



EUROPEISKA
KOMMISSIONEN

Strasbourg den 12.12.2017
COM(2017) 794 final

2017/0352 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

**om inrättande av en ram för interoperabilitet mellan EU-informationssystem
(polissamarbete och rättsligt samarbete, asyl och migration)**

{SWD(2017) 473} - {SWD(2017) 474}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Bakgrund till förslaget

Under de senaste tre åren har de irreguljära gränspassagera till EU ökat, och den inre säkerheten är ständigt ansatt av ett föränderligt hot som konkretiserats genom en rad terroristattacker. EU-medborgare förväntar sig att kontrollerna av personer vid de yttre gränserna och kontrollerna inom Schengenområdet ska vara ändamålsenliga, möjliggöra en effektiv migrationshantering och bidra till den inre säkerheten. Dessa utmaningar har satt ett skarpare fokus på det akuta behovet av att gå samman och på ett övergripande sätt stärka EU:s informationsverktyg för gränsförvaltning, migration och säkerhet.

Informationshanteringen i EU kan och måste bli mer ändamålsenlig och effektiv med fullt iakttagande av de grundläggande rättigheterna – framför allt rätten till skydd av personuppgifter – för att bättre skydda EU:s yttre gränser, förbättra migrationshanteringen och öka den inre säkerheten för alla medborgare. Det finns redan ett antal informationssystem på EU-nivå, och fler är under utveckling för att tillhandahålla tjänstemän inom gränskontroll, immigration och brottsbekämpning relevant information om personer. För att detta stöd ska vara effektivt måste de uppgifter som EU-informationssystemen ger vara fullständiga, korrekta och tillförlitliga. Det finns dock strukturella brister i EU:s informationshanteringsarkitektur. Nationella myndigheter måste hantera ett komplicerat landskap av informationssystem som administreras på olika sätt. Dessutom är uppgiftshanteringsstrukturen för gränser och säkerhet splittrad, då informationen lagras separat i fristående system. Detta leder till blindade fläckar. Till följd av detta är **de olika informationssystemen på EU-nivå för närvarande inte interoperabla**, dvs. kapabla att utbyta uppgifter och dela information så att myndigheter och behöriga tjänstemän har den information de behöver när och där den behövs. Interoperabilitet mellan informationssystemen på EU-nivå kan på ett betydande sätt bidra till att undanröja de nuvarande blindade fläckar som innebär att personer – även sådana som möjligen är involverade i terroristverksamhet – kan registreras i olika fristående databaser under olika alias.

I april 2016 lade kommissionen fram sitt **meddelande Starkare och smartare informationssystem för gränser och säkerhet**¹, för att lyfta fram ett antal strukturella brister i informationssystemen². Målet med meddelandet var att inleda en diskussion om hur EU:s informationssystem kan bidra till bättre gränsförvaltning, migrationshantering och inre säkerhet. **Rådet** har på sin sida också konstaterat det akuta behovet av åtgärder på detta område. I juni 2016 antog det en **färdplan för förbättring av informationsutbytet och informationshanteringen**, inbegripet interoperabilitetslösningar på området för rättsliga och inrikes frågor³. Syftet med färdplanen var att stödja operativa utredningar och att se till att de som arbetar på området – t.ex. poliser, gränskontrolltjänstemän, allmänna åklagare och immigrationstjänstemän – snabbt får tillgång till heltäckande, aktuell information av hög kvalitet för att kunna samarbeta och agera effektivt. **Europaparlamentet** har också krävt

¹ COM(2016) 205 av den 6 april 2016.

² 1) Undermåliga funktioner i vissa av de befintliga informationssystemen, 2) informationsluckor i EU:s uppgiftshanteringsstruktur, 3) ett komplicerat landskap av informationssystem som administreras på olika sätt och 4) en splittrad uppgiftshanteringsstruktur för gränskontroll och säkerhet då information lagras separat i fristående system, vilket leder till blindade fläckar.

³ Färdplan av den 6 juni 2016 för förbättring av informationsutbytet och informationshanteringen, inbegripet interoperabilitetslösningar på området för rättsliga och inrikes frågor, 9368/1/16 REV 1.

åtgärder på detta område. I sin resolution från juli 2016⁴ om kommissionens arbetsprogram 2017 efterlyste Europaparlamentet ”*förslag för att förbättra och utveckla befintliga informationssystem, åtgärda luckor i informationen och gå i riktning mot driftskompatibilitet samt förslag om obligatoriskt informationsutbyte på EU-nivå åtföljda av de bestämmelser om uppgiftsskydd som krävs*”. I kommissionsordförande Jean-Claude Junckers tal om tillståndet i unionen i september 2016⁵ och Europeiska rådets slutsatser från december 2016⁶ betonades vikten av att komma till rätta med de nuvarande bristerna när det gäller uppgiftshantering och att förbättra interoperabiliteten mellan befintliga informationssystem.

I juni 2016 inrättade kommissionen som en uppföljning till meddelandet från april 2016 en **expertgrupp för informationssystem och interoperabilitet**⁷ för att bedöma de rättsliga, tekniska och operativa hindren för ökad interoperabilitet mellan EU:s centrala system för gränser och säkerhet, bland annat deras nödvändighet, tekniska genomförbarhet, proportionalitet och konsekvenser för dataskyddet. Expertgruppens **slutrapport** offentliggjordes i maj 2017⁸. Den innehöll en rad rekommendationer för att stärka och utveckla EU:s informationssystem och deras interoperabilitet. Europeiska unionens byrå för grundläggande rättigheter, Europeiska datatillsynsmannen och EU:s samordnare för kampen mot terrorism deltog alla aktivt i expertgruppens arbete. De lämnade alla in positiva uttalanden men påpekade att de större frågorna om grundläggande rättigheter och dataskydd måste beaktas under det fortsatta arbetet. Företrädare för sekretariatet för Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor och rådets generalsekretariat deltog som observatörer. Expertgruppens slutsats var att det är **nödvändigt och tekniskt genomförbart att eftersträva praktiska lösningar för interoperabilitet** och att sådana i princip både kan ge operativa vinster och inrättas i överensstämmelse med dataskyddskraven.

På grundval av expertgruppens rapport och rekommendationer har kommissionen i *Sjunde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*⁹ fastställt en **ny strategi för uppgiftshantering** för gränser, säkerhet och migrationshantering där alla centraliserade EU-informationssystem för säkerhet, gränser och migrationshantering är interoperabla med full respekt för de grundläggande rättigheterna. Kommissionen tillkännagav sin avsikt att fortsätta arbeta för att skapa en europeisk sökportal som gör det möjligt att samtidigt söka i alla relevanta EU-system på områdena säkerhet, gränser och migrationshantering (eventuellt med förenklade regler för åtkomst i brottsbekämpningssyfte) och att utveckla en gemensam biometrisk matchningstjänst för dessa system (eventuellt med en flaggfunktion vid träff¹⁰) och en gemensam databas för identitetsuppgifter. Den meddelade sin avsikt att så snart som möjligt lägga fram ett lagstiftningsförslag om interoperabilitet.

⁴ Europaparlamentets resolution av den 6 juli 2016 om de strategiska prioriteringarna för kommissionens arbetsprogram 2017, [2016/2773 \(RSP\)](#).

⁵ Tillståndet i unionen 2016, 14.9.2016, https://ec.europa.eu/commission/state-union-2016_sv.

⁶ Europeiska rådets slutsatser, 15.12.2016, http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

⁷ Kommissionens beslut av den 17 juni 2016 om inrättande av en expertgrupp för informationssystem och interoperabilitet, EUT C 257, 15.7.2016, s. 3.

⁸ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.

⁹ COM(2017) 261 final.

¹⁰ Ett nytt koncept med inbyggt integritetsskydd som begränsar åtkomsten till alla uppgifter till endast ett meddelande om träff eller ingen träff, för att visa om det finns (eller inte finns) uppgifter.

Behovet av att agera upprepades i Europeiska rådets slutsatser från juni 2017¹¹. Grundat på slutsatserna i juni 2017¹² från rådet (rättsliga och inrikes frågor) uppmanade Europeiska rådet kommissionen att så snart som möjligt utarbeta ett förslag till lagstiftning för att omsätta expertgruppens rekommendationer i verklighet. Detta initiativ är också ett svar på rådets uppmaning till en övergripande ram för åtkomst i brottsbekämpningssyfte till de olika databaserna på området rättsliga och inrikes frågor, i syfte att uppnå mer förenkling, enhetlighet och ändamålsenlighet samt beakta de operativa behoven¹³. För att öka ansträngningarna att göra Europeiska unionen till ett säkrare samhälle, i full överensstämmelse med de grundläggande rättigheterna, tillkännagav kommissionen i samband med sitt arbetsprogram för 2018¹⁴ sin avsikt att lägga fram ett förslag om interoperabilitet mellan informationssystemen före slutet av 2017.

- **Syfte med förslaget**

De allmänna syftena med detta initiativ följer av de fördragsenliga målen att förbättra förvaltningen av Schengenområdets yttre gränser och bidra till Europeiska unionens inre säkerhet. De är också en följd av politiska beslut som fattats av kommissionen och relevanta slutsatser från (Europeiska) rådet. Närmare redogörelser för dessa syften finns i den europeiska migrationsagendan och efterföljande meddelanden, bland annat meddelandet om bevarande och stärkande av Schengen¹⁵, den europeiska säkerhetsagendan¹⁶ och kommissionens arbete och rapporter om framstegen i riktning mot en effektiv och verklig säkerhetsunion¹⁷.

Medan detta förslag i synnerhet bygger på meddelandet från april 2016 och expertgruppens resultat hänger dess syften nära samman med ovanstående.

De specifika syftena med detta förslag är följande:

- (1) Säkerställa att slutanvändare, framför allt gränskontrolltjänstemän, brottsbekämpande tjänstemän, immigrationstjänstemän och rättsliga myndigheter, får **snabb, smidig, systematisk och kontrollerad åtkomst** till den information de behöver för att utföra sina uppgifter.
- (2) Tillhandahålla en metod för att **spåra multipla identiteter** som används med samma biometrisk uppgift, vilket har det dubbla syftet att säkerställa en korrekt identifiering av personer med ärligt uppsåt och **bekämpa identitetsbedrägeri**.
- (3) Underlätta polismyndigheternas **identitetskontroller av tredjelandsmedborgare** på en medlemsstats territorium.

¹¹ [Slutsatser från Europeiska rådets möte](#) den 22–23 juni 2017.

¹² [Resultatet av rådets 3546:e möte \(rättsliga och inrikes frågor\) den 8–9 juni 2017, 10136/17.](#)

¹³ När ständiga representanternas kommitté (Coreper) gav rådets ordförandeskap mandatet att inleda interinstitutionella förhandlingar om EU-systemet för in- och utresa den 2 mars 2017 enades de om ett utkast till rådets uttalande, där kommissionen uppmanades att lägga fram förslag till en övergripande ram för åtkomst i brottsbekämpningssyfte till de olika databaserna på området rättsliga och inrikes frågor, i syfte att uppnå mer förenkling, enhetlighet och ändamålsenlighet samt beakta de operativa behoven (sammanfattande protokoll 7177/17, 21.3.2017).

¹⁴ COM(2017) 650 final.

¹⁵ COM(2017) 570 final.

¹⁶ COM(2015) 185 final.

¹⁷ COM(2016) 230 final.

- (4) Underlätta och **rationalisera de brottsbekämpande myndigheternas åtkomst** till EU:s informationssystem som inte är utformade för brottsbekämpning, när det är nödvändigt för att förebygga, utreda, upptäcka eller lagföra grov brottslighet och terrorism.

Utöver dessa primära, operativa mål kommer detta förslag också att bidra till följande:

- Underlätta **medlemsstaternas tekniska implementering** och operativa **drift** av befintliga och framtida nya informationssystem.
- Skärpa och enhetliggöra de **villkor för datasäkerhet och dataskydd** som reglerar respektive system.
- Förbättra och harmonisera respektive systems krav på **uppgiftskvalitet**.

Slutligen innehåller detta förslag bestämmelser om inrättandet och förvaltningen av det universella meddelandeformatet (UMF) som en EU-standard för utvecklingen av informationssystem på området rättsliga och inrikes frågor samt inrättandet av en central databas för rapporter och statistik.

- **Förslagets tillämpningsområde**

Tillsammans med det anknyttande förslag som läggs fram samma dag fokuserar detta interoperabilitetsförslag på de EU-informationssystem för säkerhet, gränser och migrationshantering som drivs på central nivå – tre befintliga, ett på väg att utvecklas och två andra som är föremål för diskussion mellan medlagstiftarna. Varje system har sina egna syften, ändamål, rättsliga grunder, regler, användargrupper och institutionella sammanhang.

De tre befintliga centraliserade informationssystemen är följande:

- **Schengens informationssystem (SIS)**, som innehåller ett brett spektrum av registreringar om personer (nekad inresa eller vistelse, europeisk arresteringsorder, försvunna personer, deltagande i ett rättsligt förfarande samt diskreta och särskilda kontroller) och föremål (bl.a. försvunna, stulna och ogiltigförklarade identitets- eller resehandlingar)¹⁸.
- **Eurodacsystemet** med fingeravtrycksuppgifter från asylsökande och tredjelandsmedborgare som har passerat de yttre gränserna irreguljärt eller som vistas olagligt i en medlemsstat.
- **Informationssystemet för viseringar (VIS)** med uppgifter om viseringar för kortare vistelser.

Utöver dessa befintliga system föreslog kommissionen under 2016 och 2017 följande tre nya centraliserade EU-informationssystem:

- **In- och utresesystemet**, vars rättsliga grund just har antagits, kommer att ersätta det nuvarande systemet med manuell stämpling av pass och kommer att elektroniskt

¹⁸ I kommissionens förslag till förordningar om SIS från december 2016 föreslås att systemet utvidgas ytterligare till att omfatta beslut om återvändande och undersökningskontroller.

registrera namn, typ av resehandling, biometriska uppgifter samt datum och plats för in- och utresa för tredjelandsmedborgare som reser in i Schengenområdet för en kortare vistelse.

- Det föreslagna **EU-systemet för reseuppgifter och resetillstånd (Etias)** skulle, när det har antagits, vara ett i huvudsak automatiserat system för att samla in och kontrollera information som tredjelandsmedborgare som är undantagna från viseringskravet lämnar in innan de reser till Schengenområdet.
- Det föreslagna **europiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN-systemet)** skulle vara ett elektroniskt system för utbyte av information om tidigare fällande domar som meddelats tredjelandsmedborgare av brottmålsdomstolar i EU.

De här sex systemen kompletterar varandra och – med undantag för Schengens informationssystem (SIS) – är uteslutande avsedda för tredjelandsmedborgare. Systemen hjälper de nationella myndigheterna att förvalta gränser, hantera migration, handlägga viseringar och asyl samt bekämpa brottslighet och terrorism. Det sistnämnda gäller i synnerhet SIS, som är det mest använda verktyget för informationsutbyte bland brottsbekämpande myndigheter idag.

Utöver dessa informationssystem som förvaltas centralt på EU-nivå omfattar detta förslag även **Interpols** databas över stulna och förkomna resehandlingar, som i enlighet med kodexen om Schengengränserna systematiskt konsulteras vid EU:s yttre gränser, och Interpols databas för resehandlingar som är föremål för ett meddelande (TDAWN). Det omfattar även **Europoluppgifter**, i den mån detta är relevant för det föreslagna Etias-systemets funktion och för stöd till medlemsstaterna när de söker uppgifter om grov brottslighet och terrorism.

Nationella informationssystem och decentraliserade EU-informationssystem omfattas inte av detta initiativ. Förutsatt att det påvisas att det är nödvändigt kan decentraliserade system såsom de som drivs inom Prümramen¹⁹, direktivet om passageraruppgifter (PNR)²⁰ och direktivet om förhandsinformation om passagerare²¹ i ett senare skede kopplas upp till en eller flera av de komponenter som föreslås i detta initiativ²².

För att ta hänsyn till skillnaden mellan de frågor som utgör en utveckling av Schengenregelverket om gränser och viseringar, å ena sidan, och andra system som berör Schengenregelverket om polissamarbete eller inte är kopplade till Schengenregelverket, å andra sidan, behandlas i detta förslag åtkomst till Schengens informationssystem, som för närvarande regleras genom rådets beslut 2007/533/RIF, samt Eurodac och [Ecris-TCN].

- **De tekniska komponenter som krävs för interoperabilitet**

För att uppnå detta förslags syften måste fyra interoperabilitetskomponenter inrättas, nämligen

- en europeisk sökportal,

¹⁹ http://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1508936184412&uri=CELEX:32008D06_15.

²⁰ http://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1508936384641&uri=CELEX:32016L06_81.

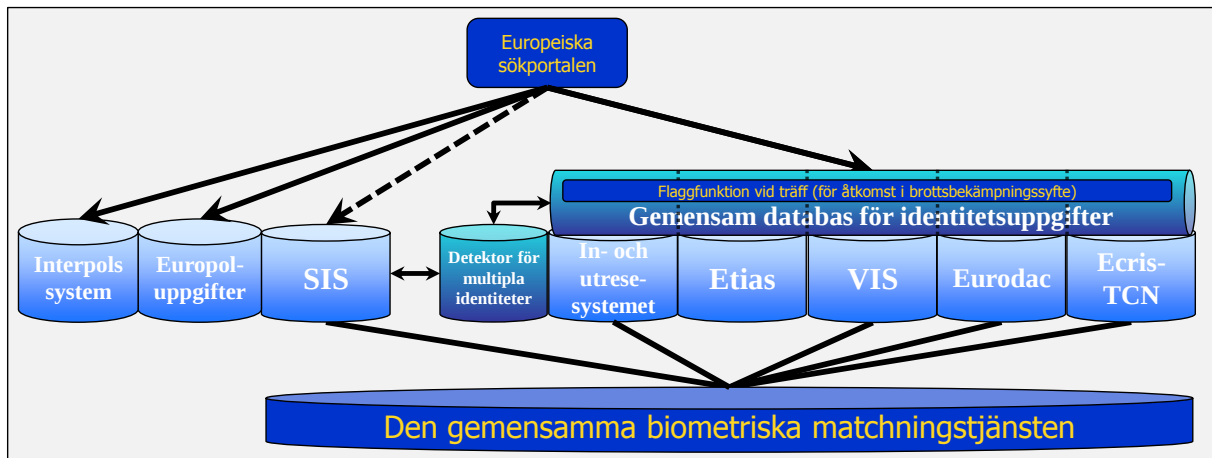
²¹ Rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare.

²² Även när det gäller tullsystemen uppmanade rådet i sina slutsatser från juni 2017 kommissionen att utföra en genomförbarhetsstudie för att ytterligare utreda de tekniska, operativa och rättsliga aspekterna av interoperabilitet mellan säkerhets- och gränsförvaltningssystemen och tullsystemen, och lägga fram sina resultat för diskussion i rådet senast i slutet av 2018.

- en gemensam biometrisk matchningstjänst,
- en gemensam databas för identitetsuppgifter,
- en detektor för multipla identiteter.

Var och en av dessa komponenter beskrivs i detalj i arbetsdokumentet från kommissionens avdelningar om den konsekvensbedömning som åtföljer detta förslag.

Tillsammans leder de fyra komponenterna till följande interoperabilitetslösning:



De fyra komponenternas syften och funktioner kan sammanfattas enligt följande:

- 1) Den **europiska sökportalen (ESP)** är den komponent som skulle göra det möjligt att samtidigt söka i flera system (det centrala SIS, Eurodac, VIS, det framtida in- och utresesystemet och de föreslagna Etias och Ecris-TCN-systemet, samt relevanta Interpolsystem och Europoluppgifter) med identitetsuppgifter (både biografiska och biometriska uppgifter). Den skulle säkerställa att EU-informationssystemens användare har snabb, smidig, effektiv, systematisk och kontrollerad åtkomst till all information som de behöver för att utföra sina uppgifter.

En sökning via den europeiska sökportalen skulle genast, på någon sekund, ge information från de olika system som användaren har laglig åtkomst till. ESP skulle vara konfigurerad enligt syftet med sökningen och de motsvarande åtkomsträttigheterna.

Den europeiska sökportalen hanterar inga nya uppgifter och inga uppgifter lagras i systemet. Den skulle fungera som en gemensam kontaktpunkt eller meddelandehanterare för att söka i olika centrala system och smidigt hämta den nödvändiga informationen, med full respekt för de underliggande systemens åtkomstkontroll och dataskyddskrav. Den skulle underlätta korrekt och bemyndigad användning av vart och ett av de befintliga EU-informationssystemen, och skulle göra det lättare och billigare för medlemsstaterna att söka i och använda systemen, i enlighet med de rättsliga instrument som reglerar dessa system.

- 2) Den **gemensamma biometriska matchningstjänsten** skulle göra det möjligt att söka och jämföra biometriska uppgifter (fingeravtryck och ansiktsbilder) ur flera centrala system (särskilt SIS, Eurodac, VIS, det framtida in- och utresesystemet och det föreslagna Ecris-

TCN-systemet). Det föreslagna Etias innehåller inga biometriska uppgifter och skulle därför inte vara kopplat till den gemensamma biometriska matchningstjänsten.

