet med relevanta bestämmelser i denna förordning om hur registreringar om stulna, bortförda, borttappade eller ogiltigförklarade pass ska läggas in i SIS.

KAPITEL XV

UPPGIFTSSKYDD

Artikel 64

Tillämplig lagstiftning

1. Förordning (EG) nr 45/2001 ska tillämpas på byråns behandling av personuppgifter inom ramen för denna förordning.

2. Förordning (EU) 2016/679 ska tillämpas på behandlingen av personuppgifter i de fall där de nationella bestämmelser som införlivar direktiv (EU) 2016/680 inte är tillämpliga.

3. När de behöriga nationella myndigheterna behandlar uppgifter för att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder inbegripet skyddsåtgärder för att förebygga hot mot den allmänna säkerheten, ska de nationella bestämmelser som införlivar direktiv (EU) 2016/680 tillämpas.

Artikel 65

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

1. Registrerades åtkomsträtt till uppgifter som har lagts in i SIS om dem och deras rätt att få dessa uppgifter rättade eller raderade ska utövas enligt den nationella lagstiftningen i den medlemsstat i vilken de åberopar denna rätt.

2. Om så föreskrivs i den nationella lagstiftningen ska den nationella tillsynsmyndigheten avgöra om uppgifterna får lämnas ut och förfarandet för detta.

3. En annan medlemsstat än den som fört in registreringen får lämna ut information om sådana uppgifter endast om den i förväg har gett den registrerande medlemsstaten tillfälle att meddela sin ståndpunkt. Detta ska göras genom utbyte av tilläggsinformation.

4. En medlemsstat får besluta att endast delvis eller inte alls lämna ut information till den registrerade, i enlighet med nationell lagstiftning, i den mån som och så länge som en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle med vederbörlig hänsyn till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, för att

   (a) inte försvåra officiella eller rättsliga utredningar, undersökningar eller förfaranden,

   (b) inte skada insatser för att förebygga, upptäcka, utreda eller lagföra brott eller verkställa straffrättsliga påföljder,

   (c) skydda den allmänna säkerheten,

   (d) skydda den nationella säkerheten,

   (e) skydda andra personers rättigheter och friheter.

5. Alla personer har rätt att få oriktiga uppgifter om sig själva rättade och olagligt lagrade uppgifter om sig själva raderade.

6. Den berörda personen ska informeras så snart som möjligt, dock senast 60 dagar räknat från dagen för begäran om åtkomst, eller tidigare om en kortare tidsfrist följer av nationell rätt.

7. Den berörda personen ska så snart som möjligt informeras om vilka åtgärder som vidtas till följd av begäran om rättelse och radering, dock senast tre månader räknat från dagen för begäran, eller tidigare om en kortare tidsfrist följer av nationell rätt.

Artikel 66
Rättsmedel

1. Var och en ska kunna få sin sak prövad i domstol eller vid den myndighet som är behörig enligt varje medlemsstats nationella lag, för att få åtkomst till, rätta, radera eller erhålla information eller få gottgörelse i samband med en registrering som berör dem.

2. Utan att det påverkar tillämpningen av artikel 70 förbinder sig medlemsstaterna ömsesidigt att verkställa slutliga avgöranden som har meddelats av sådana domstolar eller myndigheter som avses i punkt 1 i denna artikel.

3. För att få en enhetlig översikt av hur rättsmedlen fungerar ska de nationella myndigheterna utarbeta ett standardiserat statistiskt system för årlig rapportering om

   (a) hur många gånger registrerade begärt åtkomst hos registeransvariga och hur många gånger åtkomst till uppgifterna beviljats,

   (b) hur många gånger registrerade begärt åtkomst hos nationella tillsynsmyndigheter och hur många gånger åtkomst till uppgifterna beviljats,

   (c) hur många gånger rättelse av oriktiga uppgifter och radering av olagligt lagrade uppgifter begärts hos registeransvariga och i hur många fall uppgifterna rättats eller raderats,

(d) hur många gånger rättelse av oriktiga uppgifter eller radering av olagligt lagrade uppgifter begärts hos den nationella tillsynsmyndigheten,

(e) hur många ärenden som prövats i domstol,

(f) hur många ärenden som lett till att domstolen gett den klagande rätt i någon del av ärendet,

(g) anmärkningar avseende det ömsesidiga erkännandet av slutliga avgöranden från andra medlemsstaters domstolar eller myndigheter om registreringar som skapats av den registrerande medlemsstaten.

Rapporterna från de nationella tillsynsmyndigheterna ska översändas inom ramen för det samarbete som fastställs i artikel 69.

Artikel 67
Tillsyn över N.SIS

1. Varje medlemsstat ska säkerställa att den eller de nationella tillsynsmyndigheter som utses i medlemsstaten, med de befogenheter som avses i kapitel VI i direktiv (EU) 2016/680 eller kapitel VI i förordning (EU) 2016/679, på ett oberoende sätt övervakar lagenligheten i behandlingen av personuppgifter i SIS inom deras territorium, överföringen av uppgifterna från deras territorium samt utbytet och vidarebehandlingen av tilläggsinformation.

2. Den nationella tillsynsmyndigheten ska säkerställa att en revision av behandlingen av uppgifterna i N.SIS genomförs minst vart fjärde år i enlighet med internationella revisionsstandarder. Den eller de nationella tillsynsmyndigheterna ska antingen utföra revisionen själv eller begära den direkt från en oberoende uppgiftsskyddsrevisor. Revisorn ska fortlöpande kvarstå under den nationella tillsynsmyndighetens kontroll och ansvar.

3. Medlemsstaterna ska säkerställa att deras nationella tillsynsmyndighet har de resurser som krävs för att fullgöra de uppgifter som den åläggs enligt denna förordning.

Artikel 68
Tillsyn över byrån

1. Europeiska datatillsynsmannen ska säkerställa att byråns behandling av personuppgifter utförs i enlighet med denna förordning. De uppgifter och befogenheter som avses i artiklarna 46 och 47 i förordning (EG) nr 45/2001 ska tillämpas i enlighet därmed.

2. Europeiska datatillsynsmannen ska säkerställa att en revision av byråns behandling av personuppgifter genomförs minst vart fjärde år i enlighet med internationella revisionsstandarder. En rapport från denna revision ska sändas till Europaparlamentet, rådet, byrån, kommissionen och de nationella tillsynsmyndigheterna. Byrån ska ges tillfälle att yttra sig innan rapporten antas.

Artikel 69
Samarbete mellan de nationella tillsynsmyndigheterna och Europeiska datatillsynsmannen

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

2. De ska inom ramen för sina respektive befogenheter utbyta relevant information, bistå varandra vid utförandet av revisioner och inspektioner, utreda svårigheter med tolkningen eller tillämpningen av denna förordning och andra tillämpliga akter i unionslagstiftningen, undersöka problem som framkommer i samband med utövandet av oberoende tillsyn eller de registrerades rättigheter, utarbeta harmoniserade förslag till gemensamma lösningar på eventuella problem samt i förekommande fall främja medvetenheten om rättigheterna i fråga om uppgiftsskydd.

3. För de ändamål som anges i punkt 2 ska de nationella tillsynsmyndigheterna och Europeiska datatillsynsmannen hålla minst två möten om året inom ramen för Europeiska dataskyddsstyrelsen, som inrättades genom förordning (EU) nr 2016/679. Den styrelse som inrättades genom förordning (EU) nr 2016/679 ska stå för kostnaderna och tillhandahålla tjänster för dessa möten. En arbetsordning ska antas vid det första mötet. Ytterligare arbetsrutiner ska vid behov utvecklas gemensamt.

4. En gemensam verksamhetsrapport om samordnad tillsyn ska vartannat år översändas av den styrelse som inrättades genom förordning (EU) nr 2016/679 till Europaparlamentet, rådet och kommissionen.

KAPITEL XVI

ANSVAR

Artikel 70
Skadeståndsansvar

1. Varje medlemsstat ska vara skadeståndsansvarig för skada som åsamkas personer genom användningen av N.SIS. Detta ska även gälla skador som orsakats av den registrerande medlemsstaten, om medlemsstaten lagt in oriktiga uppgifter eller lagrat uppgifter på ett olagligt sätt.

2. Om den medlemsstat mot vilken talan väcks inte är registrerande medlemsstat ska den registrerande medlemsstaten på begäran ersätta utbetalade skadeståndsbelopp, såvida inte den medlemsstat som begär ersättning har använt uppgifterna i strid med denna förordning.

3. Om en medlemsstat underlåter att uppfylla sina skyldigheter enligt denna förordning och detta leder till skada för SIS ska den medlemsstaten hållas ansvarig för skadan, såvida inte byrån eller andra medlemsstater som deltar i SIS har underlåtit att vidta rimliga åtgärder för att förhindra skadan eller begränsa dess verkningar.

KAPITEL XVII

SLUTBESTÄMMELSER

Artikel 71
Övervakning och statistik

1. Byrån ska säkerställa att rutiner inrättas för att övervaka hur SIS fungerar i förhållande till målsättningarna i fråga om produktivitet, kostnadseffektivitet, säkerhet och tjänsternas kvalitet.

2. Byrån ska ha tillgång till nödvändiga upplysningar om uppgiftsbehandlingen i det centrala SIS för tekniskt underhåll, rapportering och statistik.

3. Byrån ska utarbeta daglig, månatlig och årlig statistik som visar antalet loggningsnoteringar per registreringskategori, det årliga antalet träffar per registreringskategori, hur många gånger SIS använts för sökningar och hur många gånger SIS använts för att lägga in, uppdatera eller radera registreringar totalt och för varje medlemsstat. Den statistik som utarbetas ska inte innehålla några personuppgifter. Den årliga statistiska rapporten ska offentliggöras. Byrån ska även tillhandahålla årlig statistik om användningen av funktionen att göra en registrering som förts in enligt artikel 26 i denna förordning tillfälligt otillgänglig för sökningar, totalt och för varje medlemsstat, inbegripet förlängningar av 48-timmarsperioden.

4. Medlemsstaterna, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån ska tillställa byrån och kommissionen den information som de behöver för att utarbeta de rapporter som avses i punkterna 3, 7 och 8. Denna information ska omfatta separat statistik om det antal 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, luftfartyg och containrar, eller på dessas vägnar. Statistiken ska också visa antalet träffar per registreringskategori.

5. Byrån ska tillställa medlemsstaterna, kommissionen, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån alla statistiska rapporter den har utarbetat. För att övervaka genomförandet av unionens rättsakter ska kommissionen kunna begära att byrån regelbundet eller för särskilda ändamål tillhandahåller ytterligare specifika statistiska rapporter om hur SIS och Sirenekommunikationen fungerar och används.

6. För tillämpningen av punkterna 3, 4 och 5 i denna artikel och artikel 15.5 ska byrån inrätta, implementera och i sina tekniska lokaler hysa en central databas med de uppgifter som avses i punkt 3 i denna artikel och i artikel 15.5 vilka inte möjliggör identifiering av enskilda personer men gör det möjligt för kommissionen och de byråer som anges i punkt 5 att få skräddarsydd rapportering och statistik. Enbart för rapporterings- och statistikändamål ska byrån ge medlemsstaterna, kommissionen, Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån säker åtkomst till den centrala databasen via kommunikationsinfrastrukturen med åtkomstkontroll och specifika användarprofiler.

   Närmare bestämmelser om driften av den centrala databasen och de bestämmelser om uppgiftsskydd och säkerhet som är tillämpliga på databasen ska antas genom

genomförandeåtgärder i enlighet med det granskningsförfarande som avses i artikel 72.2.

7. Två år efter det att SIS tagits i drift och vartannat år därefter ska byrån förse Europaparlamentet och rådet med en rapport om hur det centrala SIS och kommunikationsinfrastrukturen fungerat tekniskt, om säkerheten och om det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstaterna.

8. Tre år efter det att SIS tagits i drift och vart fjärde år därefter ska kommissionen göra en övergripande utvärdering av det centrala SIS och det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstaterna. Den övergripande utvärderingen ska granska uppnådda resultat i relation till målen och bedöma om de ursprungliga förutsättningarna fortfarande är aktuella, hur denna förordning tillämpats på det centrala SIS, säkerheten i det centrala SIS och om några slutsatser kan dras beträffande den framtida verksamheten. Kommissionen ska överlämna utvärderingen till Europaparlamentet och rådet.

Artikel 72
Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté enligt förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 73
Ändringar av förordning (EU) nr 515/2014

Förordning (EU) nr 515/2014[76] ska ändras på följande sätt:

I artikel 6 ska följande införas som punkt 6:

”6. Under utvecklingsfasen ska medlemsstaterna tilldelas ett extra anslag på 36,8 miljoner euro som ska fördelas som ett engångsbelopp till deras grundanslag och som i sin helhet ska användas för de nationella SIS-systemen för att säkerställa att de snabbt och effektivt uppgraderas parallellt med genomförandet av det centrala SIS enligt kraven i förordning (EU) 2018/...* och förordning (EU) 2018/...**

**Förordning om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete och i förordning (EUT....*

***Förordning (EU) 2018/... om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller och i förordning (EUT...)”.*

Artikel 74
Upphävande

Den dag då denna förordning börjar tillämpas ska följande rättsakter upphöra att gälla:

[76] Europaparlamentets och rådets förordning (EU) nr 515/2014 av den 16 april 2014 om inrättande, som en del av fonden för inre säkerhet, av ett instrument för ekonomiskt stöd för yttre gränser och visering (EUT L 150, 20.5.2014, s. 143).