För närvarande har varje befintligt centralt system (SIS, Eurodac och VIS) en särskild, proprietär sökmotor för biometriska uppgifter²³, medan en gemensam biometrisk matchningstjänst skulle fungera som en delad plattform där det går att söka och jämföra uppgifter samtidigt. Den gemensamma biometriska matchningstjänsten skulle generera betydande fördelar i fråga om säkerhet, kostnader, underhåll och drift genom att man förlitar sig på en unik teknisk komponent i stället för fem olika. De biometriska uppgifterna (fingeravtryck och ansiktsbilder) lagras uteslutande i de underliggande systemen. Den gemensamma biometriska matchningstjänsten skulle skapa och behålla en matematisk representation av de biometriska proven (en mall), men förkasta de faktiska uppgifterna, som därmed förblir lagrade endast en gång, på en enda plats.

Den gemensamma biometriska matchningstjänsten skulle vara till stor hjälp med att upptäcka kopplingar mellan olika uppgifter och olika identiteter som samma person har antagit i olika centrala system. Utan den gemensamma biometriska matchningstjänsten skulle de andra tre komponenterna inte fungera.

- 3) Den **gemensamma databasen för identitetsuppgifter (CIR)** skulle vara en delad komponent för att lagra biografiska²⁴ och biometriska identitetsuppgifter om tredjelandsmedborgare som registrerats i Eurodac, VIS, det framtida in- och utresesystemet och de föreslagna systemen Etias och Ecris-TCN. Vart och ett av dessa fem centrala system registrerar eller kommer att registrera biografiska uppgifter om specifika personer av specifika orsaker. Detta skulle inte förändras. De relevanta identitetsuppgifterna skulle lagras i CIR men skulle fortsätta att ”tillhöra” respektive underliggande system där dessa uppgifter har registrerats.

CIR skulle inte innehålla uppgifter från SIS. SIS komplexa tekniska struktur med nationella kopior, partiella nationella kopior och eventuella nationella biometriska matchningssystem skulle göra CIR så komplicerat att det inte längre vore tekniskt och ekonomiskt genomförbart.

Huvudsyftet med CIR är att underlätta biografisk identifiering av tredjelandsmedborgare. Det skulle ge snabbare drift, ökad effektivitet och stordriftsfördelar. Inrättandet av CIR är nödvändigt för att möjliggöra effektiva identitetskontroller av tredjelandsmedborgare, även på en medlemsstats territorium. Dessutom skulle det genom att lägga till en flaggfunktion vid träff i CIR vara möjligt att kontrollera om det finns (eller inte finns) uppgifter i något av de system som omfattas av CIR genom ett enkelt meddelande om träff eller ingen träff. Därigenom skulle CIR också bidra till att rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning, medan man behåller en hög garanti för dataskydd (se avsnittet om tvåstegsstrategin för åtkomst i brottsbekämpningssyfte nedan).

Av de fem system som ska omfattas av CIR är det framtida in- och utresesystemet och de föreslagna systemen Etias och Ecris-TCN nya system som ännu måste utvecklas. Det

²³ De tekniska namnen på dessa biometriska sökmotorer är automatiskt fingeravtrycksidentifieringssystem (Afis) eller automatiskt biometriskt identifieringssystem (Abis).

²⁴ Biografiska uppgifter som anges på en resehandling är bland annat efternamn, förnamn, kön, födelsedatum och resehandlingens nummer. Där ingår inte adresser, tidigare namn, biometriska uppgifter osv.

nuvarande Eurodac innehåller inga biografiska uppgifter. Den delen kommer att utvecklas när den nya rättsliga grunden för Eurodac väl har antagits. VIS innehåller visserligen biografiska uppgifter, men de nödvändiga interaktionerna mellan VIS och det framtida in- och utresesystemet kräver en uppgradering av det befintliga VIS. Skapandet av CIR skulle därför komma vid rätt tidpunkt. Inga befintliga uppgifter skulle dubbleras. Tekniskt skulle CIR utvecklas utgående från in- och utresesystemets och Etias plattform.

- 4) **Detektorn för multipla identiteter (MID)** skulle kontrollera om de identitetsuppgifter som matas in finns i fler än ett av de system som är anslutna till den. MID omfattar de system som lagrar identitetsuppgifter i CIR (Eurodac, VIS, det framtida in- och utresesystemet och de föreslagna systemen Etias och Ecris-TCN) samt SIS. MID skulle göra det möjligt att spåra multipla identiteter som används med samma biometriska uppgifter, vilket har det dubbla syftet att säkerställa en korrekt identifiering av personer med ärligt uppsåt och bekämpa identitetsbedrägeri.

MID skulle göra det möjligt att fastställa att samma person använder sig av olika namn. Det är en innovation som behövs för att effektivt komma till rätta med bedräglig användning av identiteter, som är ett allvarligt brott mot säkerheten. MID skulle endast visa de biografiska uppgifter som har en länk i olika centrala system. Dessa länkar skulle upptäckas med hjälp av den gemensamma biometriska matchningstjänsten på grundval av biometriska uppgifter, och måste bekräftas eller avslås av den myndighet som registrerade de uppgifter i informationssystemet som ledde till att länken upprättades. För att hjälpa de bemyndigade användarna av MID med denna uppgift bör systemet märka de identifierade länkarna enligt följande fyra kategorier:

- Gul länk – potentiellt avvikande biografiska identiteter för samma person.
- Vit länk – bekräftelse på att de olika biografiska identiteterna tillhör samma person med ärligt uppsåt.
- Grön länk – bekräftelse på att olika personer med ärligt uppsåt råkar dela samma personuppgifter.
- Röd länk – misstanke om att samma person olagligen använder olika biografiska identiteter.

I detta förslag beskrivs de förfaranden som skulle införas för att hantera dessa olika kategorier. Identiteten på berörda personer med ärligt uppsåt bör klargöras så fort som möjligt, genom att den gula länken byts till en bekräftad grön eller vit länk, för att säkerställa att onödiga olägenheter undviks. Om bedömningen å andra sidan leder till bekräftelse av en röd länk, eller en ändring från gul till röd länk, bör lämpliga åtgärder vidtas.

- **Tvåstegsstrategin för åtkomst i brottsbekämpningssyfte till den gemensamma databasen för identitetsuppgifter**

Brottsbekämpning fastställs som ett sekundärt eller underordnat syfte med Eurodac, VIS, det framtida in- och utresesystemet och det föreslagna Etias. På grund av detta är brottsbekämpande myndigheters möjligheter att få åtkomst till uppgifter i dessa system begränsade. Brottsbekämpande myndigheter kan endast söka direkt i dessa informationssystem som inte är utformade för brottsbekämpning i syfte att förebygga, utreda,

upptäcka eller lagföra terroristbrott och andra grova brott. Dessutom gäller olika åtkomstvillkor och skyddsåtgärder för de olika systemen, och vissa av de gällande reglerna kan försinka dessa myndigheters legitima användning av systemen. Mer allmänt begränsar principen om en tidigare sökning möjligheterna för medlemsstaternas myndigheter att söka i systemen för berättigade brottsbekämpande ändamål och kan således leda till att man går miste om chanser att upptäcka nödvändig information.

Kommissionen konstaterade i sitt meddelande från april 2016 behovet av att optimera de befintliga verktygen för brottsbekämpande ändamål, med respekt för dataskyddskraven. Detta behov har bekräftats och upprepats av medlemsstaterna och de relevanta organen inom ramen för expertgruppen.

Mot bakgrund av detta införs i detta förslag, genom inrättandet av CIR med en flaggfunktion vid träff, möjligheten att få åtkomst till in- och utresesystemet, VIS, Etias och Eurodac genom en **tvåstegsstrategi för uppgiftssökning**. Denna tvåstegsstrategi skulle inte förändra det faktum att brottsbekämpning enbart är ett underordnat syfte med dessa system, och att de brottsbekämpande myndigheterna därför måste följa strikta åtkomstregler.

Som ett första steg skulle en brottsbekämpande tjänsteman göra en sökning om en viss person med dennas identitetsuppgifter, resehandlingsuppgifter eller biometrisk uppgifter för att kontrollera om det finns information om personen i CIR. När sådana uppgifter finns får tjänstemannen **ett svar som anger vilket eller vilka EU-informationssystem som innehåller uppgifter** om denna person (**flagga vid träff**). Tjänstemannen skulle inte ha faktisk åtkomst till några uppgifter i de underliggande systemen.

Som ett andra steg kan den brottsbekämpande tjänstemannen begära separat åtkomst till varje system som enligt svaret innehåller uppgifter, för att få den fullständiga akten om personen i fråga, **i enlighet med befintliga regler och förfaranden som fastställts för varje system som berörs**. Åtkomsten i andra steget skulle fortfarande vara föremål för förhandsgodkännande från en utsedd myndighet och skulle även fortsättningsvis kräva ett särskilt användarnamn och loggning.

Denna nya strategi skulle också tillföra ett mervärde för de brottsbekämpande myndigheterna på grund av de **potentiella länkarna** i MID. MID skulle hjälpa CIR att identifiera befintliga länkar, vilket gör att sökningen ger ännu bättre resultat. MID skulle kunna ange om personen är **känd under olika identiteter** i olika informationssystem.

Tvåstegsstrategin för uppgiftssökning är särskilt värdefull i de fall då man **inte känner till** identiteten på den brottsmisstänkta, gärningsmannen eller det misstänkta offret för ett terroristbrott eller ett annat grovt brott. I dessa fall skulle CIR faktiskt göra det möjligt att slå fast vilket informationssystem som har uppgifter om personen i en enda sökning. Därigenom blir de befintliga kraven på tidigare sökningar i nationella databaser och en tidigare sökning i andra medlemsstaters automatiska fingeravtrycksidentifieringssystem enligt beslut 2008/615/RIF ("Prümkontroll") överflödiga.

Den nya tvåstegsstrategin för sökningar skulle **träda i kraft först** när de nödvändiga **interoperabilitetskomponenterna har tagits i bruk helt**.

- **Ytterligare element till stöd för interoperabilitetskomponenterna i detta förslag**

- 1) Förutom de komponenter som nämns ovan föreslås i detta förslag till förordning även att man inrättar en **central databas för rapporter och statistik (CRRS)**. Denna databas behövs för att det ska gå att skapa och dela rapporter med (anonyma) statistiska uppgifter för politiska och operativa ändamål samt syften som rör uppgifternas kvalitet. För närvarande samlas statistiska uppgifter endast in om de enskilda informationssystemen, vilket undergräver datasäkerheten och resultaten och gör det omöjligt att samordna uppgifter mellan olika system.

CRRS skulle fungera som en särskild, separat databas för anonym statistik ur SIS, VIS, Eurodac, det framtida in- och utresesystemet, de föreslagna systemen Etias och Ecris-TCN, den gemensamma databasen för identitetsuppgifter, detektorn för multipla identiteter och den gemensamma biometriska matchningstjänsten. Databasen skulle göra det möjligt att dela rapporter på ett säkert sätt (i enlighet med reglerna i de respektive rättsakterna) med medlemsstaterna, kommissionen (inbegripet Eurostat) och EU:s byråer.

Utveckling av en central databas i stället för separata databaser för varje system skulle leda till lägre kostnader och mindre arbete med inrättandet, driften och underhållet. Det skulle också medföra en högre nivå av datasäkerhet eftersom uppgifterna lagras och åtkomstkontrollen hanteras i en enda databas.

- 2) I detta förslag till förordning föreslås också att man fastställer det **universella meddelandeformatet (UMF)** som den standard som ska användas på EU-nivå för samverkan mellan flera system på ett interoperabelt sätt, även de system som utvecklas och förvaltas av eu-LISA. Europol och Interpol skulle också uppmuntras att använda standarden.

Genom UMF-standardén införs ett gemensamt och enhetligt tekniskt språk för att beskriva och länka dataelement, i synnerhet de element som rör personer och (rese)handlingar. När UMF används vid utvecklingen av nya informationssystem garanteras en enklare integrering och interoperabilitet med andra system, i synnerhet för medlemsstater som måste bygga upp gränssnitt för att kommunicera med dessa nya system. I detta hänseende kan en obligatorisk användning av UMF vid utvecklingen av nya system anses som en nödvändig förutsättning för införandet av de interoperabilitetskomponenter som föreslås i denna förordning.

För att säkerställa ett fullständigt införande av UMF-standardén i hela EU föreslås en lämplig förvaltningsstruktur. Kommissionen skulle ansvara för att inrätta och utveckla UMF-standardén, inom ramen för ett granskningsförfarande med medlemsstaterna. De Schengenassocierade länderna, EU-byråer och internationella organ som deltar i UMF-projekt (t.ex. eu-LISA, Europol och Interpol) kommer också att delta. Den föreslagna förvaltningsstrukturen är avgörande för att det ska gå att förlänga och utöka UMF-standardén och samtidigt garantera största möjliga användbarhet och tillämplighet.

- 3) I detta förslag till förordning införs också koncepten **automatiserade kontrollmekanismer för uppgiftskvalitet** och gemensamma kvalitetsindikatorer, och vikten av att medlemsstaterna säkerställer högsta möjliga kvalitet på uppgifterna när de matar in uppgifter i och använder systemen. Om uppgifterna håller sämre kvalitet kan det inte bara leda till att man inte kan identifiera efterlysta personer, utan även påverka

oskyldiga människors grundläggande rättigheter. För att undvika att problem uppstår till följd av mänsklig inmatning av uppgifter kan automatiska valideringsregler hindra operatörer från att göra misstag. Målet är att automatiskt identifiera inmatade uppgifter som verkar vara inkorrekta eller inkonsekventa, så att ursprungsmedlemsstaten kan verifiera uppgifterna och vidta de korrigerande åtgärder som behövs. Detta skulle kompletteras med eu-LISA:s regelbundna rapporter om uppgiftskvalitet.

- **Konsekvenser för andra rättsakter**

Genom detta förslag till förordning och det anknyttande förslaget införs nyheter som kräver ändringar av följande rättsakter:

- Förordning (EU) 2016/399 (kodexen om Schengengränserna).
- Förordning (EU) 2017/2226 (förordningen om in- och utresesystemet).
- Förordning (EG) nr 767/2008 (VIS-förordningen).
- Rådets beslut 2004/512/EG (VIS-beslutet).
- Rådets beslut 2008/633/RIF (beslutet om åtkomst till VIS i brottsbekämpningssyfte).
- [Etiasförordningen.]
- [Eurodacförordningen.]
- [SIS-förordningarna.]
- [Förordningen om Ecris-TCN, inklusive motsvarande bestämmelser i förordning (EU) 2016/1624 (förordningen om den europeiska gräns- och kustbevakningen).]
- [Förordningen om eu-LISA.]

Föreliggande förslag och det anknyttande förslaget föreskriver i detalj de förändringar som måste göras i de rättsakter som för närvarande är stabila texter som antagits av medlagstiftarna, dvs. kodexen om Schengengränserna, förordningen om in- och utresesystemet, VIS-förordningen, rådets beslut 2008/633/RIF och rådets beslut 2004/512/EG.

De övriga rättsakterna i förteckningen (förordningarna om Etias, Eurodac, SIS, Ecris-TCN och eu-LISA) är för närvarande föremål för förhandlingar i Europaparlamentet och rådet. För dessa rättsakter är det därför inte möjligt att i detta skede fastställa nödvändiga ändringar. Kommissionen kommer att lägga fram ändringsförslag för var och en av dessa rättsakter inom två veckor efter det att en politisk överenskommelse om respektive förslag till förordning har nåtts.

- **Förenlighet med befintliga bestämmelser inom området**

Detta förslag läggs fram inom ramen för den bredare process som inleddes genom meddelandet *Starkare och smartare informationssystem för gränser och säkerhet* i april 2016 och det därpå följande arbetet i expertgruppen för informationssystem och interoperabilitet. Syftet är att eftersträva tre mål

- a) stärka och maximera nyttan av de **befintliga informationssystemen**,
- b) åtgärda informationsluckor genom att införa nya informationssystem,
- c) öka interoperabiliteten mellan systemen.

Vad gäller det första målet antog kommissionen i december 2016 förslag för att ytterligare stärka Schengens informationssystem (SIS) i dess nuvarande form²⁵. Vad Eurodac beträffar har förhandlingarna om en reviderad rättslig grund framskridit efter kommissionens förslag i maj 2016²⁶. Ett förslag till en ny rättslig grund för Informationssystemet för viseringar (VIS) håller också på att utarbetas och kommer att läggas fram under andra kvartalet 2018.

Vad gäller det andra målet slutfördes förhandlingarna om kommissionens förslag från april 2016 om att inrätta ett in- och utresesystem²⁷ redan i juli 2017, då medlagstiftarna nådde en politisk överenskommelse, som bekräftades av Europaparlamentet i oktober 2017 och formellt antogs av rådet i november 2017. Den rättsliga grunden träder i kraft i december 2017. Förhandlingarna om förslaget om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias)²⁸ från november 2016 har inletts och förväntas nå resultat inom de kommande månaderna. I juni 2017 föreslog kommissionen en rättslig grund för att komma till rätta med en annan informationslucka, nämligen det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN-systemet)²⁹. Även för denna rättsliga grund har medlagstiftarna angett att de strävar efter ett snabbt antagande.

Föreliggande förslag berör det tredje målet som anges i meddelandet från april 2016.

- **Förenlighet med annan unionspolitik på området rättsliga och inrikes frågor**

Detta förslag är tillsammans med det anknyttande förslaget en uppföljning av och förenligt med den europeiska migrationsagendan och efterföljande meddelanden, bland annat meddelandet om bevarande och stärkande av Schengen³⁰, den europeiska säkerhetsagendan³¹ och kommissionens arbete och rapporter om framstegen i riktning mot en effektiv och verklig säkerhetsunion³². Det är förenligt med annan unionspolitik, framför allt följande:

- Inre säkerhet: i europeiska säkerhetsagendan anges att gemensamma höga normer för gränsförvaltning är grundläggande för att förebygga gränsöverskridande brottslighet och terrorism. Detta förslag bidrar ytterligare till en hög nivå av inre säkerhet genom att myndigheterna får verktyg för snabb, smidig, systematisk och kontrollerad åtkomst till den information de behöver.
- Asylfrågor: förslaget inbegriper Eurodac som ett av de centrala EU-system som ska omfattas av interoperabilitet.
- Förvaltningen av de yttre gränserna och säkerhet: detta förslag förstärker SIS och VIS, som bidrar till en effektiv kontroll av unionens yttre gränser, samt det framtida in- och utresesystemet och de föreslagna systemen Etias och Ecris-TCN.

²⁵ COM(2016) 883 final.

²⁶ COM(2016) 272 final.

²⁷ COM(2016) 194 final.

²⁸ COM(2016) 731 final.

²⁹ COM(2017) 344 final.

³⁰ COM(2017) 570 final.

³¹ COM(2015) 185 final.

³² COM(2016) 230 final.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Den huvudsakliga rättsliga grunden är följande artiklar i fördraget om Europeiska unionens funktionssätt: artiklarna 16.2, 74, 78.2 e, 79.2 c, 82.1 d, 85.1, 87.2 a och 88.2.

Enligt artikel 16.2 har unionen befogenhet att fastställa bestämmelser om skydd för enskilda personer när det gäller behandling av personuppgifter hos unionens institutioner, organ och byråer och i medlemsstaterna, när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde, samt om den fria rörligheten för sådana uppgifter. Enligt artikel 74 kan rådet besluta om åtgärder för att säkerställa ett administrativt samarbete mellan de behöriga myndigheterna i medlemsstaterna på området med rättvisa, frihet och säkerhet. Enligt artikel 78 har unionen befogenhet att besluta om åtgärder om ett gemensamt europeiskt asylsystem. Enligt artikel 79.2 c har unionen befogenhet att besluta om åtgärder på området olaglig invandring och olaglig vistelse. Enligt artiklarna 82.1 d och 87.2 a har unionen befogenhet att besluta om åtgärder för att förstärka det polisiära och rättsliga samarbetet i fråga om insamling, lagring, behandling, analys och utbyte av relevant information. Enligt artiklarna 85.1 och 88.2 har unionen befogenhet att reglera Eurojusts respektive Europols uppgifter.

• Subsidiaritetsprincipen

Fri rörlighet inom EU förutsätter att unionens yttre gränser förvaltas effektivt för att säkerställa säkerheten. Medlemsstaterna har därför enats om att gemensamt ta itu med dessa utmaningar, i synnerhet genom att dela information genom centraliserade EU-system på området rättsliga och inrikes frågor. Detta bekräftas av de olika slutsatser som har antagits av både Europeiska rådet och rådet, framför allt sedan 2015.