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.

Rådets beslut 533/2007/RIF av den 12 juli 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II).

Kommissionens beslut 2010/261/EU av den 4 maj 2010 om en säkerhetsplan för det centrala SIS II och kommunikationsinfrastrukturen[77].

Artikel 75
Ikraftträdande och tillämpning

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

2. Den ska tillämpas från och med den dag som kommissionen fastställer efter det att

   (a) de nödvändiga genomförandeåtgärderna 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) byrån har underrättat kommissionen om att alla tester avseende CS-SIS och samspelet mellan CS-SIS och N.SIS har slutförts.

3. Denna förordning är till alla delar bindande och direkt tillämplig i medlemsstaterna i enlighet med fördraget om Europeiska unionens funktionssätt.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

[77] 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).

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen

1.3. Typ av förslag eller initiativ

1.4. Mål

1.5. Motivering till förslaget eller initiativet

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

1.7. Planerad metod för genomförandet

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

2.2. Administrations- och kontrollsystem

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

3.2.2. Beräknad inverkan på driftsanslagen

3.2.3. Beräknad inverkan på anslag av administrativ natur

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3.3. Beräknad inverkan på inkomsterna

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring av förordning (EU) nr 515/2014 och om upphävande av förordning (EG) nr 1986/2006, rådets beslut 2007/533/RIF och kommissionens beslut 2010/261/EU.

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen[78]

Politikområde: Migration och inrikes frågor (avdelning 18)

1.3. Typ av förslag eller initiativ

☐ **Ny åtgärd**

☐ **Ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd[79]**

☑ **Befintlig åtgärd vars genomförande förlängs i tiden**

☐ **Tidigare åtgärd som omformas till eller ersätts av en ny**

1.4. Mål

1.4.1. Fleråriga strategiska mål för kommissionen som förslaget eller initiativet är avsett att bidra till

Mål – ”Störa organiserad brottslighet”

Mål – ”En stark EU-insats för att bekämpa terrorism och förebygga radikalisering”

Kommissionen har vid ett flertal tillfällen framhållit vikten av att se över den rättsliga grunden för SIS i syfte att ta itu med nya säkerhets- och migrationsutmaningar. I *Europeiska säkerhetsagendan*[80] tillkännagav kommissionen till exempel sin avsikt att utvärdera SIS under 2015–2016 och bedöma om det finns nya operativa behov som kräver ändringar i lagstiftningen. Dessutom betonades i säkerhetsagendan att SIS utgör kärnan i polismyndigheternas informationsutbyte och bör stärkas ytterligare. Mer nyligen konstaterade kommissionen i sitt meddelande *Starkare och smartare informationssystem för gränser och säkerhet*[81] att tilläggsfunktioner i systemet kommer att övervägas på grundval av den övergripande utvärderingsrapporten med avsikt att lägga fram förslag till ändring av den rättsliga grunden för SIS. Slutligen föreslog kommissionen den 20 april 2016 i sitt meddelande *Att genomföra den europeiska säkerhetsagendan mot terrorism och bana väg för en säkerhetsunion*[82] ett antal ändringar i SIS för att förbättra systemets mervärde vid brottsbekämpning.

---

78 Verksamhetsbaserad förvaltning och verksamhetsbaserad budgetering benämns ibland med de interna förkortningarna ABM respektive ABB.

79 I den mening som avses i artikel 54.2 a eller b i budgetförordningen.

80 COM(2015) 185 final.

81 COM(2016) 205 final.

82 COM(2016) 230 final.

Den övergripande utvärdering som utfördes av kommissionen bekräftade att SIS är en operativ framgång. Trots de många positiva sidorna gjordes dock också ett flertal rekommendationer i utvärderingen, med målet att förbättra systemets tekniska och operativa ändamålsenlighet och effektivitet.

På grundval av rekommendationerna i den övergripande utvärderingsrapporten och helt i linje med kommissionens mål som anges i de meddelanden som nämns ovan och den strategiska planen 2016–2020 för GD Migration och inrikes frågor[83], är syftet med detta förslag att genomföra

- kommissionens tillkännagivande om att förbättra SIS:s mervärde vid brottsbekämpning för att svara på nya hot,
- rekommendationer om tekniska och förfarandemässiga ändringar, på grundval av en övergripande utvärdering av SIS,
- slutanvändarnas begäranden om tekniska förbättringar,
- de preliminära resultaten från expertgruppen för informationssystem och interoperabilitet i fråga om uppgifternas kvalitet.

1.4.2. Specifika mål eller verksamheter inom den verksamhetsbaserade förvaltningen och budgeteringen som berörs

Specifikt mål nr…

Förvaltningsplan för GD Migration och inrikes frågor 2017

Specifikt mål 2.1 – En stark EU-insats för att bekämpa terrorism och förebygga radikalisering.

Specifikt mål 2.2 – Störa grov och organiserad gränsöverskridande brottslighet.

Berörda verksamheter enligt den verksamhetsbaserade förvaltningen och budgeteringen

Kapitel 18 02 – Inre säkerhet

[83] Ares(2016) 2231546 – 12.5.2016.

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

Det huvudsakliga målet med de föreslagna rättsliga och tekniska ändringarna i SIS är att effektivisera driften av systemet. Den övergripande utvärdering av SIS som genomfördes av GD Migration och inrikes frågor 2015–2016 ledde till rekommendationer om tekniska förbättringar av systemet och harmonisering av nationella förfaranden när det gäller samarbete inom brottsbekämpning.

Genom det nya förslaget införs åtgärder som beaktar slutanvändarnas operationella och tekniska behov. I synnerhet kommer nya uppgiftsfält för befintliga registreringar att göra det möjligt för poliser att få all den information de behöver för att utföra sina uppgifter effektivt. Dessutom framhålls i förslaget särskilt betydelsen av oavbruten tillgång till SIS, eftersom driftsavbrott kan få betydande konsekvenser för arbetet för tjänstemän inom brottsbekämpning. Detta förslag innehåller därutöver tekniska ändringar som kommer att göra systemet effektivare och enklare.

När dessa förslag väl har antagits och genomförts kommer de också att leda till ökad driftskontinuitet, eftersom medlemsstaterna blir skyldiga att ha en fullständig eller partiell nationell kopia och en backup av denna. Tack vare detta kommer systemet att kontinuerligt vara fullt funktionsdugligt och i drift för tjänstemän på fältet.

Genom förslaget införs nya biometriska kännetecken – handavtryck, ansiktsbilder och DNA-profiler i särskilda och begränsade fall. Tillsammans med de planerade ändringarna av artiklarna 32 och 33 (registreringar om försvunna personer) för att möjliggöra inläggande av förebyggande registreringar och kategorisering av typen av försvinnande kommer detta, för det första, att stärka skyddet avsevärt för ensamkommande barn och, för det andra, att göra det möjligt att identifiera dem på grundval av deras DNA-profiler eller deras föräldrars och/eller syskons DNA-profiler (med medgivande).

Medlemsstaternas myndigheter kommer också att kunna föra in registreringar om okända personer som efterlysts i samband med ett brott, helt på grundval av fingeravtryck eller handavtryck av latent typ eller från en brottsplats. Detta är inte möjligt enligt den befintliga rättsliga och tekniska ramen och innebär därför ett viktigt steg i utvecklingen.

1.4.4. Indikatorer för bedömning av resultat eller verkan

Ange vilka indikatorer som ska användas för att följa upp hur förslaget eller initiativet genomförs.

Medan systemet uppgraderas:

Efter det att förslaget har godkänts och de tekniska specifikationerna antagits kommer SIS att uppgraderas för att bättre harmonisera de nationella förfarandena för användningen av systemet, utvidga systemets tillämpningsområde genom att det införs nya inslag i befintliga registreringskategorier och införa tekniska ändringar för att förbättra säkerheten och minska administrativa bördor. eu-LISA kommer att samordna projektledningen av systemuppgraderingen. eu-LISA kommer att inrätta en projektledningsstruktur och tillhandahålla en detaljerad tidsplan med milstolpar för genomförandet av de föreslagna ändringarna, vilket kommer att göra det möjligt för kommissionen att noggrant övervaka genomförandet av förslaget.

Specifikt mål – De uppdaterade funktionerna i SIS ska tas i bruk under 2020

Indikator – Ett lyckat genomförande av omfattande tester av det uppdaterade systemet innan det lanseras.

När systemet tagits i drift:

När systemet väl har tagits i drift ska eu-LISA säkerställa att det finns förfaranden för övervakning av hur Schengens informationssystem fungerar i förhållande till de mål som rör produktion, kostnadseffektivitet, säkerhet och tjänsternas kvalitet. Två år efter det att SIS tagits i drift och vartannat år därefter ska eu-LISA för Europaparlamentet och rådet lägga fram en rapport om den tekniska funktionen hos det centrala SIS och kommunikationsinfrastrukturen, inklusive dess säkerhet, och det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstater. Dessutom utarbetar eu-LISA daglig, månatlig och årlig statistik som visar antalet loggningsnoteringar per registreringskategori, det årliga antalet träffar per registreringskategori, hur många gånger SIS använts för sökningar och hur många gånger SIS använts för att lägga in, uppdatera eller radera registreringar totalt och för varje medlemsstat. Utöver detta kommer byrån även att tillhandahålla årlig statistisk om användningen av funktionen att göra en registrering som förts in enligt artikel 26 i denna förordning tillfälligt otillgänglig för sökningar, totalt och för varje medlemsstat, inbegripet förlängningar av 48-timmarsperioden.

Tre år efter det att SIS tagits i drift och vart fjärde år därefter utarbetar kommissionen en övergripande utvärdering av det centrala SIS och det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstater. Den övergripande utvärderingen granskar uppnådda resultat i relation till målen och bedömer om de ursprungliga förutsättningarna fortfarande är aktuella, hur denna förordning tillämpats på det centrala SIS, säkerheten i det centrala SIS och om några slutsatser kan dras beträffande den framtida verksamheten. Kommissionen kommer att överlämna utvärderingen till Europaparlamentet och rådet.

Specifikt mål 1 – Störa organiserad brottslighet.

Indikator – Användning av EU:s mekanismer för informationsutbyte. Detta kan mätas genom ett ökat antal träffar i SIS. Indikatorerna är de statistiska rapporterna från eu-LISA och medlemsstaterna. De kommer att göra det möjligt för kommissionen att bedöma hur de nya funktionerna i systemet används.

Specifikt mål 2 – En stark EU-insats för att bekämpa terrorism och förebygga radikalisering.

Indikator – Ökning av antalet registreringar och träffar, i synnerhet avseende artikel 36.3 i förslaget, för registreringar om personer och föremål för diskreta kontroller, undersökningskontroller eller särskilda kontroller.

1.5. Motivering till förslaget eller initiativet

1.5.1. Behov som ska tillgodoses på kort eller lång sikt

1. Att bibehålla en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i EU.

2. Att bättre harmonisera de nationella förfarandena för användningen av SIS.

3. Att utvidga förteckningen över institutionella användare med åtkomst till SIS-uppgifter genom att ge Europol och den nya europeiska gräns- och kustbevakningen full åtkomst till systemet.

4. Att införa nya inslag i SIS-registreringar och nya funktioner för att utvidga systemets tillämpningsområde, utrusta det för den aktuella säkerhetsmiljön, förbättra samarbetet mellan medlemsstaternas brottsbekämpande myndigheter och säkerhetsmyndigheter samt minska den administrativa bördan.

5. Att beakta den genomgående användningen av SIS för att inte bara omfatta de centrala och nationella systemen utan även säkerställa att slutanvändarna får alla uppgifter de behöver för att utföra sina uppgifter.

6. Att stärka driftskontinuiteten och säkerställa oavbruten drift av SIS på central och nationell nivå.

7. Att förstärka kampen mot internationell brottslighet, terrorism och it-brottslighet som sammankopplade områden med en stark gränsöverskridande dimension.