Avsaknaden av kontroller vid de inre gränserna kräver en hållbar förvaltning av Schengenområdets yttre gränser, där varje medlemsstat eller Schengenassocierat land måste kontrollera de yttre gränserna på de andra Schengenstaternas vägnar. Följaktligen klarar ingen medlemsstat på egen hand av den irreguljära migrationen och gränsöverskridande brottsligheten. Tredjelandsmedborgare som rest in till området utan inre gränskontroller kan resa fritt inom det. Inom ett område utan inre gränser bör man vidta gemensamma åtgärder mot irreguljär invandring och internationell brottslighet och terrorism, även genom upptäckt av identitetsbedrägerier, och resultat kan endast nås med åtgärder på EU-nivå.

Viktiga gemensamma informationssystem har införts eller håller på att införas på EU-nivå. Ökad interoperabilitet mellan informationssystemen kräver oundvikligen åtgärder på EU-nivå. Kärnan i förslaget är ökad effektivitet och användning av de centraliserade system som förvaltas av eu-LISA. På grund av åtgärdens omfattning, effekter och konsekvenser kan de grundläggande syftena uppnås effektivt och systematiskt endast på EU-nivå.

• Proportionalitetsprincipen

Som förklaras i detalj i den konsekvensbedömning som åtföljer detta förslag till förordning anses de politiska val som görs i detta förslag vara proportionerliga. De går inte utöver vad som är nödvändigt för att uppnå de överenskomna målen.

Den **europeiska sökportalen (ESP)** är ett nödvändigt verktyg för att förbättra den bemyndigade användningen av befintliga och framtida EU-informationssystem. Konsekvenserna av den europeiska sökportalen är mycket begränsade i fråga om databehandling. Den kommer inte att lagra några uppgifter, förutom information om de olika

användarprofilerna för portalen, de uppgifter och informationssystem som de har åtkomst till samt loggar över deras användning. Den europeiska sökportalens möjliggörande och underlättande roll som meddelandehanterare är proportionerlig, nödvändig och begränsad i fråga om sökningar och åtkomsträttigheter inom de mandat som fastställs i de rättsliga grunderna för informationssystemen och den föreslagna förordningen om interoperabilitet.

Den **gemensamma biometriska matchningstjänsten** är nödvändig för att den europeiska sökportalen, den gemensamma databasen för identitetsuppgifter och detektorn för multipla identiteter ska fungera, och den underlättar användningen och underhållet av relevanta befintliga och framtida EU-informationssystem. Dess funktioner gör det möjligt att göra sökningar med biometriska uppgifter från olika källor på ett effektivt, smidigt och systematiskt sätt. De biometriska uppgifterna lagras och bevaras av de underliggande systemen. Den gemensamma biometriska matchningstjänsten skapar mallar men förkastar de faktiska bilderna. Uppgifterna lagras därmed endast en gång, på en enda plats.

Den **gemensamma databasen för identitetsuppgifter (CIR)** är nödvändig för att uppnå målet med korrekt identifiering av tredjelandsmedborgare, t.ex. under en identitetskontroll inom Schengenområdet. CIR stöder också detektorn för multipla identiteter och är därför en nödvändig komponent för att uppnå det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. Åtkomsten till CIR för detta ändamål är begränsad till de användare som behöver denna information för att utföra sina uppgifter (vilket kräver att dessa kontroller blir ett nytt underordnat syfte med Eurodac, VIS, det framtida in- och utresesystemet och de föreslagna systemen Etias och Ecris-TCN). Uppgiftsbehandlingen är strikt begränsad till vad som är nödvändigt för att uppnå detta mål, och lämpliga skyddsåtgärder kommer att inrättas för att säkerställa att åtkomsträttigheterna respekteras och att endast de uppgifter som är nödvändiga lagras i CIR. För att säkerställa uppgiftsminimering och undvika onödig dubblering av uppgifter håller CIR de erforderliga personuppgifterna från vart och ett av de underliggande systemen – lagrade, tillagda, ändrade och raderade i enlighet med deras respektive rättsliga grund – utan att kopiera dem. Bestämmelserna om lagring av uppgifter stämmer helt överens med bestämmelserna om lagring av uppgifter i de underliggande informationssystem som tillhandahåller identitetsuppgifterna.

Detektorn för multipla identiteter (MID) är nödvändig för att göra det möjligt att spåra multipla identiteter i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. MID kommer att innehålla länkar mellan personer som har registrerats i flera än ett centralt informationssystem, strikt begränsat till de uppgifter som behövs för att verifiera om en person har registrerats lagligen eller olagligen med olika biografiska identiteter i olika system, men även för att klargöra att två personer med liknande biografiska uppgifter inte är samma person. Uppgiftsbehandlingen i MID och den gemensamma biometriska matchningstjänsten begränsas till det absoluta minimum som behövs för att länka personakter i enskilda system. MID kommer att omfatta skyddsåtgärder mot potentiell diskriminering eller ogynnsamma beslut mot personer som lagligen har multipla identiteter.

- **Val av instrument**

Som instrument föreslås Europaparlamentets och rådets förordning. Den föreslagna lagstiftningen berör direkt driften av centrala EU-informationssystem för gränser och säkerhet, som alla har inrättats, eller föreslås inrättas, genom förordningar. Även eu-LISA, som kommer att ansvara för utformningen och utvecklingen – och så småningom den tekniska

förvaltningen – av komponenterna, har inrättats genom en förordning. En förordning är därför det lämpliga valet av instrument.

3. RESULTAT AV SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

• Offentligt samråd

Vid utarbetandet av detta förslag inledde kommissionen i juli 2017 ett offentligt samråd för att få in synpunkter från berörda parter om interoperabilitet. Under samrådet inkom 18 svar från olika berörda parter, bland annat medlemsstaternas regeringar, organisationer inom den privata sektorn och andra organisationer såsom icke-statliga organisationer och tankesmedjor samt privatpersoner³³. Svaren var på det hela taget positiva till de underliggande principerna i detta interoperabilitetsförslag. De allra flesta svarande höll med om att både de frågor som togs upp i samrådet och de mål som man vill uppnå med interoperabilitetspaketet är de korrekta. I synnerhet ansåg de svarande att de alternativ som beskrivs i samrådsdokumentet skulle

- hjälpa personal på fältet att få åtkomst till den information de behöver,
- bli av med dubblering av uppgifter, minska överlappningar och framhäva skillnader i uppgifterna,
- identifiera personer på ett mer tillförlitligt sätt – även personer med multipla identiteter – och minska antalet identitetsbedrägerier.

En klar majoritet av de svarande understödde vart och ett av de föreslagna alternativen och ansåg att de är nödvändiga för att uppnå initiativets mål; i sina svar underströk de behovet av starka och tydliga dataskyddsåtgärder, i synnerhet i fråga om åtkomst till den information som lagras i systemen och lagring av uppgifter samt behovet av aktuella uppgifter av hög kvalitet i systemen och åtgärder för att säkerställa detta.

Alla synpunkter som framfördes har beaktats vid utarbetandet av detta förslag.

• Eurobarometerundersökning

I juni 2017 genomfördes en särskild Eurobarometerundersökning³⁴ som visade att EU:s strategi för utbyte av information på EU-nivå för att bekämpa brottslighet och terrorism har brett stöd från allmänheten – nästan alla svarande (92 %) håller med om att de nationella myndigheterna bör utbyta information med de andra medlemsstaternas myndigheter för att bättre kunna bekämpa brottslighet och terrorism.

En klar majoritet (69 %) av de svarande ansåg att polisen och andra nationella brottsbekämpande myndigheter systematiskt bör utbyta information med andra EU-länder. I alla medlemsstater anser en majoritet av de svarande att information bör utbytas i varje enskilt fall.

³³ Mer detaljer finns i den sammanfattning som bifogas konsekvensbedömningen.

³⁴ I rapporten om européernas inställning till säkerhet analyseras resultaten av den särskilda Eurobarometerundersökningen (464b) när det gäller medborgarnas allmänna medvetenhet om, erfarenheter av och uppfattningar om säkerhet. Undersökningen genomfördes av TNS Political & Social i de 28 medlemsstaterna den 13–26 juni 2017. Man intervjuade 28 093 EU-medborgare från olika sociala och demografiska kategorier.

- **Expertgruppen för informationssystem och interoperabilitet**

Som redan angavs i inledningen bygger detta förslag på rekommendationerna från **expertgruppen för informationssystem och interoperabilitet**³⁵. Gruppen inrättades i juni 2016 med målet att bedöma de rättsliga, tekniska och operativa utmaningarna med de alternativ som finns att tillgå för att uppnå interoperabilitet mellan centrala EU-system för gränser och säkerhet. Gruppen bedömde uppgiftshanteringsstrukturen för gränsförvaltning och brottsbekämpning från ett brett och övergripande perspektiv och beaktade även tullmyndigheternas relevanta roller, ansvarsområden och system.

Gruppen bestod av experter från medlemsstaterna och de Schengenassocierade länderna och från EU-organen eu-LISA, Europol, Europeiska stödkontoret för asylfrågor, Europeiska gräns- och kustbevakningsbyrån och EU:s byrå för grundläggande rättigheter. EU:s samordnare för kampen mot terrorism och Europeiska datatillsynsmannen deltog också som fullvärdiga medlemmar i expertgruppen. Dessutom deltog företrädare för sekretariatet för Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor och rådets generalsekretariat som observatörer.

Expertgruppens slutrapport offentliggjordes i maj 2017³⁶. Där underströks behovet av att agera för att komma till rätta med de strukturella brister som identifierats i meddelandet från april 2016. Rapporten innehöll en rad rekommendationer för att stärka och utveckla EU:s informationssystem och interoperabiliteten. Slutsatsen var att det är **nödvärdigt och tekniskt genomförbart att arbeta för den europeiska sökportalen, den gemensamma biometriska matchningstjänsten och den gemensamma databasen för identitetsuppgifter som lösningar för interoperabilitet** och att de i princip kan ge både operativa fördelar och fastställas i överensstämmelse med dataskyddskraven. Gruppen rekommenderade också att man överväger det ytterligare alternativet att införa en tvåstegsstrategi för åtkomst i brottsbekämpningssyfte, på grundval av en flaggfunktion vid träff.

Detta förslag till en förordning är också ett svar på expertgruppens rekommendationer om uppgiftskvalitet, det universella meddelandeformatet (UMF) och inrättandet av ett datalager (som här presenteras som den centrala databasen för rapporter och statistik, CRRS).

Den fjärde interoperabilitetskomponent som föreslås i detta förslag till förordning (detektorn för multipla identiteter) förordades inte av expertgruppen, utan är en följd av den ytterligare tekniska analysen och kommissionens proportionalitetsbedömning.

- **Tekniska studier**

Tre studier har beställts för att stödja utarbetandet av förslaget. Enligt avtal med kommissionen har Unisys rapporterat om en genomförbarhetsstudie om den europeiska sökportalen. Eu-LISA har beställt en teknisk rapport från Gartner (med Unisys) för att stödja utvecklingen av den gemensamma biometriska matchningstjänsten. PWC har tillställt kommissionen en teknisk rapport om en gemensam databas för identitetsuppgifter.

- **Konsekvensbedömning**

Detta förslag stöds av en konsekvensbedömning som presenteras i det åtföljande arbetsdokumentet **SWD(2017) XXX**.

³⁵ Kommissionens beslut av den 17 juni 2016 om inrättande av en expertgrupp för informationssystem och interoperabilitet, EUT C 257, 15.7.2016, s. 3.

³⁶ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.

Nämnden för lagstiftningskontroll såg över utkastet till konsekvensbedömning vid sitt möte den 6 december 2017 och lämnade sitt yttrande (positivt, med förbehåll) den 8 december och angav att konsekvensbedömningen bör justeras för att integrera nämndens rekommendationer om vissa aspekter. Dessa rörde i första hand ytterligare åtgärder inom ramen för det föredragna alternativet för att enhetliggöra slutanvändarnas befintliga åtkomsträttigheter till uppgifter i EU-informationssystem och förtydliga därmed sammanhängande skyddsåtgärder för dataskydd och grundläggande rättigheter. Den andra huvudsakliga synpunkten var att man behövde klargöra integreringen av Schengens informationssystem under alternativ 2, och inkludera effektivitet och kostnader för att underlätta jämförelsen med det föredragna alternativ 3. Kommissionen har uppdaterat konsekvensbedömningen för att beakta dessa huvudsakliga synpunkter och ett flertal andra kommentarer som nämnden lämnat.

I konsekvensbedömningen utvärderades om och hur vart och ett av de fastställda målen skulle kunna uppnås med hjälp av en eller flera av de tekniska komponenter som identifierats av expertgruppen och under senare analys. Vid behov undersöktes också underalternativ som skulle krävas för att uppnå dessa mål och samtidigt respektera dataskyddsramen. Slutsatserna av konsekvensbedömningen var följande:

- För att uppfylla målet att ge bemyndigade användare snabb, smidig, systematisk och kontrollerad åtkomst till relevanta informationssystem bör man inrätta en europeisk sökportal (ESP) som bygger på en gemensam biometrisk matchningstjänst så att alla databaser beaktas.
- För att uppfylla målet att underlätta bemyndigade tjänstemäns kontroller av tredjelandsmedborgares identitet på en medlemsstats territorium bör man inrätta en gemensam databas för identitetsuppgifter (CIR) som innehåller en minimiuppsättning av identitetsuppgifter och som bygger på samma gemensamma biometriska matchningstjänst.
- För att uppfylla målet att spåra multipla identiteter som används med samma biometriska uppgifter, i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri, bör man bygga en detektor för multipla identiteter (MID) som innehåller länkar mellan olika identiteter mellan systemen.
- För att uppfylla målet att underlätta och rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning, i syfte att förebygga, utreda, upptäcka eller lagföra grov brottslighet och terrorism, bör en flaggfunktion vid träff inkluderas i CIR.

Eftersom alla målen ska uppfyllas är den **kompleta lösningen en kombination av ESP, CIR (med flaggning vid träff) och MID, som alla grundar sig på den gemensamma biometriska matchningstjänsten.**

Den största positiva effekten blir bättre gränsförvaltning och ökad inre säkerhet inom Europeiska unionen. De nya komponenterna kommer att rationalisera och påskynda de nationella myndigheternas åtkomst till nödvändig information och identifieringen av tredjelandsmedborgare. De kommer att göra det möjligt för myndigheter att korskontrollera befintlig, nödvändig information om enskilda personer vid gränskontroller, för ansökningar om visering eller asyl och för polisarbete. Detta möjliggör åtkomst till information som gör det lättare att fatta tillförlitliga beslut, oavsett om det rör sig om utredningar av grov brottslighet och terrorism eller beslut på området migration och asyl. Även om förslagen inte direkt påverkar EU-medborgare (de föreslagna åtgärderna är främst inriktade på

tredjelandssmedborgare vars uppgifter registrerats i något av EU:s centraliserade informationssystem) förväntas de öka allmänhetens förtroende genom att säkerställa att utformningen och användningen ökar säkerheten för EU-medborgare.

De omedelbara finansiella och ekonomiska konsekvenserna av förslaget är begränsade till utformningen, utvecklingen och driften av de nya anläggningarna. Kostnaderna kommer att belasta EU-budgeten och medlemsstaternas myndigheter som driver systemen. Inverkan på turismen kommer att vara positiv eftersom de föreslagna åtgärderna både förbättrar säkerheten i Europeiska unionen och gynnar snabbare gränskontroller. Likaledes väntas konsekvenserna för flygplatser, hamnar och operatörer bli positiva, i synnerhet på grund av snabbare in- och utresekontroller.

- **Grundläggande rättigheter**

Vid konsekvensbedömningen granskades särskilt de föreslagna åtgärdernas konsekvenser för de grundläggande rättigheterna, och då i synnerhet rätten till dataskydd.

I enlighet med EU:s stadga om de grundläggande rättigheterna (nedan kallad *stadgan*), som är bindande för EU-institutionerna och medlemsstaterna, när dessa tillämpar unionsrätten (artikel 51.1 i stadgan), måste interoperabilitetens möjligheter att förbättra säkerheten och skyddet av de yttre gränserna vägas mot skyldigheten att säkerställa att sådana ingrepp i de grundläggande rättigheterna som kan uppkomma till följd av den nya interoperabilitetsmiljön begränsas till vad som är strikt nödvändigt för att faktiskt svara mot de mål av allmänt samhällsintresse som eftersträvas, med förbehåll för proportionalitetsprincipen (artikel 52.1 i stadgan).

De föreslagna interoperabilitetslösningarna är kompletterande komponenter till befintliga system. Som sådana skulle de inte rubba den jämvikt som redan säkerställs av varje befintligt centralt system vad gäller deras positiva inverkan på de grundläggande rättigheterna.

Trots det har interoperabiliteten en potential att få en ytterligare, indirekt inverkan på flera grundläggande rättigheter. En korrekt identifiering av en person har faktiskt en positiv inverkan på rätten till respekt för privatlivet, och i synnerhet rätten till en persons identitet (artikel 7 i stadgan), då detta kan bidra till mindre förvirring kring identiteten. Å andra sidan kan kontroller baserade på biometriska uppgifter uppfattas som en kränkning av personens rätt till värdighet (särskilt om det uppfattas som förödmjukande) (artikel 1 i stadgan). Emellertid tillfrågades deltagarna i en enkät³⁷ gjord av EU:s byrå för grundläggande rättigheter uttryckligen om de anser att det skulle vara förödmjukande att lämna sina biometriska uppgifter i samband med gränskontroll. Merparten av de svarande ansåg inte att detta skulle vara fallet.

De föreslagna interoperabilitetskomponenterna ger möjligheten att anta riktade förebyggande åtgärder för att öka säkerheten. Därmed kan de bidra till att skydda människors rätt till liv (artikel 2 i stadgan), vilket även innebär en positiv skyldighet för myndigheterna att vidta förebyggande operativa åtgärder för att skydda en person vars liv är i fara, om de känner till eller borde ha känt till att det föreligger en överhängande risk³⁸, samt att upprätthålla förbudet

³⁷ Rapport om en enkät från Europeiska unionens byrå för grundläggande rättigheter inom ramen för eu-LISA:s pilotprojekt om smarta gränser – resenärers åsikter om och erfarenheter av smarta gränser: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

³⁸ Europeiska domstolen för de mänskliga rättigheternas dom av den 28 oktober 1998, Osman/Förenade kungariket, nr. 87/1997/871/1083, punkt 116.

mot slaveri och tvångsarbete (artikel 5 i stadgan). Tack vare en tillförlitlig, mer tillgänglig och enklare identifiering kan interoperabilitet stödja upptäckten av försvunna barn eller barn som utsätts för människohandel samt underlätta snabba och riktade insatser.

En tillförlitlig, mer tillgänglig och enklare identifiering skulle också bidra till att i praktiken säkerställa rätten till asyl (artikel 18 i stadgan) och förbudet mot avvisning (artikel 19 i stadgan). Interoperabilitet skulle faktiskt kunna förhindra situationer där asylsökande olagligen grips, hålls i förvar och blir föremål för otillbörlig avvisning eller utvisning. Dessutom skulle interoperabiliteten göra det lättare att identifiera identitetsbedrägeri. Det skulle också minska behovet av att dela uppgifter om asylsökande med tredjeländer (framför allt ursprungslandet) i syfte att fastställa personens identitet och erhålla resehandlingar, vilket potentiellt kan utsätta den berörda personen för fara.

• **Skydd av personuppgifter**

Med tanke på de personuppgifter som är involverade kommer interoperabiliteten särskilt att ha en inverkan på rätten till skydd av personuppgifter. Denna rätt fastställs i artikel 8 i stadgan, artikel 16 i fördraget om Europeiska unionens funktionssätt och artikel 8 i Europakonventionen om de mänskliga rättigheterna. Såsom har framhållits av Europeiska unionens domstol³⁹ är rätten till skydd av personuppgifter inte en absolut rättighet, utan ska beaktas i förhållande till dess funktion i samhället⁴⁰. Dataskyddet är nära knutet till respekten för privatlivet och familjelivet som skyddas genom artikel 7 i stadgan.

Enligt den allmänna dataskyddsförordningen⁴¹ får det fria flödet av uppgifter inom EU inte begränsas av dataskyddsskäl. Ett antal principer måste dock följas. För att vara laglig måste varje begränsning i utövandet av grundläggande rättigheter som skyddas i stadgan uppfylla följande kriterier, som anges i artikel 52.1:

- Den ska vara föreskriven i lag.
- Den ska vara förenlig med det väsentliga innehållet i rättigheterna.
- Den ska faktiskt svara mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.
- Den ska vara nödvändig.
- Den ska vara proportionerlig.

Genom detta förslag införlivas alla dessa dataskyddregler, vilket beskrivs i detalj i den konsekvensbedömning som åtföljer detta förslag till förordning. Förslaget bygger på principerna om inbyggt dataskydd och dataskydd som standard. Det innehåller alla lämpliga bestämmelser varigenom behandlingen av uppgifter begränsas till vad som är nödvändigt för

³⁹ Domstolens dom av den 9 november 2010, Volker und Markus Schecke och Eifert/Land Hessen, förenade målen C-92/09 och C-93/09, ECR I-0000.