1.5.2. Mervärdet av en åtgärd på unionsnivå

SIS är den viktigaste säkerhetsdatabasen i Europa. Utan inre gränskontroller har den praktiska bekämpningen av brottslighet och terrorism fått en europeisk dimension. Förslagets mål avser tekniska förbättringar för att öka systemets effektivitet och ändamålsenlighet och att harmonisera användingen i alla deltagande medlemsstater. Den gränsöverskridande karaktären hos dessa mål, tillsammans med utmaningarna med att säkerställa ett effektivt informationsutbyte för att bekämpa ständigt föränderliga hot, innebär att EU är bäst lämpat att föreslå lösningar på dessa problem. Målen att öka effektiviteten och harmonisera användningen av SIS, dvs. en ökning av volymen, kvaliteten och snabbheten i informationsutbytet genom ett centraliserat storskaligt informationssystem som förvaltas av en tillsynsmyndighet (eu-LISA) kan inte uppnås av medlemsstaterna på egen hand och kräver åtgärder på unionsnivå. Om de befintliga problemen inte åtgärdas kommer SIS fortsättningsvis att drivas enligt de bestämmelser som gäller för närvarande, vilket innebär att man går miste om de möjligheter att maximera effektiviteten och det europeiska mervärdet som fastställts genom utvärderingen av SIS och medlemsstaternas användning av systemet.

Enbart under 2015 har medlemsstaternas behöriga myndigheter använt systemet nästan 2,9 miljarder gånger, vilket är ett tydligt bevis på systemets väsentliga bidrag till brottsbekämpningssamarbetet inom Schengenområdet. Denna höga nivå av informationsutbyte mellan medlemsstaterna skulle inte ha uppnåtts genom decentraliserade nationella lösningar, och det skulle ha varit omöjligt att uppnå dessa resultat på medlemsstatsnivå. Dessutom har SIS visat sig vara det effektivaste verktyget för informationsutbyte när det gäller att bekämpa terrorism och det ger ett europeiskt mervärde eftersom det gör det möjligt för de nationella säkerhetstjänsterna att samarbeta på ett snabbt, konfidentiellt och effektivt sätt. De nya förslagen kommer att ytterligare underlätta informationsutbytet och samarbetet mellan EU:s medlemsstater. Dessutom kommer Europol och den nya Europeiska gräns- och kustbevakningsbyrån att inom ramen för deras befogenheter ges full åtkomst till systemet som ett tydligt tecken på att EU:s engagemang ger ett mervärde.

1.5.3. Huvudsakliga erfarenheter från liknande försök eller åtgärder

1. Utvecklingsfasen bör inledas först efter det att driftsbehoven och slutanvändarnas krav fullt ut har fastställts. Utvecklingen kan ske först när de underliggande rättsliga instrument som fastställer ändamålet, tillämpningsområdet, funktionerna och de tekniska detaljerna har antagits slutgiltigt.

2. Kommissionen har genomfört (och genomför fortsättningsvis) fortlöpande samråd med berörda parter, bland annat medlemmarna i SISVIS-kommittén enligt kommittéförfarandet. I kommittén ingår medlemsstaternas företrädare för både operativa Sirenefrågor (det gränsöverskridande samarbetet i fråga om SIS) och tekniska frågor om utvecklingen och underhållet av SIS och den relaterade Sireneapplikationen. De ändringar som föreslås i denna förordning har diskuterats på ett mycket öppet och uttömmande sätt vid särskilda möten och seminarier. Internt inrättade kommissionen en styrgrupp med företrädare från generalsekretariatet och generaldirektoraten för migration och inrikes frågor, rättsliga frågor och konsumentfrågor, personal och säkerhet samt informationsteknik. Denna styrgrupp har övervakat utvärderingsförfarandet och gett vägledning vid behov.

3. Kommissionen har också begärt extern sakkunskap genom följande två studier, vars resultat har tagits med vid utarbetandet av detta förslag:

- En teknisk bedömning av SIS – vid bedömningen konstaterades centrala problem i samband med SIS och framtida behov som bör övervägas, t.ex. orosmoment i fråga om att maximera driftskontinuiteten och säkerställa att den övergripande strukturen kan anpassas till ökande kapacitetskrav.

- En IKT-konsekvensbedömning av möjliga förbättringar av SIS II-strukturen – i denna studie bedömdes de löpande kostnaderna för driften av SIS på nationell nivå och utvärderades tre möjliga tekniska scenarier för en förbättring av systemet. Alla scenarierna omfattar en rad tekniska förslag med fokus på förbättringar av det centrala systemet och den övergripande strukturen.

1.5.4. Förenlighet med andra finansieringsformer och eventuella synergieffekter

Detta förslag bör ses som ett genomförande av de åtgärder som ingår i meddelandet *Starkare och smartare informationssystem för gränser och säkerhet* av den 6 april 2016[84], där det understryks att EU måste stärka och förbättra it-systemen, it-strukturen och informationsutbytet på området brottsbekämpning, terrorismbekämpning och gränsförvaltning.

Förslaget har därutöver en nära koppling till och kompletterar unionens politik på andra områden, nämligen följande:

a) Den inre säkerheten, som betonades i den europeiska säkerhetsagendan[85], för att förebygga, upptäcka, utreda och lagföra grova brott och terroristbrott genom att ge brottsbekämpande myndigheter rätt att behandla personuppgifter om personer som misstänks vara inblandade i terroristdåd eller grova brott.

b) Uppgiftsskydd, i den mån detta förslag måste säkerställa skyddet av de grundläggande rättigheterna för att respektera privatlivet för de personer vars personuppgifter behandlas i SIS.

Förslaget är också förenligt med gällande EU-lagstiftning, nämligen följande:

a) Den europeiska gräns- och kustbevakningen[86] när det gäller, för det första, möjligheterna för byråns personal att utföra riskanalyser och, för det andra, deras

84 COM(2016) 205 final.

85 COM(2015) 185 final.

86 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

åtkomst till SIS i samband med det föreslagna Etias. Förslaget syftar också till att inrätta ett tekniskt gränssnitt för åtkomst till SIS för de europeiska gräns- och kustbevakningsenheterna, enheter som arbetar med återvändande samt medlemmarna i stödgruppen för migrationshantering, vilka, inom ramen för sitt mandat, ska ha rätt att få åtkomst till och söka uppgifter som har lagts in i SIS.

b) Europol, i den mån detta förslag ger Europol ytterligare rätt att få åtkomst till och söka uppgifter som har lagts in i SIS inom ramen för dess mandat.

c) Prüm[87], i den mån de utökade möjligheterna i detta förslag att identifiera personer på grundval av fingeravtryck (samt ansiktsbilder och DNA-profiler) kompletterar de befintliga Prümbestämmelserna om ömsesidig gränsöverskridande onlineåtkomst till utsedda nationella DNA-databaser och automatiska system för identifiering av fingeravtryck.