⁴⁰ I enlighet med artikel 52.1 i stadgan får utövandet av rätten till dataskydd begränsas, under förutsättning att begränsningarna har föreskrivits i lag, är förenliga med det väsentliga innehållet i rättigheten och friheterna och, med beaktande av proportionalitetsprincipen, endast görs om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

⁴¹ 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).

det särskilda ändamålet och åtkomst till uppgifterna beviljas endast till de som verkligen har ett behov av att känna till dem. Perioderna för lagring av uppgifter (i tillämpliga fall) är lämpliga och begränsade. Åtkomsten till uppgifter är uteslutande förbehållen vederbörligen bemyndigad personal vid medlemsstaternas myndigheter eller EU-organ som är behöriga för respektive informationssystemets särskilda ändamål och begränsad i den utsträckning uppgifterna behövs för att utföra uppgifter i enlighet med dessa ändamål.

4. BUDGETKONSEKVENSER

Budgetkonsekvenserna anges i den bifogade finansieringsöversikten. Den täcker den period som återstår av den gällande fleråriga budgetramen (fram till 2020) och de sju åren i följande period (2021–2027). Den föreslagna budgeten för år 2021 och framåt inkluderas i illustrerande syfte och föregriper inte nästa fleråriga budgetram.

Genomförandet av detta förslag kräver budgetmedel för följande:

- (1) Eu-LISA:s **utveckling** och integrering av de fyra interoperabilitetskomponenterna och den centrala databasen för rapporter och statistik samt efterföljande **underhåll och drift**.
- (2) **Datamigreringen** till den gemensamma biometriska matchningstjänsten och den gemensamma databasen för identitetsuppgifter (CIR). När det gäller den gemensamma biometriska matchningstjänsten måste de biometriska mallarna för motsvarande uppgifter från de tre system som för närvarande utnyttjar biometriska uppgifter (SIS, VIS och Eurodac) återskapas i den gemensamma biometriska matchningstjänsten. När det gäller CIR måste persondataelementen från VIS migreras till CIR och möjliga länkar mellan identiteter i SIS, VIS och Eurodac valideras. I synnerhet den sistnämnda processen är mycket resurskrävande.
- (3) Eu-LISA:s uppdatering av det **enhetliga nationella gränssnitt** som redan ingår i förordningen om in- och utresesystemet till att bli en generisk komponent som möjliggör utbyte av meddelanden mellan medlemsstaterna och centrala system.
- (4) **Integreringen av medlemsstaternas nationella system** med det enhetliga nationella gränssnitt som vidarebefordrar de meddelanden som utbyts med CIR/detektorn för multipla identiteter genom den europeiska sökportalen.
- (5) **Utbildning** om slutanvändarnas användning av interoperabilitetskomponenterna, bland annat genom Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Cepol).

Interoperabilitetskomponenterna byggs och underhålls som ett program. Den europeiska sökportalen, detektorn för multipla identiteter och den centrala databasen för rapporter och statistik är helt nya komponenter, medan den gemensamma biometriska matchningstjänsten och CIR är delade komponenter som kombinerar befintliga uppgifter som lagras (eller kommer att lagras) i befintliga eller nya system med deras befintliga budgetberäkningar.

Den **europeiska sökportalen** kommer att utnyttja befintliga, kända gränssnitt mot SIS, VIS och Eurodac och kommer i sinom tid att utvidgas till de nya systemen.

ESP kommer att användas av medlemsstaterna och organ genom ett gränssnitt som baseras på det universella meddelandeformatet (UMF). Detta nya gränssnitt kommer att kräva utveckling, anpassning, integrering och provning av medlemsstaterna, eu-LISA, Europol och Europeiska gräns- och kustbevakningsbyrån. ESP skulle använda konceptet med det enhetliga

nationella gränssnitt som introducerades för in- och utresesystemet, vilket skulle underlätta integreringsarbetet.

Den europeiska sökportalen kommer att leda till extrakostnader för Europol för arbetet med att göra QUEST-gränssnittet tillgängligt för användning med uppgifter med grundläggande skyddsnivå.

Grunden för den **gemensamma biometriska matchningstjänsten** kommer i praktiken att inrättas i och med skapandet av det nya in- och utresesystemet eftersom detta utgör den avgjort största volymen av nya biometriska uppgifter. Den budget som krävs reserverades genom det rättsliga instrumentet för in- och utresesystemet. Tillägg av ytterligare biometriska uppgifter från VIS, SIS och Eurodac till den gemensamma biometriska matchningstjänsten utgör extra kostnader främst i samband med migreringen av befintliga uppgifter. Dessa uppskattas till 10 miljoner EUR för alla tre systemen. Tillägg av nya biometriska uppgifter från det föreslagna Ecris-TCN-systemet utgör en begränsad extra kostnad som kan täckas med de medel som avsatts i systemets rättsliga instrument för att inrätta ett system för automatisk identifiering av fingeravtryck i Ecris-TCN.

Den **gemensamma databasen för identitetsuppgifter** kommer att inrättas i samband med skapandet av det framtida in- och utresesystemet och utvidgas ytterligare vid utvecklingen av det föreslagna Etias. Lagring och sökmotorer för dessa uppgifter ingår i den budget som avsatts genom de rättsliga instrumenten för det framtida in- och utresesystemet och det föreslagna Etias. Att lägga till nya biografiska uppgifter från både Eurodac och det föreslagna Ecris-TCN-systemet utgör en mindre ytterligare kostnad som redan avsatts genom de rättsliga instrumenten för Eurodac och det föreslagna Ecris-TCN-systemet.

Den totala budget som krävs under nio år (2019–2027) uppgår till 424,7 miljoner EUR, vilket inbegriper följande:

- (1) En budget på 225 miljoner EUR för eu-LISA, vilken täcker de totala programkostnaderna för utvecklingen av de fem interoperabilitetskomponenterna (68,3 miljoner EUR), underhållskostnaderna från leveransen av komponenterna fram till 2027 (56,1 miljoner EUR), en särskild budget på 25 miljoner EUR för migration av uppgifter från befintliga system till den gemensamma biometriska matchningstjänsten och de extra kostnaderna för uppdateringen av det enhetliga nationella gränssnittet, nätverk, utbildning och möten. En särskild budget på 18,7 miljoner EUR täcker kostnaderna för uppgradering och drift av Ecris-TCN med hög tillgänglighet från och med 2022.
- (2) En budget på 136,3 miljoner EUR till medlemsstaterna för att täcka ändringarna av deras nationella system för att använda interoperabilitetskomponenterna, det enhetliga nationella gränssnitt som eu-LISA levererar och en budget för utbildning av det betydande antalet slutanvändare.
- (3) En budget på 48,9 miljoner EUR till Europol för att täcka uppgraderingen av kapaciteten hos byråns it-system att hantera mängden meddelanden och den ökade prestandanivån⁴². Interoperabilitetskomponenterna kommer att användas av Etias för att konsultera Europoluppgifter.
- (4) En budget på 4,8 miljoner EUR till Europeiska gräns- och kustbevakningsbyrån för

⁴² Europols nuvarande kapacitet att hantera information är inte förenlig med de betydande volymerna (i genomsnitt 100 000 sökningar per dag) och den kortare svarstid som kommer att krävas för Etias.

att ta emot en grupp specialister som under ett år kommer att validera länkarna mellan identiteter vid den tidpunkt då detektorn för multipla identiteter tas i bruk.

- (5) En budget på 2,0 miljoner EUR till Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Cepol) för att täcka utarbetande och tillhandahållande av utbildning för operativ personal.
- (6) Ett anslag på 7,7 miljoner EUR till GD Migration och inrikes frågor för att täcka en begränsad ökning av personalen och därmed sammanhängande kostnader under utvecklingen av de olika komponenterna, eftersom kommissionen också måste fullgöra ytterligare uppgifter under den perioden och tar ansvaret för det utskott som sköter det universella meddelandeformatet.

Förordningen om fonden för inre säkerhet och stödet för yttre gränser är det finansieringsinstrument som innehåller budgeten för genomförande av interoperabilitetsinitiativet. I artikel 5 b anges att 791 miljoner EUR ska användas genom ett program för utveckling av it-system på grundval av befintliga och/eller nya system som stöd för hanteringen av migrationsströmmar över de yttre gränserna, med förbehåll för att de relevanta unionslagstiftningsakterna antas och på de villkor som avses i artikel 15.5. Av dessa 791 miljoner EUR är 480,2 miljoner EUR avsatta för utvecklingen av in- och utresesystemet, 210 miljoner EUR för Etias och 67,9 miljoner EUR för översynen av SIS. Återstoden (32,9 miljoner EUR) ska omfördelas med mekanismer inom fonden för inre säkerhet – gränser och viseringar. Det föreliggande förslaget kräver 32,1 miljoner EUR för den nuvarande fleråriga budgetramperioden (2019–20), vilket därmed är förenligt med den återstående budgeten.

5. ÖVRIGT

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

Eu-LISA ansvarar för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa. Därmed har byrån redan anförtrots driften och tekniska och operativa förbättringar av befintliga system samt utveckling av framtida system som redan planeras. I enlighet med detta förslag till förordning kommer den att fastställa utformningen av den fysiska arkitekturen för interoperabilitetskomponenterna, utveckla och implementera dem, och i slutändan hysa dem. Respektive komponent kommer att tas i bruk gradvis, i samma takt som de underliggande systemen utvecklas.

Kommissionen kommer att säkerställa att det finns system för att övervaka utvecklingen av och funktionen hos de fyra komponenterna (den europeiska sökportalen, den gemensamma biometriska matchningstjänsten, den gemensamma databasen för identitetsuppgifter och detektorn för multipla identiteter) och den centrala databasen för rapporter och statistik samt utvärdera dem mot de huvudsakliga politiska målen. Fyra år efter det att funktionerna har införts och är i drift, och vart fjärde år därefter, bör eu-LISA tillstålla Europaparlamentet, rådet och kommissionen en rapport om interoperabilitetskomponenternas tekniska funktion. Dessutom bör kommissionen fem år efter det att funktionerna har införts och är i drift, och vart fjärde år därefter, utarbeta en övergripande utvärdering av komponenterna, bland annat deras direkta eller indirekta effekter och de praktiska konsekvenserna för de grundläggande rättigheterna. Vid utvärderingen bör man granska uppnådda resultat jämfört med målen och bedöma huruvida de underliggande orsakerna fortfarande är aktuella och eventuella följder för

framtida alternativ. Kommissionen bör lämna utvärderingsrapporterna till Europaparlamentet och rådet.

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

I kapitel I anges de allmänna bestämmelserna i denna förordning. Där förklaras de principer som ligger till grund för förordningen, de komponenter som inrättas, de mål man vill uppnå genom interoperabilitet, förordningens tillämpningsområde, definitionerna av de termer som används i förordningen och principen om icke-diskriminering i fråga om behandling av uppgifter inom ramen för denna förordning.

I kapitel II fastställs bestämmelserna för den europeiska sökportalen (ESP). I kapitlet föreskrivs inrättandet av ESP och dess tekniska struktur, som ska utvecklas av eu-LISA. Där fastställs målet med ESP, vem som får använda portalen och hur de ska använda den i enlighet med befintliga åtkomsträttigheter för vart och ett av de centrala systemen. Det anges att eu-LISA ska skapa användarprofiler för varje kategori av användare. I detta kapitel fastställs hur den europeiska sökportalen kommer att söka i centrala system och föreskrivs innehållet i och formatet för svar till användarna. I kapitel II föreskrivs också att eu-LISA ska föra logg över all behandling av uppgifter, och det föreskrivs ett alternativt förfarande utifall att ESP inte kan tillgå ett eller flera av de centrala systemen.

I kapitel III fastställs bestämmelser för den gemensamma biometriska matchningstjänsten. I kapitlet föreskrivs inrättandet av den gemensamma biometriska matchningstjänsten och dess tekniska struktur, som ska utvecklas av eu-LISA. Där fastställs målet med den gemensamma biometriska matchningstjänsten och vilka uppgifter som lagras. Där förklaras förhållandet mellan den gemensamma biometriska matchningstjänsten och de andra komponenterna. I kapitel III fastställs också att den gemensamma biometriska matchningstjänsten kommer att upphöra att lagra uppgifterna så snart uppgifterna inte längre finns i respektive centrala system och att eu-LISA kommer att föra logg över all behandling.

I kapitel IV fastställs bestämmelser för den gemensamma databasen för identitetsuppgifter (CIR). I kapitlet föreskrivs inrättandet av CIR och dess tekniska struktur, som ska utvecklas av eu-LISA. Där fastställs målet med CIR och klargörs vilka uppgifter som kommer att lagras och hur, bland annat bestämmelser som säkerställer kvaliteten på de uppgifter som lagras. I detta kapitel anges att CIR kommer att skapa personakter på grundval av uppgifter som lagras i centrala system, och att personakter uppdateras i enlighet med ändringar i de enskilda centrala systemen. I kapitel IV specificeras det också hur CIR kommer att fungera i förhållande till detektorn för multipla identiteter. I detta kapitel anges vilka som kan få åtkomst till CIR och hur de kan komma åt uppgifterna i enlighet med åtkomsträttigheter, och mer specifika bestämmelser beroende på om åtkomsten syftar till identifiering eller, som ett första steg i en tvåstegsstrategi, åtkomst till in- och utresesystemet, VIS, Etias och Eurodac via CIR för brottsbekämpande ändamål. I kapitel IV anges också att eu-LISA kommer att föra logg över all behandling av uppgifter i CIR.

I kapitel V fastställs bestämmelser för detektorn för multipla identiteter (MID). I kapitlet föreskrivs inrättandet av MID och dess tekniska struktur, som ska utvecklas av eu-LISA. Där fastställs målet med MID och regleras användningen av MID i enlighet med åtkomsträttigheterna för vart och ett av de centrala systemen. I kapitel V anges när och hur MID kommer att inleda sökningar för att spåra multipla identiteter, och hur resultat levereras och följs upp, även genom manuell verifiering vid behov. I kapitlet anges en klassificering av de typer av länkar som kan vara resultatet av sökningen beroende på om resultatet visar en enda identitet, multipla identiteter eller gemensamma identitetsuppgifter. Enligt detta kapitel kommer MID att lagra länkade uppgifter lagrade i centrala system, medan uppgifterna blir

kvar i två eller flera enskilda centrala system. I kapitel V anges också att eu-LISA kommer att föra logg över all behandling av uppgifter i MID.

I kapitel VI föreskrivs åtgärder till stöd för interoperabilitet. Åtgärderna ska förbättra uppgifternas kvalitet, fastställa det universella meddelandeformatet som den gemensamma standarden för informationsutbyte för ökad interoperabilitet och skapa en central databas för rapporter och statistik.

Kapitel VII handlar om dataskydd. Kapitlet innehåller bestämmelser som säkerställer att uppgifter som behandlas enligt denna förordning behandlas lagligt och korrekt, i enlighet med förordning nr 45/2001. Där förklaras vem som kommer att vara databehandlare för var och en av de åtgärder för interoperabilitet som föreslås i denna förordning, fastställs åtgärder som krävs av eu-LISA och medlemsstaternas myndigheter för att säkerställa databehandlingens säkerhet, uppgifternas konfidentialitet, lämplig hantering av säkerhetsincidenter och lämplig övervakning av att bestämmelserna i denna förordning efterlevs. Kapitlet innehåller också bestämmelser om registrerades rättigheter, bland annat rätten att bli informerad om att uppgifter om dem har lagrats och behandlats i enlighet med denna förordning samt rätten att få åtkomst till, rätta och radera personuppgifter som har lagrats och behandlats i enlighet med denna förordning. Kapitlet fastställer vidare principen om att uppgifter som behandlas i enlighet med denna förordning inte får överföras eller göras tillgängliga för tredjeländer, internationella organisationer eller privata aktörer, förutom när det gäller Interpol för vissa specifika syften och uppgifter som erhållits från Europol via den europeiska sökportalen för vilka bestämmelserna i förordning 2016/794 om databehandling i senare led är tillämpliga. Slutligen innehåller kapitlet bestämmelser om tillsyn och revision i fråga om dataskydd.

I kapitel VIII fastställs eu-LISA:s skyldigheter före och efter det att åtgärderna i detta förslag tas i drift samt medlemsstaternas, Europol och Etias centralenhets skyldigheter.

Kapitel IX innehåller uppgifter om statistik- och rapporteringskrav för uppgifter som behandlas i enlighet med denna förordning, övergångsåtgärder som kommer att krävas, arrangemang kring kostnader som följer av denna förordning, meddelandekrav, processen för driftsättning av åtgärder som föreslås i denna förordning, styrformer, bland annat inrättandet av en kommitté och en rådgivande grupp, eu-LISA:s ansvar avseende utbildning och en praktisk handbok till stöd för implementering och förvaltning av interoperabilitetskomponenterna, förfaranden för övervakning och utvärdering av de åtgärder som föreslås i denna förordning samt bestämmelser om förordningens ikraftträdande.

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om inrättande av en ram för interoperabilitet mellan EU-informationssystem (polissamarbete och rättsligt samarbete, asyl och migration)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 16.2, 74, 78.2 e, 79.2 c, 82.1 d, 85.1, 87.2 a och 88.2,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

efter samråd med Europeiska datatillsynsmannen,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande⁴³,

med beaktande av Regionkommitténs yttrande⁴⁴,

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

- (1) Kommissionen underströk i sitt meddelande *Starkare och smartare informationssystem för gränser och säkerhet*⁴⁵ av den 6 april 2016 behovet av att förbättra unionens uppgiftshanteringsstruktur för gränsförvaltning och säkerhet. Kommissionen inledde ett arbete för att uppnå interoperabilitet mellan EU-informationssystem för säkerhet, gränser och migrationshantering, i syfte att komma till rätta med systemens strukturella brister som hindrar de nationella myndigheternas arbete och att säkerställa att gränskontrolltjänstemän, tullmyndigheter, poliser och rättsliga myndigheter har tillgång till den information de behöver.
- (2) Rådet identifierade i sin Färdplan för förbättring av informationsutbytet och informationshanteringen, inbegripet interoperabilitetslösningar på området för rättsliga och inrikes frågor av den 6 juni 2016⁴⁶ olika rättsliga, tekniska och operativa utmaningar när det gäller interoperabilitet mellan EU-informationssystem och efterlyste en strävan efter lösningar.
- (3) I sin resolution av den 6 juli 2016 om de strategiska prioriteringarna för kommissionens arbetsprogram 2017⁴⁷ efterlyste Europaparlamentet förslag för att förbättra och utveckla befintliga EU-informationssystem, åtgärda luckor i

⁴³ EUT C , , s . .

⁴⁴

⁴⁵ COM(2016) 205, 6.4.2016.

⁴⁶ Färdplan av den 6 juni 2016 för förbättring av informationsutbytet och informationshanteringen, inbegripet interoperabilitetslösningar på området för rättsliga och inrikes frågor, 9368/1/16 REV 1.

⁴⁷ Europaparlamentets resolution av den 6 juli 2016 om de strategiska prioriteringarna för kommissionens arbetsprogram 2017, [2016/2773 \(RSP\)](#).

informationen och gå i riktning mot interoperabilitet samt förslag om obligatoriskt informationsutbyte på EU-nivå åtföljda av de bestämmelser om dataskydd som krävs.

- (4) Vid Europeiska rådets möte den 15 december 2016⁴⁸ efterlystes fortsatta resultat i fråga om interoperabilitet mellan EU:s informationssystem och databaser.
- (5) Expertgruppen för informationssystem och interoperabilitet konstaterade i sin slutrapport av den 11 maj 2017⁴⁹ att det är nödvändigt och tekniskt genomförbart att eftersträva praktiska lösningar för interoperabilitet och att de i princip både kan ge operativa vinster och fastställas i överensstämmelse med dataskyddskraven.
- (6) Kommissionen presenterade i sitt meddelande *Sjunde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*⁵⁰ av den 16 maj 2017, i enlighet med sitt meddelande av den 6 april 2016 och resultaten och rekommendationerna från expertgruppen för informationssystem och interoperabilitet, en ny strategi för uppgiftshantering för gränser, säkerhet och migration där alla EU-informationssystem för säkerhet, gränsförvaltning och migrationshantering är interoperabla med full respekt för de grundläggande rättigheterna.
- (7) I rådets slutsatser av den 9 juni 2017⁵¹ om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabiliteten mellan EU-informationssystem uppmanades kommissionen att eftersträva lösningarna för interoperabilitet enligt expertgruppens förslag.
- (8) Europeiska rådet underströk den 23 juni 2017⁵² behovet av att förbättra interoperabiliteten mellan databaser och uppmanade kommissionen att så snart som möjligt utarbeta förslag till lagstiftning där förslagen från expertgruppen för informationssystem och interoperabilitet införlivas.
- (9) I syfte att förbättra förvaltningen av de yttre gränserna, bidra till att förebygga och bekämpa irreguljär migration och främja en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen – bland annat för att upprätthålla den allmänna säkerheten och allmänna ordningen och trygga säkerheten inom medlemsstaternas territorier – bör interoperabilitet inrättas mellan EU-informationssystemen, dvs. in- och utresesystemet, Informationssystemet för viseringar (VIS), [EU-systemet för reseuppgifter och resetillstånd (Etias)], Eurodac, Schengens informationssystem (SIS) och [det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN)] så att dessa EU-informationssystem och deras uppgifter kompletterar varandra. För att uppnå detta bör en europeisk sökportal (ESP), en gemensam biometrisk matchningstjänst, en gemensam databas för identitetsuppgifter (CIR) och en detektor för multipla identiteter (MID) inrättas som interoperabilitetskomponenter.
- (10) Interoperabiliteten mellan EU-informationssystem bör göra det möjligt för nämnda system att komplettera varandra för att underlätta korrekt identifiering av personer, bidra till att bekämpa identitetsbedrägeri, förbättra och harmonisera kvalitetskraven på uppgifterna i respektive EU-informationssystem, underlätta medlemsstaternas tekniska implementering och operativa drift av befintliga och framtida EU-informationssystem, stärka och förenkla de skyddsåtgärder för datasäkerhet och dataskydd som reglerar

⁴⁸ <http://www.consilium.europa.eu/sv/press/press-releases/2016/12/15/euco-conclusions-final/>.

⁴⁹ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.

⁵⁰ COM(2017) 261 final, 16.5.2017.

⁵¹ <http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf>.

⁵² [Slutsatser från Europeiska rådets möte](#) den 22–23 juni 2017.

respektive EU-informationssystem, rationalisera åtkomst i brottsbekämpningssyfte till in- och utresesystemet, VIS, [Etias] och Eurodac samt stödja syftena med in- och utresesystemet, VIS, [Etias], Eurodac, SIS och [Ecris-TCN-systemet].

- (11) Interoperabilitetskomponenterna bör omfatta in- och utresesystemet, VIS, [Etias], Eurodac, SIS och [Ecris-TCN-systemet]. De bör också omfatta Europoluppgifterna i den mån som krävs för att de ska kunna sökas samtidigt med dessa EU-informationssystem.
- (12) Interoperabilitetskomponenterna bör beröra personer vars personuppgifter får behandlas i EU-informationssystemen och av Europol, dvs. tredjelandsmedborgare vars personuppgifter behandlas i EU-informationssystemen och av Europol, samt EU-medborgare vars personuppgifter behandlas i SIS och av Europol.
- (13) Den europeiska sökportalen (ESP) bör inrättas för att tekniskt underlätta medlemsstaternas myndigheters och EU-organens möjligheter att få snabb, smidig, effektiv, systematisk och kontrollerad åtkomst till EU-informationssystem, Europoluppgifter och Interpols databaser så att de kan utföra sina uppgifter, i enlighet med deras åtkomsträttigheter, och för att stödja syftena med in- och utresesystemet, VIS, [Etias], Eurodac, SIS, [Ecris-TCN-systemet] och Europoluppgifterna. Den europeiska sökportalen möjliggör samtidiga parallella sökningar i alla relevanta EU-informationssystem, Europoluppgifter och Interpols databaser och bör fungera som en gemensam kontaktpunkt eller meddelandehanterare för att söka i olika centrala system och smidigt hämta den nödvändiga informationen, med full respekt för de underliggande systemens åtkomstkontroll och dataskyddskrav.
- (14) De ESP-slutanvändare som har åtkomsträtt till Europoluppgifter enligt Europaparlamentets och rådets förordning (EU) 2016/794⁵³ bör kunna göra sökningar i Europoluppgifter samtidigt med de EU-informationssystem som de har åtkomst till. All ytterligare behandling av uppgifter efter en sådan sökning bör ske i enlighet med förordning (EU) 2016/794, inklusive restriktioner om åtkomst eller användning som dataleverantören har fastställt.
- (15) Den europeiska sökportalen (ESP) bör utvecklas och konfigureras så att det inte går att använda datafält för sökningar som inte rör personer eller resehandlingar eller som inte finns i ett EU-informationssystem, i Europoluppgifter eller i Interpols databas.
- (16) För att säkerställa snabb och systematisk användning av alla EU-informationssystem bör den europeiska sökportalen (ESP) användas för att söka i den gemensamma databasen för identitetsuppgifter, in- och utresesystemet, VIS, [Etias], Eurodac och [Ecris-TCN-systemet]. Den nationella uppkopplingen till de olika EU-informationssystemen bör dock behållas som en teknisk reserv. ESP bör också användas av unionens organ för att göra sökningar i det centrala SIS i enlighet med deras åtkomsträttigheter och för att de ska kunna utföra sina uppgifter. ESP bör vara ytterligare ett sätt att söka i det centrala SIS, Europoluppgifter och Interpols system, som ett komplement till de befintliga särskilda gränssnitten.
- (17) Biometriska uppgifter, såsom fingeravtryck och ansiktsbilder, är unika och ger därför en mycket mer tillförlitlig identifiering av en person än alfanumeriska uppgifter. Den gemensamma biometriska matchningstjänsten bör vara ett tekniskt verktyg för att

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

stärka och underlätta arbetet för de relevanta EU-informationssystemen och de andra interoperabilitetskomponenterna. Huvudsyftet med den gemensamma biometriska matchningstjänsten bör vara att underlätta identifiering av en person som kan ha registrerats i olika databaser, genom att matcha biometriska uppgifter mellan olika system och genom att bygga på en unik teknisk komponent i stället för fem olika i vart och ett av de underliggande systemen. Den gemensamma biometriska matchningstjänsten bör främja säkerhet och ge fördelar i fråga om kostnader, underhåll och drift, tack vare att den grundar sig på en unik teknisk komponent i stället för olika komponenter i vart och ett av de underliggande systemen. Alla automatiska fingeravtrycksidentifieringssystem, även de som för närvarande används för Eurodac, VIS och SIS, använder biometriska mallar bestående av uppgifter som härrör från en särdragsextraktion från faktiska biometriska prov. Den gemensamma biometriska matchningstjänsten bör samla och lagra dessa biometriska mallar på ett enda ställe och därigenom underlätta jämförelser mellan systemen med biometriska uppgifter och möjliggöra stordriftsfördelar vid utveckling och underhåll av de centrala EU-systemen.

- (18) Biometriska uppgifter är känsliga personuppgifter. Denna förordning bör fastställa grunden och skyddsåtgärder för behandlingen av sådana uppgifter i syfte att entydigt identifiera de berörda personerna.
- (19) För att vara effektiva kräver de system som inrättats genom Europaparlamentets och rådets förordning (EU) 2017/2226⁵⁴, Europaparlamentets och rådets förordning (EG) nr 767/2008⁵⁵, [Etiasförordningen] för förvaltningen av unionens gränser, det system som inrättats genom [Eurodacförordningen] för att identifiera personer som ansöker om internationellt skydd och bekämpa irreguljär migration samt det system som inrättats genom [förordningen om Ecris-TCN-systemet] en korrekt identifiering av de tredjelandsmedborgare vars personuppgifter lagras i dem.
- (20) Den gemensamma databasen för identitetsuppgifter (CIR) bör därför underlätta och stödja en korrekt identifiering av personer som har registrerats i in- och utresesystemet, VIS, [Etias], Eurodac och [Ecris-TCN-systemet].
- (21) Personuppgifter som lagras i dessa EU-informationssystem kan avse samma personer men under olika eller ofullständiga identiteter. Medlemsstaterna förfogar över effektiva metoder att identifiera sina medborgare eller personer som är registrerade som varaktigt bosatta på deras territorium, men detsamma gäller inte för tredjelandsmedborgare. Interoperabiliteten mellan EU-informationssystem bör bidra till en korrekt identifiering av tredjelandsmedborgare. Den gemensamma databasen för identitetsuppgifter (CIR) bör lagra de personuppgifter om tredjelandsmedborgare i systemen vilka behövs för att göra det möjligt att mer korrekt identifiera dessa personer, därför även deras identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter, oavsett vilket system uppgifterna ursprungligen samlades in i. Endast de personuppgifter som är absolut nödvändiga för att utföra en korrekt identitetskontroll bör lagras i CIR. De personuppgifter som registreras i CIR bör inte behållas längre än vad som är absolut nödvändigt för de underliggande systemens syften och bör raderas

⁵⁴ Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) 1077/2011 (EUT L 327, 9.12.2017, s. 20).

⁵⁵ Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) (EUT L 218, 13.8.2008, s. 60).

automatiskt när uppgifterna har raderats i det underliggande systemet i enlighet med den logiska separeringen.

- (22) Den nya behandlingen, som består i lagring av sådana uppgifter i den gemensamma databasen för identitetsuppgifter (CIR) i stället för lagring i vart och ett av de separata systemen, krävs för att förbättra identifieringens korrekthet vilket möjliggörs av den automatiska jämförelsen och matchningen av sådana uppgifter. Det faktum att tredjelandsmedborgares personuppgifter och biometriska uppgifter lagras i CIR bör inte på något sätt hindra den behandling av uppgifter som avses i förordningarna om in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN-systemet, eftersom CIR är en ny gemensam komponent i dessa underliggande system.
- (23) I detta sammanhang är det nödvändigt att skapa en personakt i den gemensamma databasen för identitetsuppgifter (CIR) för varje person som har registrerats i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN-systemet, för att uppnå syftet med en korrekt identifiering av tredjelandsmedborgare inom Schengenområdet och för att stödja detektorn för multipla identiteter i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. Personakten bör lagras på ett enda ställe och ge vederbörligen bemyndigade slutanvändare åtkomst till alla möjliga identiteter som är länkade till en person.
- (24) Den gemensamma databasen för identitetsuppgifter (CIR) bör därigenom stödja detektorn för multipla identiteter i dess funktion och underlätta och rationalisera de brottsbekämpande myndigheternas åtkomst till de EU-informationssystem som inte har inrättats uteslutande i syfte att förebygga, utreda, upptäcka och lagföra grov brottslighet.
- (25) Den gemensamma databasen för identitetsuppgifter (CIR) bör tillhandahålla en gemensam lagringsplats för identitetsuppgifter och biometriska uppgifter om tredjelandsmedborgare som har registrerats i in- och utresesystemet, VIS, [Etias], Eurodac och [Ecris-TCN-systemet] samt fungera som en gemensam komponent mellan dessa system för att lagra dessa uppgifter och möjliggöra sökningar.
- (26) Alla uppgifter i den gemensamma databasen för identitetsuppgifter (CIR) bör separeras logiskt genom att varje uppgift automatiskt taggas med det underliggande system som äger den uppgiften. CIR:s åtkomstkontroll bör använda dessa taggar för att göra en uppgift åtkomlig eller ej.
- (27) För att säkerställa en korrekt identifiering av en person bör medlemsstaternas myndigheter som är behöriga att förebygga och bekämpa irreguljär migration och de behöriga myndigheter som avses i artikel 3.7 i direktiv 2016/680 ha rätt att söka i den gemensamma databasen för identitetsuppgifter (CIR) med de biometriska uppgifter som personen i fråga lämnar under en identitetskontroll.
- (28) Om personens biometriska uppgifter inte kan användas eller sökningen med dessa uppgifter misslyckas bör sökningen utföras med vederbörandes identitetsuppgifter i kombination med resehandlingsuppgifter. Om sökningen visar att det finns uppgifter om personen i den gemensamma databasen för identitetsuppgifter (CIR) bör medlemsstaternas myndigheter ha åtkomst att läsa de identitetsuppgifter som lagrats om personen i CIR, utan att det anges vilket EU-informationssystem uppgifterna tillhör.
- (29) Medlemsstaterna bör anta nationella lagstiftningsåtgärder för att utse de myndigheter som är behöriga att utföra identitetskontroller med hjälp av den gemensamma databasen för identitetsuppgifter (CIR) och fastställa förfarandena, villkoren och

kriterierna för sådana kontroller i enlighet med proportionalitetsprincipen. I synnerhet bör befogenheten för en anställd vid en sådan myndighet att ta biometriska uppgifter av en person under en identitetskontroll föreskrivas i nationell lagstiftning.

- (30) Genom denna förordning bör det också införas en ny möjlighet till rationaliserad åtkomst till andra uppgifter än identitetsuppgifter i in- och utresesystemet, VIS, [Etias] eller Eurodac för medlemsstaternas utsedda brottsbekämpande myndigheter och Europol. Andra uppgifter än identitetsuppgifter som finns i dessa system kan vara nödvändiga för att förebygga, upptäcka, utreda och lagföra terroristbrott eller grova brott i ett specifikt fall.
- (31) Fullständig åtkomst till de uppgifter som finns i EU-informationssystemen och som är nödvändiga för att förebygga, upptäcka och utreda terroristbrott eller andra grova brott, utöver de relevanta identitetsuppgifter som ingår i den gemensamma databasen för identitetsuppgifter (CIR) och som erhållits med hjälp av de biometriska uppgifter som tagits av personen i fråga under en identitetskontroll, bör även i fortsättningen regleras genom bestämmelserna i de respektive rättsliga instrumenten. De utsedda brottsbekämpande myndigheterna och Europol vet inte på förhand vilket EU-informationssystem som innehåller uppgifter om de personer de behöver göra sökningar om. Det här leder till förseningar och ineffektivitet när de ska utföra sina uppgifter. Den slutanvändare som har bemyndigats av den utsedda myndigheten bör därför ha rätt att se vilket EU-informationssystem de uppgifter som motsvarar sökningen är registrerade i. Det berörda systemet skulle på så vis flaggas efter den automatiska kontrollen att det finns en träff i systemet (en så kallad flaggfunktion för träff).
- (32) Loggarna över sökningarna i den gemensamma databasen för identitetsuppgifter bör visa syftet med sökningen. Om en sådan sökning har gjorts med tvåstegsstrategin för sökningar bör loggarna innehålla en referens till den nationella akten för utredningen eller ärendet, och därmed ange att sökningen gjordes för att förebygga, utreda och undersöka terroristbrott eller andra grova brott.
- (33) Den sökning i den gemensamma databasen för identitetsuppgifter (CIR) som görs av medlemsstaternas utsedda myndigheter och Europol för att få ett svar i form av en flagga som anger att uppgifterna finns i in- och utresesystemet, VIS, [Etias] eller Eurodac kräver automatiserad behandling av personuppgifter. En flagga vid träff skulle inte avslöja några personuppgifter om den berörda personen, utan endast en angivelse om att vissa uppgifter om vederbörande lagras i ett av systemen. Den bemyndigade slutanvändaren bör inte fatta några negativa beslut om den berörda personen endast utifrån det faktum att en sökning gett en flagga vid träff. Slut användarens åtkomst till en flagga vid träff skulle därför utgöra ett mycket begränsat ingrepp i den berörda personens rätt till skydd av personuppgifter, medan det skulle vara nödvändigt för att den utsedda myndigheten och Europol mer effektivt ska kunna rikta en begäran om åtkomst till personuppgifter direkt till det system som enligt flaggningen innehåller uppgifterna.
- (34) Tvåstegsstrategin för uppgiftssökning är särskilt värdefull i de fall då man inte känner till identiteten på den brottsmisstänkta, gärningsmannen eller det misstänkta offret för ett terroristbrott eller ett annat grovt brott. I dessa fall bör den gemensamma databasen för identitetsuppgifter (CIR) göra det möjligt att identifiera det informationssystem som har uppgifter om personen i en enda sökning. Genom att införa en skyldighet att använda denna nya strategi för åtkomst i brottsbekämpningssyfte i dessa fall bör åtkomsten till de personuppgifter som lagras i in- och utresesystemet, VIS, [Etias] och

Eurodac ske utan krav på att först göra en sökning i nationella databaser och inleda en sökning i andra medlemsstaters automatiska fingeravtrycksidentifieringssystem i enlighet med beslut 2008/615/RIF. Principen om en tidigare sökning begränsar i praktiken medlemsstaternas myndigheters möjligheter att söka i systemen för berättigade brottsbekämpande ändamål och kan således leda till att man går miste om möjligheter att upptäcka nödvändig information. Kraven på att först göra en sökning i nationella databaser och inleda en sökning i andra medlemsstaters automatiska fingeravtrycksidentifieringssystem i enlighet med beslut 2008/615/RIF bör upphöra att gälla först när den alternativa skyddsåtgärden med tvåstegsstrategin för åtkomst i brottsbekämpningssyfte genom CIR har tagits i bruk.

- (35) Detektorn för multipla identiteter (MID) bör inrättas för att stödja den gemensamma databasen för identitetsuppgifter i dess funktion och för att stödja syftena med in- och utresesystemet, VIS, [Etias], Eurodac, SIS och [Ecris-TCN-systemet]. För att effektivt uppfylla sina respektive syften kräver alla dessa EU-informationssystem en korrekt identifiering av de personer vars personuppgifter lagras i dem.
- (36) Möjligheten att uppnå syftena med EU-informationssystemen undergrävs av att myndigheterna för närvarande inte kan använda dessa system för att utföra en tillräckligt tillförlitlig verifiering av identiteten på de tredjelandmedborgare vars uppgifter lagras i olika system. Detta beror på att den uppsättning identitetsuppgifter som lagras i ett visst enskilt system kan vara falska, inkorrekta eller ofullständiga, och att det i dagsläget inte finns någon möjlighet att upptäcka sådana falska, inkorrekta eller ofullständiga identitetsuppgifter genom jämförelser med uppgifter som lagras i ett annat system. För att råda bot på denna situation är det nödvändigt att på unionsnivå ha ett tekniskt instrument som möjliggör en korrekt identifiering av tredjelandmedborgare för dessa ändamål.
- (37) Detektorn för multipla identiteter (MID) bör skapa och lagra länkar mellan uppgifter i de olika EU-informationssystemen för att spåra multipla identiteter, i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. MID bör endast innehålla länkar mellan personer som har registrerats i flera än ett EU-informationssystem, strikt begränsat till de uppgifter som krävs för att verifiera att en person har registrerats lagligen eller olagligen med olika biografiska identiteter i olika system eller för att klargöra att två personer med liknande biografiska uppgifter inte är samma person. Behandlingen av uppgifter i den europeiska sökportalen (ESP) och den gemensamma biometriska matchningstjänsten för att länka personakter mellan enskilda system bör hållas till ett absolut minimum och är således begränsad till spårning av multipla identiteter vid den tidpunkt då nya uppgifter läggs till i ett av de informationssystem som ingår i den gemensamma databasen för identitetsuppgifter och SIS. MID bör omfatta skyddsåtgärder mot potentiell diskriminering eller ogynnsamma beslut mot personer som lagligen har multipla identiteter.
- (38) I denna förordning föreskrivs ny uppgiftsbehandling som syftar till att korrekt identifiera de berörda personerna. Detta utgör ett ingrepp i deras grundläggande rättigheter som skyddas genom artiklarna 7 och 8 i EU:s stadga om de grundläggande rättigheterna. Eftersom EU-informationssystemen är beroende av att de berörda personerna identifieras korrekt för att fungera effektivt är detta ingrepp motiverat av samma syften som lett till att vart och ett av dessa system har inrättats, nämligen en effektiv förvaltning av unionens gränser, den inre säkerheten i unionen, ett effektivt genomförande av unionens asyl- och viseringspolitik samt kampen mot irreguljär migration.

- (39) Den europeiska sökportalen (ESP) och den gemensamma biometriska matchningstjänsten bör jämföra uppgifter i den gemensamma databasen för identitetsuppgifter (CIR) och SIS om personer när en nationell myndighet eller ett EU-organ skapar nya uppgifter. Dessa jämförelser bör göras automatiskt. CIR och SIS bör använda den gemensamma biometriska matchningstjänsten för att upptäcka möjliga länkar på grundval av biometriska uppgifter. CIR och SIS bör använda ESP för att upptäcka möjliga länkar på grundval av alfanumeriska uppgifter. CIR och SIS bör kunna identifiera identiska eller liknande uppgifter om tredjelandsmedborgare vilka är lagrade i flera system. När så är fallet bör en länk som anger att det är samma person skapas. CIR och SIS bör konfigureras på ett sätt som gör att små translittereringsfel eller stavfel upptäcks, så att det inte skapar omotiverade olägenheter för den berörda tredjelandsmedborgaren.
- (40) Den nationella myndighet eller det EU-organ som registrerade uppgifterna i respektive EU-informationssystem bör bekräfta eller ändra dessa länkar. Den myndigheten bör ha åtkomst till de uppgifter som lagras i den gemensamma databasen för identitetsuppgifter (CIR) eller SIS och i detektorn för multipla identiteter (MID) för manuell verifiering av identitet.
- (41) Åtkomsten till detektorn för multipla identiteter (MID) för medlemsstaternas myndigheter och EU-organ som har åtkomst till minst ett EU-informationssystem som omfattas av den gemensamma databasen för identitetsuppgifter (CIR) eller till SIS bör begränsas till så kallade röda länkar, som innebär att de länkade uppgifterna består av samma biometriska uppgifter men olika identitetsuppgifter och att den myndighet som ansvarar för verifiering av olika identiteter har konstaterat att samma person olagligen använder multipla identiteter, eller att de länkade uppgifterna består av liknande identitetsuppgifter och att den myndighet som ansvarar för verifiering av olika identiteter har konstaterat att samma person olagligen använder multipla identiteter. Om de länkade identitetsuppgifterna inte är liknande bör en gul länk skapas och en manuell verifiering göras för att bekräfta länken eller ändra färgen i enlighet med detta.
- (42) Den manuella verifieringen av multipla identiteter bör säkerställas av den myndighet som skapat eller uppdaterat de uppgifter som lett till en träff som ger upphov till en länk med uppgifter som redan finns lagrade i ett annat EU-informationssystem. Den myndighet som ansvarar för verifieringen av multipla identiteter bör bedöma om det finns multipla lagliga eller olagliga identiteter. En sådan bedömning bör om möjligt utföras i tredjelandsmedborgarens närvaro och vid behov genom att begära ytterligare klagöranden eller information. Bedömningen bör göras utan dröjsmål, i enlighet med de rättsliga kraven på korrekt information enligt unionsrätten och nationell lagstiftning.
- (43) För länkar till Schengens informationssystem (SIS) med registreringar avseende personer som är efterlysta för gripande för överlämnande eller utlämning, försvunna eller utsatta personer, personer som söks för att delta i ett rättsligt förfarande, personer som omfattas av diskreta kontroller eller särskilda kontroller eller okända efterlysta personer bör den myndighet som ansvarar för verifiering av multipla identiteter vara Sirenekontoret i den medlemsstat som har skapat registreringen. Dessa kategorier av SIS-registreringar är känsliga och bör inte nödvändigtvis delas med de myndigheter som skapar eller uppdaterar uppgifter i ett av de andra EU-informationssystemen. Skapandet av en länk med SIS-uppgifter bör inte påverka de åtgärder som ska vidtas i enlighet med [SIS-förordningarna].