Förslaget är också förenligt med framtida EU-lagstiftning, nämligen följande:

a) Förvaltning av de yttre gränserna. Förslaget kompletterar den planerade nya principen i kodexen om Schengengränserna om systematiska kontroller av alla resande, även EU-medborgare, mot relevanta databaser vid inresa till och utresa från Schengenområdet, vilken inrättas som ett svar på problemet med utländska terroristtstridande.

b) In- och utresesystemet[88], i den mån detta förslag syftar till att återspegla den föreslagna användningen av en kombination av fingeravtryck och ansiktsbilder som biometriska kännetecken vid driften av in- och utresesystemet.

c) Etias, i den mån detta förslag beaktar det föreslagna Etias, som möjliggör en grundlig säkerhetskontroll, bland annat en kontroll i SIS, av tredjelandsmedborgare som avser att resa i Europeiska unionen.

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).

87 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) och 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).

88 Förslag till Europaparlamentets och rådets förordning om inrättande av ett in- och utresesystem som har till syfte att registrera in- och utreseuppgifter och uppgifter om nekad inresa för tredjelandsmedborgare som passerar Europeiska unionens medlemsstaters yttre gränser och om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av förordning (EG) nr 767/2008 och förordning (EU) nr 1077/2011 (COM(2016) 194 final).

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

☐ Förslag eller initiativ som pågår under en **begränsad tid**

– ☐ Förslaget eller initiativet ska gälla från [den DD/MM]ÅÅÅÅ till [den DD/MM]ÅÅÅÅ.

– ☐ Det påverkar resursanvändningen från ÅÅÅÅ till ÅÅÅÅ.

☑ Förslag eller initiativ som pågår under en **obegränsad tid**

– Förberedande fas 2017

– Efter en inledande period 2018–2020,

– beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad metod för genomförandet[89]

☑**Direkt förvaltning** som sköts av kommissionen

– ☑ inom dess avdelningar, vilket också inbegriper personalen vid unionens delegationer

– ☐ via genomförandeorgan

☑ **Delad förvaltning** med medlemsstaterna

☑ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet delegeras till

– ☐ tredjeländer eller organ som de har utsett

– ☐ internationella organisationer och organ kopplade till dem (ange vilka)

– ☐ EIB och Europeiska investeringsfonden

– ☑ organ som avses i artiklarna 208 och 209 i budgetförordningen

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som anförtrotts uppgifter som faller inom offentlig förvaltning och som lämnat tillräckliga ekonomiska garantier

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandet av ett offentlig-privat partnerskap och som lämnat tillräckliga ekonomiska garantier

– ☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder inom Gusp som följer av avdelning V i fördraget om Europeiska unionen och som anges i den grundläggande rättsakten

– *Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.*

Anmärkningar

Kommissionen kommer att ansvara för den övergripande strategiförvaltningen och eu-LISA kommer att ansvara för utveckling, drift och underhåll av systemet.

[89] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

SIS är ett enda informationssystem. Följaktligen bör de utgifter som anges i två av förslagen (det föreliggande och förslaget till förordning om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller) inte ses som två separata belopp utan som ett enda. Budgetkonsekvenserna av de ändringar som krävs för genomförandet av bägge förslagen ingår i en enda finansieringsöversikt för rättsakterna.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder

Kommissionen, medlemsstaterna och byrån kommer regelbundet att se över och övervaka användningen av SIS för att säkerställa att det fortsätter att fungera effektivt och ändamålsenligt. Kommissionen kommer att bistås av kommittén för genomförandet av de tekniska och operativa åtgärder som beskrivs i detta förslag.

Dessutom inbegriper detta förslag till förordning (i artikel 71.7 och 71.8) bestämmelser om ett formellt, regelbundet översyns- och utvärderingsförfarande.

Vartannat år måste eu-LISA lämna en rapport till Europaparlamentet och rådet om den tekniska funktionen – bland annat säkerheten – hos SIS, den kommunikationsinfrastruktur som stöder systemet samt det bilaterala och multilaterala utbytet av tilläggsinformation mellan medlemsstaterna.

Dessutom måste kommissionen vart fjärde år genomföra en övergripande utvärdering av SIS och informationsutbytet mellan medlemsstaterna och lämna den till Europaparlamentet och rådet. I utvärderingen kommer man att

a) granska uppnådda resultat i förhållande till målen,

b) bedöma om de ursprungliga förutsättningarna för systemet fortfarande är aktuella,

c) granska hur förordningen tillämpas på det centrala systemet,

d) utvärdera det centrala systemets säkerhet,

e) utreda konsekvenserna för systemets framtida funktion.

Dessutom måste eu-LISA nu också tillhandahålla daglig, månatlig och årlig statistik om användningen av SIS, för att säkerställa fortlöpande övervakning av systemet och dess funktion i förhållande till målen.

2.2. Administrations- och kontrollsystem

2.2.1. Risker som identifierats

Följande risker har identifierats:

1. Potentiella svårigheter för eu-LISA att hantera de uppdateringar som anges i detta förslag parallellt med andra pågående uppdateringar (t.ex. genomförandet av Afis i SIS) och framtida uppdateringar (t.ex. in- och utresesystemet, Etias och uppgraderingen av Eurodac). Denna risk skulle kunna minskas genom att säkerställa att eu-LISA har tillräckligt med personal och resurser för att utföra dessa uppgifter och den fortlöpande förvaltningen av avtalet om underhållet av funktionsdugligheten.

2. Svårigheter för medlemsstaterna

2.1 Dessa svårigheter är framför allt av en ekonomisk karaktär. Lagförslagen inbegriper till exempel obligatorisk utveckling av en partiell nationell kopia i varje N.SIS II. De medlemsstater som inte redan har utarbetat en sådan kommer att behöva göra en investering. Likaledes bör det nationella genomförandet av dokumentet för gränssnittskontroll genomföras fullständigt. De medlemsstater som inte redan har gjort detta kommer att behöva anslå medel för detta i de relevanta ministeriernas budgetar. Denna risk skulle kunna minskas genom tillhandahållande av EU-medel till medlemsstaterna, t.ex. från gränsdelen av fonden för inre säkerhet.

2.2 De nationella systemen måste anpassas till centrala krav och diskussioner med medlemsstaterna om detta kan leda till att utvecklingen fördröjs. Denna risk skulle kunna minskas genom tidig dialog med medlemsstaterna om den här frågan för att säkerställa att åtgärder kan vidtas vid lämplig tidpunkt.

2.2.2. Uppgifter om det interna kontrollsystemet

Ansvaret för de centrala delarna av SIS innehas av eu-LISA. För att möjliggöra en bättre övervakning av användningen av SIS och att analysera tendenser när det gäller migrationstryck, gränsförvaltning och brott bör eu-LISA kunna utveckla en avancerad kapacitet för statistisk rapportering till medlemsstaterna och kommissionen.

eu-LISA:s räkenskaper ska godkännas av revisionsrätten och behandlas enligt förfarandet för beviljande av ansvarsfrihet. Kommissionens interna revisionstjänst kommer att genomföra revisioner i samarbete med eu-LISA:s internrevisor.