- (44) Eu-LISA bör inrätta automatiserade mekanismer för kvalitetskontroll av uppgifter och gemensamma indikatorer för uppgiftskvalitet. Eu-LISA bör ansvara för att utveckla en central övervakningskapacitet för uppgiftskvalitet och regelbundet utarbeta dataanalysrapporter för att förbättra kontrollen av medlemsstaternas implementering och tillämpning av EU-informationssystemen. De gemensamma kvalitetsindikatorerna bör inbegripa minimikvalitetsstandarder för att lagra uppgifter i EU-informationssystemen eller interoperabilitetskomponenterna. Målet med sådana standarder för uppgiftskvalitet bör vara att EU-informationssystemen och interoperabilitetskomponenterna automatiskt ska kunna identifiera inmatade uppgifter som verkar vara inkorrekta eller inkonsekventa, så att ursprungsmedlemsstaten kan verifiera uppgifterna och vidta de korrigerande åtgärder som behövs.
- (45) Kommissionen bör utvärdera eu-LISA:s kvalitetsrapporter och utfärda rekommendationer till medlemsstaterna i tillämpliga fall. Medlemsstaterna bör ansvara för utarbetandet av en handlingsplan som beskriver åtgärder för att rätta till eventuella brister i uppgifternas kvalitet och bör regelbundet rapportera om framstegen.
- (46) Det universella meddelandeformatet (UMF) bör utgöra en standard för strukturerat, gränsöverskridande informationsutbyte mellan informationssystem, myndigheter och/eller organisationer på området rättsliga och inrikes frågor. UMF bör definiera en gemensam vokabulär och logiska strukturer för information som ofta utbyts, i syfte att underlätta interoperabilitet genom att möjliggöra skapande och läsning av utbyttets innehåll på ett konsekvent och semantiskt likvärdigt sätt.
- (47) En central databas för rapporter och statistik (CRRS) bör inrättas för att generera systemöverskridande statistiska uppgifter och analytisk rapportering för politiska och operativa skäl samt för uppgiftskvalitet. Eu-LISA bör inrätta, implementera och hysa CRRS i sina tekniska anläggningar som innehåller anonyma statistiska uppgifter från ovan nämnda system, den gemensamma databasen för identitetsuppgifter, detektorn för multipla identiteter och den gemensamma biometriska matchningstjänsten. Uppgifterna i CRRS bör inte möjliggöra identifiering av enskilda personer. Eu-LISA bör anonymisera uppgifterna och registrera de anonyma uppgifterna i CRRS. Anonymiseringsprocessen bör vara automatisk och eu-LISA:s personal bör inte beviljas direkt åtkomst till några personuppgifter som lagras i EU-informationssystemen eller i interoperabilitetskomponenterna.
- (48) Förordning (EU) 2016/679 bör tillämpas på de nationella myndigheternas behandling av personuppgifter inom ramen för denna förordning, förutom om behandlingen görs av medlemsstaternas utsedda myndigheter eller centrala kontaktpunkter i syfte att förebygga, upptäcka eller utreda terroristbrott eller andra grova brott, då Europaparlamentets och rådets direktiv (EU) 2016/680 bör tillämpas.
- (49) De särskilda bestämmelserna om dataskydd i [Eurodacförordningen], [förordningen om SIS på området brottsbekämpning], [förordningen om SIS på området återvändande] och [förordningen om Ecris-TCN-systemet] bör tillämpas på behandlingen av personuppgifter i respektive system.
- (50) Europaparlamentets och rådets förordning (EG) nr 45/2001⁵⁶ bör tillämpas på behandling av personuppgifter som utförs av eu-LISA och unionens andra institutioner och organ när de utför sina skyldigheter enligt denna förordning, utan att det påverkar

⁵⁶ 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).

tillämpningen av förordning (EU) 2016/794, som bör tillämpas på Europols behandling av personuppgifter.

- (51) De nationella tillsynsmyndigheter som har inrättats i enlighet med [förordning (EU) 2016/679] bör övervaka att medlemsstaternas behandling av personuppgifter är laglig, medan den europeiska datatillsynsmannen, som inrättades genom förordning (EG) nr 45/2001, bör övervaka unionsinstitutionernas och unionsorganens behandling av personuppgifter. Europeiska datatillsynsmannen och tillsynsmyndigheterna bör samarbeta kring övervakningen av interoperabilitetskomponenternas behandling av personuppgifter.
- (52) ”(...) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den ...”.
- (53) 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.
- (54) Både medlemsstaterna och eu-LISA bör ha säkerhetsplaner för att underlätta genomförandet av säkerhetsskyldigheterna och bör samarbeta med varandra för att hantera säkerhetsproblem. Eu-LISA bör också se till att man fortlöpande utnyttjar den senaste tekniska utvecklingen för att säkerställa dataintegritet i fråga om utveckling, utformning och förvaltning av interoperabilitetskomponenterna.
- (55) För att stödja syftena med statistik och rapportering är det nödvändigt att bevilja bemyndigad personal vid de behöriga myndigheter, institutioner och organ som anges i denna förordning åtkomst till vissa uppgifter som rör vissa interoperabilitetskomponenter utan att möjliggöra individuell identifiering.
- (56) För att de behöriga myndigheterna och EU-organen ska kunna anpassa sig till de nya kraven på att använda den europeiska sökportalen (ESP) är det nödvändigt att föreskriva en övergångsperiod. Likaledes bör övergångsåtgärder fastställas för driftsättningen av detektorn för multipla identiteter (MID) för att den ska fungera konsekvent och optimalt.
- (57) De kostnader som avsatts för utveckling av interoperabilitetskomponenterna i den nuvarande fleråriga budgetramen är lägre än det återstående beloppet av den budget som öronmärkts för smarta gränser i Europaparlamentets och rådets förordning (EU) nr 515/2014⁵⁷. Genom denna förordning bör man således, i enlighet med artikel 5.5 b i förordning (EU) nr 515/2014, omfördela det belopp som för närvarande anslagits till utveckling av it-system som stöd för hanteringen av migrationsströmmar över de yttre gränserna.
- (58) För att komplettera vissa detaljerade tekniska aspekter i denna förordning bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt delegeras till kommissionen med avseende på användarprofiler i den europeiska sökportalen (ESP) och ESP-svarens innehåll och format. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april

⁵⁷ 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 och om upphävande av beslut nr 574/2007/EG (EUT L 150, 20.5.2014, s. 143).

2016⁵⁸. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter bör Europaparlamentet och rådet erhålla alla handlingar samtidigt som medlemsstaternas experter, och deras experter bör ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

- (59) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter att anta närmare bestämmelser om mekanismer, förfaranden och indikatorer för automatiserad kontroll av uppgiftskvalitet, utveckling av UMF-standarderna, förfaranden för fastställande av likheten mellan identiteter, driften av den centrala databasen för rapporter och statistik och samarbetsförfarandet i händelse av säkerhetsincidenter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011⁵⁹.
- (60) Förordning 2016/794 ska gälla all behandling av Europoluppgifter vid tillämpningen av denna förordning.
- (61) Denna förordning påverkar inte tillämpningen av direktiv 2004/38/EG.
- (62) I enlighet med artikel 3 i avtalet mellan Europeiska gemenskapen och Konungariket Danmark om kriterier och mekanismer för att avgöra vilken medlemsstat som har ansvaret för att pröva en asylansökan som en medborgare i tredjeland har gett in i Danmark eller någon annan medlemsstat i Europeiska unionen, och om Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av Dublinkonventionen⁶⁰, ska Danmark meddela kommissionen om huruvida landet kommer att genomföra innehållet i denna förordning i den utsträckning som den rör Eurodac [och det automatiska system för registrering, övervakning och tilldelningsmekanismen för ansökningar om internationellt skydd vilket avses i artikel 44 i förordning (EU) XX/XX om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat (omarbetning)].
- (63) I den utsträckning som dess bestämmelser rör SIS, så som systemet regleras i beslut 2007/533/RIF, deltar Förenade kungariket i denna förordning i enlighet med artikel 5.1 i protokoll nr 19 om Schengenregelverket införlivat inom Europeiska unionens ramar, fogat till EU-fördraget och EUF-fördraget (protokollet om Schengenregelverket), 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 Schengenregelverket⁶¹. I enlighet med artikel 3 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och till EUF-fördraget (protokollet om Förenade kungarikets och Irlands ställning) får Förenade kungariket meddela rådets ordförande att landet önskar delta i antagandet och tillämpningen av denna förordning, i den utsträckning som dess bestämmelser rör Eurodac [och det automatiska system för registrering, övervakning och tilldelningsmekanismen för ansökningar om internationellt skydd vilket avses i artikel 44 i förordning (EU) XX/XX om kriterier och mekanismer för att avgöra vilken medlemsstat som är

⁵⁸ http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

⁵⁹ 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).

⁶⁰

⁶¹

ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat (omarbetning)]. I enlighet med artiklarna 1, 2 och 4a.1 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, deltar Förenade kungariket inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Förenade kungariket, i den utsträckning som dess bestämmelser rör [Ecris-TCN-systemet]. I enlighet med artiklarna 3 och 4a.1 i protokoll nr 21 får Förenade kungariket meddela att landet önskar delta i antagandet av denna förordning.

- (64) I den utsträckning som dess bestämmelser rör SIS, så som systemet regleras i beslut 2007/533/RIF, deltar Irland i denna förordning i enlighet med artikel 5.1 i protokoll nr 19 om Schengenregelverket införlivat inom Europeiska unionens ramar, fogat till EU-fördraget och EUF-fördraget (protokollet om Schengenregelverket), 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 Schengenregelverket⁶². I enlighet med artikel 3 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och till EUF-fördraget (protokollet om Förenade kungarikets och Irlands ställning) får Irland meddela rådets ordförande att landet önskar delta i antagandet och tillämpningen av denna förordning, i den utsträckning som dess bestämmelser rör Eurodac [och det automatiska system för registrering, övervakning och tilldelningsmekanismen för ansökningar om internationellt skydd vilket avses i artikel 44 i förordning (EU) XX/XX om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat (omarbetning)]. I enlighet med artiklarna 1, 2 och 4a.1 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, deltar Irland inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Irland, i den utsträckning som dess bestämmelser rör [Ecris-TCN-systemet]. I enlighet med artiklarna 3 och 4a.1 i protokoll nr 21 får Irland meddela att landet önskar delta i antagandet av denna förordning.
- (65) När det gäller Island och Norge i förhållande till Eurodac [och det automatiska system för registrering, övervakning och tilldelningsmekanismen för ansökningar om internationellt skydd vilket avses i artikel 44 i förordning (EU) XX/XX om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat (omarbetning)] innebär denna förordning en ny åtgärd i den mening som avses i avtalet mellan Europeiska gemenskapen och Republiken Island och Konungariket Norge om kriterier och mekanismer för att fastställa vilken stat som skall ansvara för handläggningen av en asylansökan som görs i en medlemsstat eller i Island eller Norge.
- (66) När det gäller Schweiz i förhållande till Eurodac [och det automatiska system för registrering, övervakning och tilldelningsmekanismen för ansökningar om internationellt skydd vilket avses i artikel 44 i förordning (EU) XX/XX om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös

62

person har lämnat in i någon medlemsstat (omarbetning)] innebär denna förordning en ny åtgärd rörande Eurodac i den mening som avses i avtalet mellan Europeiska gemenskapen och Schweiziska edsförbundet om kriterier och mekanismer för att fastställa vilken stat som ska ansvara för handläggningen av en asylansökan som görs i en medlemsstat eller i Schweiz.

- (67) När det gäller Liechtenstein i förhållande till Eurodac [och det automatiska system för registrering, övervakning och tilldelningsmekanismen för ansökningar om internationellt skydd vilket avses i artikel 44 i förordning (EU) XX/XX om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat (omarbetning)] innebär denna förordning en ny åtgärd i den mening som avses i protokollet mellan Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska gemenskapen och Schweiziska edsförbundet om kriterier och mekanismer för att fastställa vilken stat som ska ansvara för handläggningen av en asylansökan som görs i en medlemsstat eller i Schweiz.
- (68) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns i synnerhet i Europeiska unionens stadga om de grundläggande rättigheterna, och ska tillämpas i enlighet med dessa rättigheter och principer.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1 *Syfte*

1. Genom denna förordning tillsammans med [förordning 2018/xx om interoperabilitet för gränser och viseringar] inrättas en ram för att säkerställa interoperabilitet mellan in- och utresesystemet, Informationssystemet för viseringar (VIS), [EU-systemet för reseuppgifter och resetillstånd (Etias)], Eurodac, Schengens informationssystem (SIS) och [Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN-systemet)] så att dessa system och data ska komplettera varandra.
2. Denna ram ska omfatta följande interoperabilitetskomponenter:
 - (a) En europeisk sökportal.
 - (b) En gemensam biometrisk matchningstjänst.
 - (c) En gemensam databas för identitetsuppgifter (CIR).
 - (d) En detektor för multipla identiteter.
3. Denna förordning innehåller också bestämmelser om kraven på uppgifternas kvalitet, ett universellt meddelandeformat (UMF), en central databas för rapporter och statistik och om ansvarsområden för medlemsstaterna och Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA) vad gäller utformningen och driften av interoperabilitetskomponenterna.

4. Genom denna förordning anpassas också förfarandena och villkoren för att medlemsstaternas brottsbekämpande myndigheter och Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) ska få åtkomst till in- och utresesystemet, Informationssystemet för viseringar (VIS), [EU-systemet för reseuppgifter och resetillstånd (Etias)] och Eurodac i syfte att förhindra, upptäcka och utreda terroristbrott eller andra grova brott som omfattas av deras behörighet.

Artikel 2

Målen med interoperabilitet

1. Genom att denna förordning säkerställer interoperabilitet ska den ha följande mål:
 - (a) Förbättra förvaltningen av de yttre gränserna.
 - (b) Bidra till att förebygga och bekämpa irreguljär migration.
 - (c) Bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, bland annat genom att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier.
 - (d) Förbättra genomförandet av den gemensamma viseringspolitiken. .
 - (e) Bistå vid prövningen av en ansökan om internationellt skydd.
2. Målen med att säkerställa interoperabilitet ska uppnås på följande sätt:
 - (a) Säkerställa en korrekt identifiering av personer.
 - (b) Bidra till kampen mot identitetsbedrägerier.
 - (c) Förbättra och harmonisera kraven på uppgiftskvalitet för respektive EU-informationssystem.
 - (d) Underlätta medlemsstaternas tekniska implementering och operativa drift av befintliga och framtida EU-informationssystem.
 - (e) Stärka, förenkla och göra de villkor för datasäkerhet och dataskydd som reglerar respektive EU-informationssystem mer enhetliga.
 - (f) Rationalisera villkoren för brottsbekämpande myndigheters åtkomst till in- och utresesystemet, VIS, [Etias] och Eurodac.
 - (g) Stödja syftena med in- och utresesystemet, VIS, [Etias], Eurodac, SIS och [Ecris-TCN-systemet].

Artikel 3

Tillämpningsområde

1. Denna förordning ska tillämpas på Eurodac, Schengens informationssystem (SIS) och [Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN-systemet)].
2. Denna förordning ska också tillämpas på Europoluppgifter i den utsträckning det ska vara möjligt att söka i dem samtidigt som i de EU-informationssystem som avses i punkt 1 i enlighet med unionsrätten.
3. Denna förordning ska tillämpas på personer vilkas personuppgifter får behandlas i de EU-informationssystem som avses i punkt 1 och i de Europoluppgifter som avses i punkt 2.

Artikel 4 *Definitioner*

I denna förordning gäller följande definitioner:

- (1) *yttre gränser*: yttre gränser enligt definitionen i artikel 2.2 i förordning (EU) 2016/399.
- (2) *in- och utresekontroller*: in- och utresekontroller enligt definitionen i artikel 2.11 i förordning (EU) 2016/399.
- (3) *gränsmyndighet*: den gränskontrolltjänsteman som i enlighet med nationell rätt tilldelats uppgiften att genomföra in- och utresekontroller.
- (4) *tillsynsmyndigheter*: den tillsynsmyndighet som inrättats i enlighet med artikel 51.1 i förordning (EU) 2016/679 och den tillsynsmyndighet som inrättats i enlighet med artikel 41.1 i direktiv (EU) 2016/680.
- (5) *verifiering*: förfarandet att jämföra en uppsättning uppgifter med en annan för att fastställa om en påstådd identitet är riktig ("one-to-one-check").
- (6) *identifiering*: förfarandet att fastställa en persons identitet genom en databassökning mot flera grupper av uppgifter ("one-to-many-check").
- (7) *tredjelandsmedborgare*: en person som inte är unionsmedborgare i den mening som avses i artikel 20.1 i fördraget, eller en statslös person eller en person vars medborgarskap är okänt.
- (8) *alfanumeriska uppgifter*: uppgifter som återges med bokstäver, siffror, specialtecken, mellanslag och skiljetecken.
- (9) *identitetsuppgifter*: de uppgifter som avses i artikel 27.3 a–h.
- (10) *fingeravtrycksuppgifter*: uppgifter om en persons fingeravtryck.
- (11) *ansiktsbild*: digitala bilder av ansiktet.
- (12) *biometriska uppgifter*: uppgifter om fingeravtryck och/eller ansiktsbild.
- (13) *biometrisk mall*: en matematisk representation som erhålls genom särdragsextraktion från biometriska uppgifter och som är begränsad till de egenskaper som är nödvändiga för att utföra identifikationer och verifieringar.
- (14) *resehandling*: pass eller motsvarande handling som ger innehavaren rätt att passera de yttre gränserna och i vilken en visering kan föras in.
- (15) *resehandlingsuppgifter*: resehandlingens typ, nummer och utfärdandeland samt sista giltighetsdag och koden på tre bokstäver för det land som utfärdat resehandlingen.
- (16) *resetillstånd*: ett resetillstånd enligt definitionen i artikel 3 i [Etiasförordningen].
- (17) *visering för kortare vistelse*: en visering enligt definitionen i artikel 2.2 a i förordning (EG) nr 810/2009.
- (18) *EU-informationssystem*: de stora it-system som förvaltas av eu-LISA.
- (19) *Europoluppgifter*: de personuppgifter som tillhandahålls Europol för det syfte som avses i artikel 18.2 a i förordning (EU) 2016/794.

- (20) *Interpols databaser*: Interpols databas över stulna och förkomna resehandlingar och Interpols databas för resehandlingar som är föremål för ett meddelande.
- (21) *matchning*: förekomsten av en motsvarighet som fastställts genom att jämföra två eller flera förekomster av personuppgifter som har registrerats eller är i färd att registreras i ett informationssystem eller en databas.
- (22) *träff*: bekräftelse av en matchning eller flera matchningar.
- (23) *polismyndighet*: behörig myndighet enligt definitionen i artikel 3.7 i direktiv 2016/680.
- (24) *utsedda myndigheter*: medlemsstaternas utsedda myndigheter som avses i artikel 29.1 i förordning (EU) 2017/2226, artikel 3.1 i rådets beslut 2008/633/RIF, [artikel 43 i Etiasförordningen] och [artikel 6 i Eurodacförordningen].
- (25) *terroristbrott*: ett brott enligt nationell rätt som motsvarar eller är likvärdigt med ett av de brott som avses i direktiv (EU) 2017/541.
- (26) *grovt brott*: ett brott som motsvarar eller är likvärdigt med ett av de brott som avses i artikel 2.2 i rambeslut 2002/584/RIF om det enligt nationell rätt kan leda till fängelse eller annan frihetsberövande åtgärd under en maximal tidsperiod på minst tre år.
- (27) *in- och utresesystemet*: det in- och utresesystem som avses i förordning (EU) 2017/2226.
- (28) *VIS*: Informationssystemet för viseringar som avses i förordning (EG) nr 767/2008.
- (29) [*Etias*: EU-systemet för reseuppgifter och resetillstånd som avses i Etiasförordningen].
- (30) *Eurodac*: Eurodac som avses i [Eurodacförordningen].
- (31) *SIS*: Schengens informationssystem som avses i [förordningen om SIS på området in- och utresekontroller, förordningen om SIS på området brottsbekämpning och förordningen om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna].
- (32) [*Ecris-TCN-systemet*: Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare och statslösa personer vilket avses i förordningen om Ecris-TCN-systemet].
- (33) *den europeiska sökportalen*: den europeiska sökportal som avses i artikel 6.
- (34) *den gemensamma biometriska matchningstjänsten*: den delade biometriska matchningstjänst som avses i artikel 15.
- (35) *CIR*: den gemensamma databas för identitetsuppgifter som avses i artikel 17.
- (36) *MID*: den detektor för multipla identiteter som avses i artikel 25.
- (37) *CRRS*: den centrala databas för rapporter och statistik som avses i artikel 39.

Artikel 5
Icke-diskriminering

Behandling av personuppgifter enligt denna förordning får inte leda till diskriminering av personer på någon grund, varken kön, ras eller etniskt ursprung, religion eller övertygelse, funktionsnedsättning, ålder eller sexuell läggning. Den ska ske med fullständig respekt för mänsklig värdighet och integritet. Särskild hänsyn ska tas till barn, äldre och personer med funktionsnedsättning.

KAPITEL II
Den europeiska sökportalen

Artikel 6
Den europeiska sökportalen

1. Det ska inrättas en europeisk sökportal för att säkerställa att medlemsstaternas myndigheter och EU:s organ har snabb, kontinuerlig, effektiv, systematisk och kontrollerad åtkomst till de EU-informationssystem, Europoluppgifter och Interpols databaser som krävs för att de ska kunna utföra sina uppgifter i enlighet med sina åtkomsträttigheter och för att stödja målen för in- och utresesystemet, VIS, [Etias], Eurodac, SIS [Ecris-TCN-systemet] och Europoluppgifterna.
2. Den europeiska sökportalen ska bestå av följande:
 - (a) En central infrastruktur, inbegripet en sökportal som gör det möjligt att samtidigt söka i in- och utresesystemet, VIS, [Etias], Eurodac, SIS, [Ecris-TCN-systemet] samt i Europoluppgifter och Interpols databaser.
 - (b) En säker kommunikationskanal mellan den europeiska sökportalen, medlemsstaterna och de EU-organ som har rätt att använda sökportalen i enlighet med unionsrätten.
 - (c) En säker kommunikationsinfrastruktur mellan den europeiska sökportalen och in- och utresesystemet, VIS, [Etias], Eurodac, det centrala SIS, [Ecris-TCN-systemet], Europoluppgifter och Interpols databaser samt mellan den europeiska sökportalen och de centrala infrastrukturerna för den gemensamma databasen för identitetsuppgifter (CIR) och detektorn för multipla identiteter.
3. Eu-LISA ska utveckla den europeiska sökportalen och säkerställa den tekniska förvaltningen.

Artikel 7
Användning av den europeiska sökportalen

1. Användningen av den europeiska sökportalen ska begränsas till de myndigheter i medlemsstaterna och de EU-organ som har åtkomst till in- och utresesystemet, [Etias], VIS, SIS, Eurodac och [Ecris-TCN-systemet], CIR och detektorn för multipla identiteter samt Europoluppgifter och Interpols databaser i enlighet med unionsrätten eller nationell lagstiftning avseende sådan åtkomst.
2. De myndigheter som avses i punkt 1 ska använda den europeiska sökportalen för att söka på uppgifter om personer eller deras resehandlingar i Eurodacs och [Ecris-TCN-systemets] centrala system i enlighet med sina åtkomsträttigheter enligt unionsrätten

och nationell lagstiftning. De ska också använda den europeiska sökportalen för att söka i CIR i enlighet med sina åtkomsträttigheter enligt denna förordning för de syften som avses i artiklarna 20, 21 och 22.

3. De myndigheter i medlemsstaterna som avses i punkt 1 får använda den europeiska sökportalen för att söka på uppgifter om personer eller deras resehandlingar i det centrala SIS som avses i [förordningen om SIS på området in- och utresekontroller och i förordningen om SIS på området brottsbekämpning]. Åtkomst till det centrala SIS via den europeiska sökportalen ska inrättas genom det nationella systemet (N.SIS) i varje medlemsstat i enlighet med [artikel 4.2 i förordningen om SIS på området in- och utresekontroller och i förordningen om SIS på området brottsbekämpning].
4. EU:s organ ska använda den europeiska sökportalen för att söka på uppgifter om personer eller deras resehandlingar i det centrala SIS.
5. De myndigheter som avses i punkt 1 får använda den europeiska sökportalen för att söka på uppgifter om personer eller deras resehandlingar i Europoluppgifter i enlighet med sina åtkomsträttigheter enligt unionsrätten och nationell lagstiftning.

Artikel 8

Profiler för användarna av den europeiska sökportalen

1. För att det ska vara möjligt att använda den europeiska sökportalen ska eu-LISA skapa en profil för varje kategori av sökportalens användare i enlighet med de tekniska detaljer och åtkomsträttigheter som avses i punkt 2, däribland följande, i enlighet med unionsrätten och nationell lagstiftning:
 - (a) De uppgiftsfält som ska användas vid sökningar.
 - (b) De EU-informationssystem, Europoluppgifter och Interpols databaser som ska och får konsulteras och som ska tillhandahålla användaren ett svar. .
 - (c) De uppgifter som tillhandahålls i varje svar.
2. Kommissionen ska anta delegerade akter i enlighet med artikel 63 för att närmare ange de tekniska detaljerna för de profiler som avses i punkt 1 för de användare av den europeiska sökportalen vilka avses i artikel 7.1 i enlighet med deras åtkomsträttigheter.

Artikel 9

Sökningar

1. Den europeiska sökportalens användare ska inleda en sökning genom att mata in uppgifter i sökportalen i enlighet med sin användarprofil och sina åtkomsträttigheter. När en sökning har inletts ska den europeiska sökportalen, med hjälp av de uppgifter som matats in av sökportalens användare, söka samtidigt i in- och utresesystemet, [Etias], VIS, SIS, Eurodac, [Ecris-TCN-systemet] och CIR samt i Europoluppgifter och Interpols databaser.
2. De uppgiftsfält som används för att inleda en sökning via den europeiska sökportalen ska motsvara de uppgiftsfält om personer eller resehandlingar som kan användas för att söka i de olika EU-informationssystemen, Europoluppgifter och Interpols databaser i enlighet med de rättsakter genom vilka de regleras.

3. Eu-LISA ska ta fram ett dokument för gränssnittskontroll för den europeiska sökportalen på grundval av det universella meddelandeformat som avses i artikel 38.
4. In- och utresesystemet, [Etias], VIS, SIS, Eurodac, [Ecris-TCN-systemet], CIR och detektorn för multipla identiteter samt Europoluppgifter och Interpols databaser ska tillhandahålla de uppgifter som de innehåller som ett resultat av sökningen i den europeiska sökportalen.
5. Vid en sökning i Interpols databaser ska utformningen av den europeiska sökportalen säkerställa att de uppgifter som används av sökportalens användare för att inleda en sökning inte delas med ägarna av Interpols uppgifter.
6. Svaret till användaren av den europeiska sökportalen ska vara unikt och ska innehålla alla de uppgifter som användaren har åtkomst till enligt unionsrätten. Svaret från den europeiska sökportalen ska vid behov ange vilket informationssystem eller vilken databas som uppgifterna tillhör.
7. Kommissionen ska anta en delegerad akt i enlighet med artikel 63 för att specificera innehållet i och formatet för svaren från den europeiska sökportalen.

Artikel 10 *Registerföring av loggar*

1. Utan att det påverkar tillämpningen av [artikel 39 i Eurodacförordningen], [artiklarna 12 och 18 i förordningen om SIS på området brottsbekämpning], [artikel 29 i ECRIS-TCN-förordningen] och artikel 40 i förordning (EU) 2016/794, ska eu-LISA föra logg över all uppgiftsbehandling inom den europeiska sökportalen. Dessa loggar ska särskilt innehålla följande:
 - (a) Myndighet i medlemsstaten och den enskilda användaren av den europeiska sökportalen, inklusive den profil för sökportalen som används och som avses i artikel 8.
 - (b) Datum och tidpunkt för sökningen.
 - (c) De EU-informationssystem och Europoluppgifter som varit föremål för sökning.
 - (d) I enlighet med nationella regler eller med förordning (EU) 2016/794 eller, i tillämpliga fall, förordning (EU) 45/2001, beteckningen för den person som utförde sökningen.
2. Loggarna får endast användas för övervakning av dataskyddet, inbegripet för kontroll av om en sökning är tillåten och om uppgifter har behandlats på ett lagligt sätt samt för att säkerställa datasäkerhet i enlighet med artikel 42. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats, såvida de inte behövs för övervakningsförfaranden som redan har inletts.

Artikel 11 *Reservförfaranden om det är tekniskt omöjligt att använda den europeiska sökportalen*

1. Om det är tekniskt omöjligt att använda den europeiska sökportalen för att söka i ett eller flera av de EU-informationssystem som avses i artikel 9.1 eller i CIR, på grund av ett fel i den europeiska sökportalen, ska sökportalens användare underrättas av eu-LISA.

2. Om det är tekniskt omöjligt att använda den europeiska sökportalen för att söka i ett eller flera av de EU-informationssystem som avses i artikel 9.1 eller i CIR, på grund av ett fel i en medlemsstats nationella infrastruktur, ska medlemsstatens behöriga myndighet underrätta eu-LISA och kommissionen.
3. I båda scenarierna och till dess att det tekniska felet har åtgärdats ska den skyldighet som avses i artikel 7.2 och 7.4 inte tillämpas och medlemsstaterna får ha direkt åtkomst till de informationssystem som avses i artikel 9.1 eller till CIR med hjälp av sina respektive nationella enhetliga gränssnitt eller nationella kommunikationsinfrastrukturer.

KAPITEL III

En gemensam biometrisk matchningstjänst

Artikel 12

En gemensam biometrisk matchningstjänst

1. Det ska inrättas en gemensam biometrisk matchningstjänst för lagring av biometriska mallar och möjliggörande av sökningar med biometriska uppgifter i flera EU-informationssystem för att stödja CIR och detektorn för multipla identiteter och målen för in- och utresesystemet, VIS, Eurodac, SIS och [Ecris-TCN-systemet].
2. Den gemensamma biometriska matchningstjänsten ska bestå av följande:
 - (a) En central infrastruktur som omfattar en sökmotor och lagring av de uppgifter som avses i artikel 13.
 - (b) En säker kommunikationsinfrastruktur mellan den gemensamma biometriska matchningstjänsten, det centrala SIS och CIR.
3. Eu-LISA ska utveckla den gemensamma biometriska matchningstjänsten och säkerställa den tekniska förvaltningen.

Artikel 13

Uppgifter som lagras i den gemensamma biometriska matchningstjänsten

1. Den gemensamma biometriska matchningstjänsten ska lagra de biometriska mallar som den ska få från följande biometriska uppgifter:
 - (a) De uppgifter som avses i artikel 16.1 d och artikel 17.1 b och c i förordning (EU) 2017/2226.
 - (b) De uppgifter som avses i artikel 9.6 i förordning (EG) nr 767/2008.
 - (c) [De uppgifter som avses i artikel 20.2 w och x i förordningen om SIS på området in- och utresekontroller.
 - (d) De uppgifter som avses i artikel 20.3 w och x i förordningen om SIS på området brottsbekämpning.
 - (e) De uppgifter som avses i artikel 4.3 t och u i förordningen om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna.]
 - (f) [De uppgifter som avses i artikel 13 a i Eurodacförordningen.]
 - (g) [De uppgifter som avses i artikel 5.1 b och artikel 5.2 i Ecris-TCN-förordningen.]

2. Varje biometrisk mall i den gemensamma biometriska matchningstjänsten ska innehålla en hänvisning till de informationssystem där motsvarande biometriska uppgifter lagras.
3. Biometriska mallar ska endast registreras i den gemensamma biometriska matchningstjänsten efter en automatisk kvalitetskontroll av de biometriska uppgifter som läggs in i ett av informationssystemen vilken utförs av den gemensamma biometriska matchningstjänsten för att säkerställa att en minimistandard för uppgifternas kvalitet uppfylls.
4. Lagringen av de uppgifter som avses i punkt 1 ska uppfylla de kvalitetsstandarder som avses i artikel 37.2.

Artikel 14

Sökning på biometriska uppgifter med den gemensamma biometriska matchningstjänsten

För att söka på de biometriska uppgifter som lagrats i den gemensamma databasen för personuppgifter och SIS ska CIR och SIS använda de biometriska mallar som lagrats i den gemensamma biometriska matchningstjänsten. Sökningar med biometriska uppgifter ska äga rum i enlighet med de syften som anges i denna förordning och i förordningen om in- och utresesystemet, VIS-förordningen, Eurodacförordningen, [SIS-förordningarna] och [Ecris-TCN-förordningen].

Artikel 15

Lagring av uppgifter i den gemensamma biometriska matchningstjänsten

De uppgifter som avses i artikel 13 ska lagras i den gemensamma biometriska matchningstjänsten under den tid som motsvarande biometriska uppgifter lagras i CIR eller SIS.

Artikel 16

Registerföring av loggar

1. Utan att det påverkar tillämpningen av [artikel 39 i Eurodacförordningen], [artiklarna 12 och 18 i förordningen om SIS på området brottsbekämpning] och [artikel 29 i Ecris-TCN-förordningen] ska eu-LISA föra logg över all uppgiftsbehandling inom den gemensamma biometriska matchningstjänsten. Dessa loggar ska särskilt omfatta följande:
 - (a) Historiken i samband med skapandet och lagringen av biometriska mallar.
 - (b) En hänvisning till de EU-informationssystem som varit föremål för sökning med de biometriska mallar som lagrats i den gemensamma biometriska matchningstjänsten.
 - (c) Datum och tidpunkt för sökningen.
 - (d) Den typ av biometriska uppgifter som används för att inleda sökningen.
 - (e) Längden på sökningen.
 - (f) Resultaten av sökningen och datum och tidpunkt för resultatet.
 - (g) I enlighet med nationella regler eller med förordning (EU) 2016/794 eller, i tillämpliga fall, förordning (EU) 45/2001, beteckningen för den person som utförde sökningen.

2. Loggarna får endast användas för övervakning av dataskyddet, inbegripet för kontroll av om en sökning är tillåten och om uppgifter har behandlats på ett lagligt sätt samt för att säkerställa datasäkerhet i enlighet med artikel 42. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats, såvida de inte behövs för övervakningsförfaranden som redan har inletts. De loggar som avses i punkt 1 a ska raderas så snart uppgifterna har raderats.

KAPITEL IV

En gemensam databas för identitetsuppgifter

Artikel 17

En gemensam databas för identitetsuppgifter

1. Det ska inrättas en gemensam databas för identitetsuppgifter (CIR) varigenom det skapas en personakt för varje person som är registrerad i in- och utresesystemet, VIS, [Etias], Eurodac eller [Ecris-TCN-systemet] och som innehåller de uppgifter som avses i artikel 18, för att underlätta och bistå vid en korrekt identifiering av personer som är registrerade i in- och utresesystemet, VIS, [Etias], Eurodac och [Ecris-TCN-systemet], stödja funktionen av detektorn för multipla identiteter och underlätta och rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning på EU-nivå, om det är nödvändigt för att förebygga, utreda, upptäcka eller lagföra grov brottslighet.
2. CIR ska bestå av följande:
 - (a) En central infrastruktur som ska ersätta de centrala systemen för in- och utresesystemet, VIS, [Etias], Eurodac respektive [Ecris-TCN-systemet] i den mån den ska lagra de uppgifter som avses i artikel 18.
 - (b) En säker kommunikationskanal mellan CIR, medlemsstaterna och de EU-organ som har rätt att använda den europeiska sökportalen i enlighet med unionsrätten.
 - (c) En säker kommunikationsinfrastruktur mellan CIR och in- och utresesystemet, [Etias], VIS, Eurodac och [Ecris-TCN-systemet] samt de centrala infrastrukturerna för den europeiska sökportalen, den gemensamma biometriska matchningstjänsten och detektorn för multipla identiteter.
3. Eu-LISA ska utveckla CIR och säkerställa den tekniska förvaltningen.

Artikel 18

Uppgifter i den gemensamma databasen för identitetsuppgifter

1. CIR ska lagra följande uppgifter, logiskt åtskilda, enligt det informationssystem från vilket uppgifterna härrör:
 - (a) – (ej tillämpligt)
 - (b) – (ej tillämpligt)
 - (c) – (ej tillämpligt)
 - (d) [De uppgifter som avses i artikel 13 a–e, 13 g och 13 h i [Eurodacförordningen].]

- (e) [De uppgifter som avses i artikel 5.1 b och 5.2 och följande uppgifter i artikel 5.1 a i Ecris-TCN-förordningen: efternamn eller familjenamn, samtliga förnamn, kön, födelsedatum, födelseort och födelseland, samtliga medborgarskap, kön och, i förekommande fall, tidigare namn, pseudonymer och/eller alias.]
2. För varje uppsättning uppgifter som avses i punkt 1 ska CIR innehålla en hänvisning till de informationssystem som uppgifterna tillhör.
 3. Lagringen av de uppgifter som avses i punkt 1 ska uppfylla de kvalitetsstandarder som avses i artikel 37.2.

Artikel 19

Tillägg, ändring och radering av uppgifter i den gemensamma databasen för identitetsuppgifter

1. Om uppgifter läggs till, ändras eller raderas i Eurodac eller [Ecris-TCN-systemet] ska de uppgifter som avses i artikel 18 vilka lagras i personakten i CIR automatiskt läggas till, ändras eller raderas.
2. Om detektorn för multipla identiteter skapar en vit eller en röd länk i enlighet med artiklarna 32 och 33 mellan uppgifter i två eller flera av EU-informationssystemen som utgör CIR, ska CIR i stället för att skapa en ny personakt lägga till de nya uppgifterna i den personakt som innehåller de länkade uppgifterna.

Artikel 20

Åtkomst till den gemensamma databasen för identitetsuppgifter i identifieringssyfte

1. Om en medlemsstats polismyndighet har bemyndigats genom de nationella lagstiftningsåtgärder som avses i punkt 2, får myndigheten, endast i syfte att identifiera en person, söka i CIR med denna persons biometriska uppgifter som tagits under en identitetskontroll.

Om sökningen visar att uppgifter om denna person finns lagrade i CIR, ska medlemsstatens myndighet ha åtkomst till att konsultera de uppgifter som avses i artikel 18.1.

Om personens biometriska uppgifter inte kan användas eller om sökningen med dessa uppgifter misslyckas, ska sökningen utföras med vederbörandes identitetsuppgifter i kombination med resehandlingsuppgifter eller med de identitetsuppgifter som tillhandahållits av personen.
2. Medlemsstater som vill utnyttja den möjlighet som anges i denna artikel ska anta nationella lagstiftningsåtgärder. I sådana lagstiftningsåtgärder ska de exakta syftena med identitetskontroller anges inom ramen för de mål som avses i artikel 2.1 b och c. De polismyndigheter som är behöriga ska utses och förfaranden, villkor och kriterier för sådana kontroller ska fastställas i dem.

Artikel 21

Åtkomst till den gemensamma databasen för identitetsuppgifter för spårning av multipla identiteter

1. Om en sökning i CIR resulterar i en gul länk i enlighet med artikel 28.4, ska den myndighet som ansvarar för verifieringen av olika identiteter och som fastställts i enlighet med artikel 29 enbart i verifieringssyfte ha åtkomst till de identitetsuppgifter

som lagrats i CIR och som tillhör de olika informationssystem som är kopplade till en gul länk.

2. Om en sökning i CIR ger upphov till en röd länk i enlighet med artikel 32, ska de myndigheter som avses i artikel 26.2 enbart i syfte att bekämpa identitetsbedrägerier ha åtkomst till de identitetsuppgifter som lagrats i CIR och som tillhör de olika informationssystem som är kopplade till en röd länk.

Artikel 22

Sökningar i den gemensamma databasen för identitetsuppgifter i brottsbekämpande syfte

1. I syfte att förhindra, upptäcka och utreda terroristbrott eller andra grova brott i ett specifikt fall och för att få information om huruvida det finns uppgifter om en viss person i Eurodac får medlemsstaternas utsedda myndigheter och Europol söka i CIR.
2. Medlemsstaternas utsedda myndigheter och Europol får inte söka i uppgifter som tillhör [Ecris-TCN] när de söker i CIR för de syften som anges i punkt 1.
3. Om ett svar på en sökning i CIR visar att det finns uppgifter om personen i Eurodac ska CIR tillhandahålla medlemsstaternas utsedda myndigheter och Europol ett svar i form av en hänvisning om vilka informationssystem som innehåller motsvarande uppgifter som avses i artikel 18.2. CIR ska svara på ett sådant sätt att uppgifternas säkerhet inte äventyras.
4. Fullständig åtkomst till uppgifterna i EU-informationssystemen i syfte att förebygga, upptäcka och utreda terroristbrott eller andra grova brott omfattas fortfarande av de villkor och förfaranden som fastställs i respektive lagstiftningsinstrument där sådan åtkomst regleras.