2.2.3. Beräknade kostnader för och fördelar med kontroller – bedömning av förväntad risk för fel

Ej tillämpligt.

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade)

De åtgärder som planeras för att bekämpa bedrägerier anges i artikel 35 i förordning (EU) nr 1077/2011 där följande föreskrivs:

1. I syfte att bekämpa bedrägerier, korruption och andra rättsstridiga handlingar ska förordning (EG) nr 1073/1999 gälla.

2. Byrån ska ansluta sig till det interinstitutionella avtalet om interna utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och ska utan dröjsmål utfärda lämpliga föreskrifter som gäller för alla anställda vid byrån.

3. I beslut om finansiering samt i de avtal om och instrument för genomförande som införts till följd av dessa beslut, ska det uttryckligen föreskrivas att revisionsrätten och Olaf vid behov får utföra kontroller på plats hos dem som mottagit anslag från byrån samt hos de tjänstemän som har fördelat dessa anslag.

I enlighet med denna bestämmelse fattade styrelsen för byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa den 28 juni 2012 ett beslut om villkor och närmare bestämmelser för interna utredningar för att bekämpa bedrägerier, korruption och all annan olaglig verksamhet som kan skada unionens intressen.

GD Migration och inrikes frågors strategi för bekämpning och upptäckt av bedrägerier kommer att tillämpas.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av anslag	Bidrag			
	3 – Säkerhet och medborgarskap	Diff./Icke-diff[90].	från Efta-länder[91]	från kandidat-länder[92]	från tredje-länder	enligt artikel 21.2 b i budget-förordningen
	18.0208 – Schengens informationssystem	Diff.	NEJ	NEJ	JA	NEJ
	18.020101 – Stöd till gränsförvaltning och en gemensam viseringspolitik för att underlätta lagligt resande	Diff.	NEJ	NEJ	JA	NEJ
	18.0207 – Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA)	Diff.	NEJ	NEJ	JA	NEJ

90 Differentierade respektive icke-differentierade anslag.
91 Efta: Europeiska frihandelssammanslutningen.
92 Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Rubrik i den fleråriga budgetramen	3	Säkerhet och medborgarskap

GD HOME			År **2018**	År **2019**	År **2020**	**TOTALT**
• Driftsanslag						
18.0208 Schengens informationssystem	Åtaganden	(1)	6,234	1,854	1,854	**9,942**
	Betalningar	(2)	6,234	1,854	1,854	**9,942**
18.020101 (Gränsförvaltning och viseringspolitik)	Åtaganden	(1)		18,405	18,405	**36,810**
	Betalningar	(2)		18,405	18,405	**36,810**
TOTALA anslag för GD Migration och inrikes frågor	Åtaganden	=1+1a +3	6,234	20,259	20,259	**46,752**
	Betalningar	=2+2a +3	6,234	20,259	20,259	**46,752**

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	3	Säkerhet och medborgarskap

eu-LISA			År **2018**	År **2019**	År **2020**	**TOTALT**
• Driftsanslag						
Budgetrubrik 1: Personalkostnader	Åtaganden	(1)	0,210	0,210	0,210	**0,630**
	Betalningar	(2)	0,210	0,210	0,210	**0,630**
Budgetrubrik 2: Infrastruktur- och driftsutgifter	Åtaganden	(1a)	0	0	0	**0**
	Betalningar	(2a)	0	0	0	**0**
Budgetrubrik 3: Driftsutgifter	Åtaganden	(1a)	12,893	2,051	1,982	**16,926**
	Betalningar	(2a)	2,500	7,893	4,651	**15,044**
TOTALA anslag för eu-LISA	Åtaganden	=1+1a +3	13,103	2,261	2,192	**17,556**
	Betalningar	=2+2a +3	2,710	8,103	4,861	**15,674**

3.2.2. Beräknad inverkan på driftsanslagen

•TOTALA driftsanslag	Åtaganden	(4)								
	Betalningar	(5)								
•TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program		(6)								
TOTALA anslag	Åtaganden	=4+ 6								

för RUBRIK <….> i den fleråriga budgetramen	Betalningar	=5+ 6								

Följande ska anges om flera rubriker i budgetramen påverkas av förslaget eller initiativet:

•TOTALA driftsanslag	Åtaganden	(4)							
	Betalningar	(5)							
•TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program		(6)							
TOTALA anslag för RUBRIKERNA 1–4 i den fleråriga budgetramen (referensbelopp)	Åtaganden	=4+ 6	19,337	22,520	22,451				**64,308**
	Betalningar	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3. Beräknad inverkan på anslag av administrativ natur

Rubrik i den fleråriga budgetramen	**5**	”Administrativa utgifter”

		År **N**	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
GD: <…….>									
•Personalresurser									
•Övriga administrativa utgifter									
GD <….> **TOTALT**	Anslag								

Miljoner euro (avrundat till tre decimaler)

TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)								

Miljoner euro (avrundat till tre decimaler)

		År **N**[93]	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
TOTALA anslag för RUBRIKERNA 1–5 i den fleråriga budgetramen	Åtaganden								
	Betalningar								

93 Med år n avses det år då förslaget eller initiativet ska börja genomföras.

3.2.3.1. Beräknad inverkan på GD HOME:s anslag

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☑ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Mål- och resultatbeteckning ⇩			År **2018**		År **2019**		År **2020**		För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)						**TOTALT**			
	RESULTAT																	
	Typ[94]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[95] Utveckling av nationellt system			1		1	1,221	1	1,221										2,442
SPECIFIKT MÅL nr 2 Infrastruktur			1		1	17,184	1	17,184										34,368
TOTALA KOSTNADER						18,405		18,405										36,810

94 Resultaten som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

95 Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål…”.

3.2.3.2. Beräknad inverkan på eu-LISA:s driftsanslag

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☑ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Mål- och resultatbeteckning ⇩			År **2018**		År **2019**		År **2020**		För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)						**TOTALT**			
	RESULTAT																	
	Typ[96]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[97] Utveckling av centralt system																		
- Entreprenör			1	5,013														5,013
- Programvara			1	4,050														4,050
- Hårdvara			1	3,692														3,692
Delsumma för specifikt mål nr 1				12,755														12,755
SPECIFIKT MÅL nr 2 Underhåll av centralt system																		
- Entreprenör			1	0	1	0,365	1	0,365										0,730
Programvara			1	0	1	0,810	1	0,810										1,620
Hårdvara			1	0	1	0,738	1	0,738										1,476

[96] Resultaten som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

[97] Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål…”.

Delsumma för specifikt mål nr 2				1,913		1,913										3,826
SPECIFIKT MÅL nr 3 Möten/utbildning																
Utbildningsverksamhet	1	0,138	1	0,138	1	0,069										0,345
Delsumma för specifikt mål nr 3		0,138		0,138		0,069										0,345
TOTALA KOSTNADER		12,893		2,051		1,982										16,926

3.2.3.3. Beräknad inverkan på eu-LISA:s personalresurser

Sammanfattning

– ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

– ☑ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År **2018**	År **2019**	År **2020**	**TOTALT**
Tjänstemän (AD-tjänster)				
Tjänstemän (AST-tjänster)				
Kontraktsanställda	0,210	0,210	0,210	0,630
Tillfälligt anställda				
Utstationerade nationella experter				
TOTALT	**0,210**	**0,210**	**0,210**	**0,630**

Rekrytering är planerad till januari 2018. All personal måste stå till förfogande från och med början av 2018 så att utvecklingen ska kunna påbörjas i tid för att säkerställa att det uppdaterade SIS II kan tas i drift under 2020. De tre nya kontraktsanställda behövs för att täcka behov både för genomförandet av projektet och för operativt stöd och underhåll från utveckling till produktion. De kommer att göra följande:

- Stödja genomförandet av projektet som medlemmar av projektgruppen, med uppgifter som bland annat fastställande av krav och tekniska specifikationer, samarbete och stöd till medlemsstaterna under genomförandet, uppdatering av dokumentet om gränssnittskontroll, uppföljning av de avtalsenliga leveranserna, leverans och uppdatering av dokumentation osv.
- Stödja övergången för ibruktagandet av systemet i samarbete med entreprenören (uppföljning av lanseringar, uppdatering av operativa processer, utbildning (inbegripet medlemsstaternas utbildningsverksamhet) osv.).
- Stödja långsiktig verksamhet, fastställande av specifikationer och förberedande av avtal om systemets konstruktion ändras (t.ex. på grund av bildigenkänning) eller om det nya avtalet för underhåll av SIS II:s funktionsduglighet behöver ändras för att omfatta ytterligare ändringar (ur en teknisk och budgetmässig synvinkel).
- Verkställa andra linjens support efter idrifttagandet, under löpande underhåll och drift.

Det bör noteras att de tre nya kontraktsanställda kommer att agera utöver de interna arbetsgrupper som även de kommer att arbeta med projektet/avtalsförvaltning och finansiell uppföljning/operativ verksamhet. Användningen av kontraktsanställda ger avtalen tillräcklig varaktighet och kontinuitet för att säkerställa driftskontinuitet och användning av samma specialiserade personer för operativa stödåtgärder efter det att projektet har avslutats. Utöver detta kräver de operativa stödåtgärderna sådan åtkomst till produktionsmiljön som inte kan tilldelas entreprenörer eller extern personal.

3.2.3.4. Beräknat personalbehov

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– ☐ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

		År **N**	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)		
• **Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)**								
XX 01 01 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)								
XX 01 01 02 (vid delegationer)								
XX 01 05 01 (indirekta forskningsåtgärder)								
10 01 05 01 (direkta forskningsåtgärder)								
• **Extern personal (i heltidsekvivalenter)**[98]								
XX 01 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)								
XX 01 02 02 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)								
XX 01 04 **yy** [99]	- vid huvudkontoret							
	- vid delegationer							
XX 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med indirekta forskningsåtgärder)								
10 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
TOTALT								

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

98 [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

99 Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

Tjänstemän och tillfälligt anställda	
Extern personal	

3.2.4. Förenlighet med den gällande fleråriga budgetramen

– ☐ Förslaget/initiativet är förenligt med den gällande fleråriga budgetramen

– ☑ Förslaget/initiativet kräver omfördelningar under den berörda rubriken i den fleråriga budgetramen

En omfördelning av återstoden av anslaget för smarta gränser inom ramen för fonden för inre säkerhet planeras för att genomföra de funktioner och ändringar som planeras i de båda förslagen. Förordningen om fonden för inre säkerhet och stödet för yttre gränser är det finansieringsinstrument som innehåller budgeten för genomförande av paketet för smarta gränser. Enligt artikel 5 ska 791 miljoner euro satsas på ett program för inrättande av it-system till stöd för förvaltningen av migrationsströmmar över de yttre gränserna, enligt de villkor som fastställs i artikel 15. Av de 791 miljoner euro som nämns ovan är 480 miljoner euro avsedda för utvecklingen av in- och utresesystemet och 210 miljoner euro för utvecklingen av EU-systemet för reseuppgifter och resetillstånd (Etias). Återstoden – 100,828 miljoner euro – kommer delvis att användas för att täcka kostnaderna för de ändringar som planeras i de två förslagen avseende uppgraderingen av SIS II-funktionerna.

– ☐ Förslaget/initiativet förutsätter att flexibilitetsmekanismen utnyttjas eller att den fleråriga budgetramen revideras.

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt belopp.

3.2.5. Bidrag från tredje part

– ☑Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet

– Förslaget eller initiativet kommer att medfinansieras enligt följande:

Anslag i miljoner euro (avrundat till tre decimaler)

	År **N**	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilken extern organisation eller annan källa som bidrar till finansieringen								
TOTALA anslag som tillförs genom medfinansiering								

3.3. Beräknad inverkan på inkomsterna

– ☐ Förslaget/initiativet påverkar inte budgetens inkomstsida.

– ☑ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på egna medel

– ☑ Påverkan på ”diverse inkomster”

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Belopp som förts in för det innevarande budgetåret	Förslagets eller initiativets inverkan på inkomsterna[100]						
		2018	2019	2020	2021	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel 6313 – Bidrag från länder som deltar i Schengensamarbetet (Schweiz, Norge, Liechtenstein, Island).		p.m.	p.m.	p.m.	p.m.			

Ange vilka budgetrubriker i utgiftsdelen som berörs i de fall där inkomster i diversekategorin kommer att avsättas för särskilda ändamål.

18.02.08 (Schengens informationssystem), 18.02.07 (eu-LISA)

Ange med vilken metod inverkan på inkomsterna har beräknats.

Budgeten ska omfatta ett bidrag från länder som deltar i genomförandet, tillämpningen och utvecklingen av Schengenregelverket.

[100] När det gäller traditionella egna medel (tullar och sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 25 % avdrag för uppbördskostnader.