Artikel 23

Lagring av uppgifter i den gemensamma databasen för identitetsuppgifter

1. De uppgifter som avses i artikel 18.1 och 18.2 ska raderas från CIR i enlighet med bestämmelserna om lagring av uppgifter i [Eurodacförordningen] respektive [Ecris-TCN-förordningen].
2. Personakten ska lagras i CIR så länge de motsvarande uppgifterna lagras i minst ett av de informationssystem vars uppgifter finns i CIR. Skapandet av en länk ska inte påverka lagringsperioden för varje post av de länkade uppgifterna.

Artikel 24

Registerföring av loggar

1. Utan att det påverkar tillämpningen av [artikel 39 i Eurodacförordningen] och [artikel 29 i Ecris-TCN-förordningen] ska eu-LISA föra logg över all uppgiftsbehandling inom CIR i enlighet med punkterna 2, 3 och 4.
2. Vad gäller åtkomst till CIR i enlighet med artikel 20 ska eu-LISA föra logg över all uppgiftsbehandling inom CIR. Dessa loggar ska särskilt omfatta följande:
 - (a) Syftet med användarens åtkomst för att söka via CIR.
 - (b) Datum och tidpunkt för sökningen.
 - (c) Den typ av uppgifter som används för att inleda sökningen.
 - (d) Sökningens resultat.

- (e) I enlighet med nationella regler eller med förordning (EU) 2016/794 eller, i tillämpliga fall, förordning (EU) 45/2001, beteckningen för den person som utförde sökningen.
3. Vad gäller åtkomst till CIR i enlighet med artikel 21 ska eu-LISA föra logg över all uppgiftsbehandling inom CIR. Dessa loggar ska särskilt omfatta följande:
- (a) Syftet med användarens åtkomst för att söka via CIR.
 - (b) Datum och tidpunkt för sökningen.
 - (c) De uppgifter som används för att inleda sökningen, i förekommande fall.
 - (d) Sökningens resultat i förekommande fall.
 - (e) I enlighet med nationella regler eller med förordning (EU) 2016/794 eller, i tillämpliga fall, förordning (EU) 45/2001, beteckningen för den person som utförde sökningen.
4. Vad gäller åtkomst till CIR i enlighet med artikel 22 ska eu-LISA föra logg över all uppgiftsbehandling inom CIR. Dessa loggar ska särskilt omfatta följande:
- (a) Referensnummer för den nationella akten.
 - (b) Datum och tidpunkt för sökningen.
 - (c) Den typ av uppgifter som används för att inleda sökningen.
 - (d) Sökningens resultat.
 - (e) Namnet på den myndighet som söker i CIR.
 - (f) I enlighet med nationella regler eller med förordning (EU) 2016/794 eller, i tillämpliga fall, förordning (EU) 45/2001, beteckningen för den tjänsteman som utförde sökningen och den tjänsteman som beställde sökningen.
- Loggarna över sådan åtkomst ska kontrolleras regelbundet av den behöriga tillsynsmyndighet som inrättats i enlighet med artikel 51 i förordning (EU) 2016/679 eller i enlighet med artikel 41 i direktiv 2016/680, med högst sex månaders mellanrum, för att kontrollera om förfarandena och villkoren i artikel 22.1–3 är uppfyllda.
5. Varje medlemsstat ska föra logg över de sökningar som görs av personal som är vederbörligen bemyndigad att använda CIR enligt artiklarna 20, 21 och 22.
6. De loggar som avses i punkterna 1 och 5 får endast användas för övervakning av dataskyddet, inbegripet för kontroll av om en begäran är tillåten och om uppgifter har behandlats på ett lagligt sätt samt för att säkerställa datasäkerhet i enlighet med artikel 42. De ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats, såvida de inte behövs för övervakningsförfaranden som redan har inletts.
7. Eu-LISA ska föra logg över historiken avseende de uppgifter som lagras i personakten för de syften som anges i punkt 6. Loggarna över historiken avseende de lagrade uppgifterna ska raderas så snart uppgifterna har raderats.

KAPITEL V

[Detektorn för multipla identiteter]

Artikel 25

Detektorn för multipla identiteter

1. Det ska inrättas en detektor för multipla identiteter som skapar och lagrar länkar mellan uppgifter i de EU-informationssystem som ingår i den gemensamma databasen för identitetsuppgifter (CIR) och SIS och därför spårar multipla identiteter, med det dubbla syftet att underlätta identitetskontroller och bekämpa identitetsbedrägerier, för att stödja CIR:s funktion och målen för in- och utresesystemet, VIS, [Etias], Eurodac, SIS och [Ecris-TCN-systemet].
2. Detektorn för multipla identiteter ska bestå av följande:
 - (a) En central infrastruktur som lagrar länkar och hänvisningar till informationssystem.
 - (b) En säker kommunikationsinfrastruktur som kopplar detektorn för multipla identiteter till SIS och den europeiska sökportalens och CIR:s centrala infrastrukturer.
3. Eu-LISA ska utveckla detektorn för multipla identiteter och säkerställa den tekniska förvaltningen.

Artikel 26

Åtkomst till detektorn för multipla identiteter

1. För den manuella identitetsverifiering som avses i artikel 29 ska åtkomst till de uppgifter som avses i artikel 34 och som är lagrade i detektorn för multipla identiteter beviljas
 - (a) – (ej tillämpligt)
 - (b) – (ej tillämpligt)
 - (c) – (ej tillämpligt)
 - (d) de myndigheter som är behöriga att bedöma en ansökan om internationellt skydd enligt Eurodacförordningen vid bedömning av en ny ansökan om internationellt skydd,
 - (e) Sirenekontoren i den registrerande medlemsstaten [förordningen om SIS på området brottsbekämpning eller förordningen om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna],
 - (f) [de centrala myndigheterna i den dömande medlemsstaten vid registrering eller uppdatering av uppgifter i Ecris-TCN-systemet i enlighet med artikel 5 i Ecris-TCN-förordningen].
2. De myndigheter i medlemsstaterna och de EU-organ som har åtkomst till minst ett av de EU-informationssystem som ingår i den gemensamma databasen för identitetsuppgifter eller till SIS ska ha åtkomst till de uppgifter som avses i artikel 34 a och b vad gäller samtliga röda länkar som avses i artikel 32.

Artikel 27
Spårning av multipla identiteter

1. En spårning av multipla identiteter ska i följande fall inledas i den gemensamma databasen för identitetsuppgifter och i SIS:
 - (a) – (ej tillämpligt)
 - (b) – (ej tillämpligt)
 - (c) – (ej tillämpligt)
 - (d) [En ansökan om internationellt skydd skapas eller uppdateras i Eurodac i enlighet med artikel 10 i Eurodacförordningen].
 - (e) [En registrering om en person skapas eller uppdateras i SIS i enlighet med kapitlen VI, VII, VIII och IX i förordningen om SIS på området brottsbekämpning och artikel 3 i förordningen om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna].
 - (f) [En datapost skapas eller uppdateras i Ecris-TCN-systemet i enlighet med artikel 5 i Ecris-TCN-förordningen].
2. Om de uppgifter i ett informationssystem som avses i punkt 1 innehåller biometriska uppgifter ska den gemensamma databasen för identitetsuppgifter (CIR) och det centrala SIS använda den gemensamma biometriska matchningstjänsten för att utföra en spårning av multipla identiteter. Den gemensamma biometriska matchningstjänsten ska jämföra de biometriska mallar som erhållits från nya biometriska uppgifter med de biometriska mallar som redan finns i den gemensamma biometriska matchningstjänsten i syfte att verifiera huruvida uppgifter som tillhör samma tredjelandsmedborgare redan finns lagrade i CIR eller i det centrala SIS.
3. Utöver det förfarande som avses i punkt 2 ska CIR och det centrala SIS använda den europeiska sökportalen för att söka i uppgifter som lagrats i CIR och det centrala SIS med hjälp av följande uppgifter:
 - (a) – (ej tillämpligt)
 - (b) – (ej tillämpligt)
 - (c) – (ej tillämpligt)
 - (d) [Samtliga efternamn, samtliga förnamn, namn vid födelsen och tidigare använda namn och alias, födelsedatum, födelseort, samtliga medborgarskap och kön enligt artikel 12 i Eurodacförordningen].
 - (e) – (ej tillämpligt)
 - (f) [Samtliga efternamn, samtliga förnamn, namn vid födelsen och tidigare använda namn och alias, födelsedatum, födelseort, samtliga medborgarskap och kön enligt artikel 20.3 i förordningen om SIS på området brottsbekämpning].
 - (g) [Samtliga efternamn, samtliga förnamn, namn vid födelsen och tidigare använda namn och alias, födelsedatum, födelseort, samtliga medborgarskap och kön enligt artikel 4 i förordningen om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna].
 - (h) [Efternamn, förnamn, födelsedatum, födelseort, medborgarskap och kön enligt artikel 5.1 a i Ecris-TCN-förordningen].

4. En spårning av multipla identiteter ska endast inledas för att jämföra tillgängliga uppgifter i ett informationssystem med tillgängliga uppgifter i andra informationssystem.

Artikel 28

Resultat av en spårning av multipla identiteter

1. Om de sökningar som avses i artikel 27.2 och 27.3 inte ger någon träff ska de förfaranden som avses i artikel 27.1 fortsätta i enlighet med respektive förordning genom vilka de regleras.
2. Om den sökning som avses i artikel 27.2 och 27.3 ger en eller flera träffar ska den gemensamma databasen för identitetsuppgifter och, i förekommande fall, SIS skapa en länk mellan de uppgifter som används för att inleda sökningen och de uppgifter som gett upphov till träffen.

Vid flera träffar ska en länk skapas mellan alla de uppgifter som gett upphov till träffen. Om uppgifter redan har länkats, ska den befintliga länken utvidgas till att omfatta de uppgifter som använts för att inleda sökningen.

3. Om den sökning som avses i artikel 27.2 eller 27.3 ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är identiska eller liknande, ska en vit länk skapas i enlighet med artikel 33.
4. Om den sökning som avses i artikel 27.2 eller 27.3 ger en eller flera träffar och identitetsuppgifterna i de länkade akterna inte kan anses vara liknande, ska en gul länk skapas i enlighet med artikel 30 och det förfarande som avses i artikel 29 ska tillämpas.
5. Kommissionen ska i genomförandeakter fastställa förfaranden för att avgöra ärenden där identitetsuppgifter kan anses vara identiska eller liknande. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 64.2.
6. Länkarna ska lagras i den akt med identitetsbekräftelse som avses i artikel 34.

Kommissionen ska fastställa de tekniska reglerna för länkning av uppgifter från olika informationssystem genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 64.2.

Artikel 29

Manuell verifiering av olika identiteter

1. Utan att det påverkar tillämpningen av punkt 2 ska den myndighet som ansvarar för verifieringen av olika identiteter vara följande:
 - (a) – (ej tillämpligt)
 - (b) – (ej tillämpligt)
 - (c) – (ej tillämpligt)
 - (d) Den myndighet som bedömer en ansökan om internationellt skydd i enlighet med Eurodacförordningen vad gäller träffar som uppkommit vid bedömningen av en sådan begäran.
 - (e) Medlemsstatens Sirenekontor vad gäller träffar som uppkommit vid skapandet av en SIS-registrering i enlighet med [förordningarna om SIS på området

brottsbekämpning och på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna].

- (f) De centrala myndigheterna i den dömande medlemsstaten vad gäller träffar som uppkommit vid registrering eller uppdatering av uppgifter i Ecris-TCN-systemet i enlighet med artikel 5 i [Ecris-TCN-förordningen].

Detektorn för multipla identiteter ska ange den myndighet som ansvarar för verifieringen av olika identiteter i identitetsverifieringsakten.

2. Den myndighet som ansvarar för verifieringen av olika identiteter i akten med identitetsbekräftelse ska vara Sirenekontoret i den medlemsstat som skapade registreringen om det skapas en länk till uppgifterna i
 - (a) en registrering om personer som är efterlysta för gripande för överlämnande eller utlämning enligt artikel 26 i [förordningen om SIS på området brottsbekämpning],
 - (b) en registrering om försvunna eller sårbara personer enligt artikel 32 i [förordningen om SIS på området brottsbekämpning],
 - (c) en registrering om personer som söks för att delta i ett rättsligt förfarande enligt artikel 34 i [förordningen om SIS på området brottsbekämpning],
 - (d) [en registrering om återvändande i enlighet med förordningen om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna],
 - (e) en registrering om personer för diskreta kontroller, undersökningskontroller eller särskilda kontroller enligt artikel 36 i [förordningen om SIS på området brottsbekämpning],
 - (f) en registrering om okända efterlysta personer för identifiering i enlighet med nationell lagstiftning samt sökning med biometriska uppgifter enligt artikel 40 i [förordningen om SIS på området brottsbekämpning].
3. Utan att det påverkar tillämpningen av punkt 4 ska den myndighet som ansvarar för verifieringen av olika identiteter ha åtkomst till de relaterade uppgifterna i den relevanta akten med identitetsbekräftelse och till de identitetsuppgifter som är länkade i den gemensamma databasen för identitetsuppgifter och, i förekommande fall, i SIS och ska bedöma de olika identiteterna och uppdatera länken i enlighet med artiklarna 31, 32 och 33 samt utan dröjsmål lägga till den i akten med identitetsbekräftelse.
4. – (Ej tillämpligt).
5. Om fler än en länk erhålls, ska den myndighet som ansvarar för verifieringen av olika identiteter bedöma varje länk separat.
6. Om uppgifter som ger en träff redan var länkade, ska den myndighet som ansvarar för verifieringen av olika identiteter beakta de befintliga länkarna vid bedömningen av skapandet av nya länkar.

Artikel 30 *Gul länk*

1. En länk mellan uppgifter från två eller flera informationssystem ska klassificeras som gul i samtliga följande fall:

- (a) De länkade uppgifterna innehåller samma biometriska uppgifter men olika identitetsuppgifter och ingen manuell verifiering av olika identiteter har ägt rum.
 - (b) De länkade uppgifterna innehåller olika identitetsuppgifter och ingen manuell verifiering av olika identiteter har ägt rum.
2. Om en länk klassificeras som gul i enlighet med punkt 1 ska förfarandet i artikel 29 tillämpas.

Artikel 31
Grön länk

1. En länk mellan uppgifter från två eller flera informationssystem ska klassificeras som grön om de länkade uppgifterna inte har samma biometriska uppgifter men har liknande identitetsuppgifter och om den myndighet som ansvarar för verifieringen av olika identiteter har konstaterat att uppgifterna gäller två olika personer.
2. Om en sökning görs i den gemensamma databasen för identitetsuppgifter (CIR) eller SIS och om det finns en grön länk mellan två eller fler av de informationssystem som utgör CIR, eller till SIS, ska detektorn för multipla identiteter ange att identitetsuppgifterna i de länkade uppgifterna inte tillhör samma person. Det informationssystem som varit föremål för sökning ska svara genom att ange endast uppgifter om den person vars uppgifter användes vid sökningen, utan att ge upphov till en träff mot de uppgifter som omfattas av den gröna länken.

Artikel 32
Röd länk

1. En länk mellan uppgifter från två eller flera informationssystem ska klassificeras som röd i samtliga följande fall:
- (a) De länkade uppgifterna har samma biometriska uppgifter men olika identitetsuppgifter och den myndighet som ansvarar för verifieringen av olika identiteter har konstaterat att den olagligen gäller en och samma person.
 - (b) De länkade uppgifterna har liknande identitetsuppgifter och den myndighet som ansvarar för verifieringen av olika identiteter har konstaterat att den olagligen hänvisar till en och samma person.
2. Om CIR eller SIS är föremål för sökning och om det finns en röd länk mellan två eller fler av de informationssystem som utgör CIR, eller med SIS, ska detektorn för multipla identiteter svara genom att ange de uppgifter som avses i artikel 34. En uppföljning av en röd länk ska ske i enlighet med unionsrätten och nationell lagstiftning.
3. Om det skapas en röd länk mellan uppgifter från in- och utresesystemet, VIS, [Etias], Eurodac eller [Ecris-TCN-systemet] ska den personakt som lagras i CIR uppdateras i enlighet med artikel 19.1.
4. Utan att det påverkar tillämpningen av bestämmelserna om hantering av registreringar i SIS som avses i [förordningarna om SIS på området in- och utresekontroller, om SIS på området brottsbekämpning och om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna], och

utan att det påverkar begränsningar som är nödvändiga för att trygga säkerheten och den allmänna ordningen, förebygga brott samt garantera att nationella utredningar inte kommer att äventyras, ska den myndighet som ansvarar för verifieringen av olika identiteter, vid skapandet av en röd länk, underrätta personen om förekomsten av multipla olagliga identiteter.

5. När en röd länk skapas ska den myndighet som ansvarar för verifieringen av olika identiteter tillhandahålla en hänvisning till de myndigheter som ansvarar för de länkade uppgifterna.

Artikel 33

Vit länk

1. En länk mellan uppgifter från två eller flera informationssystem ska klassificeras som vit i samtliga följande fall:
 - (a) De länkade uppgifterna har samma biometriska uppgifter och samma eller liknande identitetsuppgifter.
 - (b) De länkade uppgifterna har samma eller liknande identitetsuppgifter och minst ett av informationssystemen saknar biometriska uppgifter om personen.
 - (c) De länkade uppgifterna har samma biometriska uppgifter men olika identitetsuppgifter och den myndighet som ansvarar för verifieringen av olika identiteter har konstaterat att den hänvisar till en och samma person som lagligen har olika identitetsuppgifter.
2. Om CIR eller SIS är föremål för sökning och om det finns en vit länk mellan ett eller fler av de informationssystem som utgör CIR, eller med SIS, ska detektorn för multipla identiteter ange att identitetsuppgifterna i de länkade uppgifterna gäller samma person. De informationssystem som är föremål för sökning ska svara genom att i förekommande fall ange alla länkade uppgifter om personen vilka ger upphov till en träff mot de uppgifter som omfattas av den vita länken, om den myndighet som inlett sökningen har åtkomst till de länkade uppgifterna enligt unionsrätten eller nationell lagstiftning.
3. Om det skapas en vit länk mellan uppgifter från in- och utresesystemet, VIS, [Etias], Eurodac eller [Ecris-TCN-systemet] ska den personakt som lagras i CIR uppdateras i enlighet med artikel 19.1.
4. Utan att det påverkar tillämpningen av bestämmelserna om hantering av registreringar i SIS som avses i [förordningarna om SIS på området in- och utresekontroller, om SIS på området brottsbekämpning och om SIS på området återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna] ska den myndighet som ansvarar för verifieringen av olika identiteter vid skapandet av en vit länk efter en manuell verifiering av multipla identiteter underrätta personen om att det förekommer skillnader mellan dennas personuppgifter mellan systemen, och ska tillhandahålla en referens till de myndigheter som ansvarar för de länkade uppgifterna.

Artikel 34

Akt med identitetsbekräftelse

Akten med identitetsbekräftelse ska innehålla följande uppgifter:

- (a) Länkarna, inbegripet en beskrivning av dem i form av färger, i enlighet med

artiklarna 30–33.

- (b) En hänvisning till de informationssystem vilkas uppgifter är länkade.
- (c) Ett enda identifikationsnummer som gör det möjligt att hämta uppgifter från de informationssystem som har motsvarande länkade akter.
- (d) I tillämpliga fall, den myndighet som ansvarar för verifieringen av olika identiteter.

Artikel 35

Lagring av uppgifter i detektorn för multipla identiteter

Akterna med identitetsbekräftelse och uppgifterna i dem, inbegripet länkarna, ska lagras i detektorn för multipla identiteter endast under den tid som de länkade uppgifterna lagras i två eller fler EU-informationssystem.

Artikel 36

Registerföring av loggar

1. Eu-LISA ska föra logg över all uppgiftsbehandling som sker i detektorn för multipla identiteter. Dessa loggar ska särskilt omfatta följande:
 - (a) Syftet med användarens åtkomst och dennas åtkomsträttigheter.
 - (b) Datum och tidpunkt för sökningen.
 - (c) Den typ av uppgifter som används för att inleda sökningen eller sökningarna.
 - (d) Hänvisning till de länkade uppgifterna.
 - (e) Historik tillhörande akten med identitetsbekräftelse.
 - (f) Beteckning för den person som utförde sökningen.
2. Varje medlemsstat ska föra logg över den personal som är vederbörligen bemyndigad att använda detektorn för multipla identiteter.
3. Loggarna får endast användas för övervakning av dataskyddet, inbegripet för kontroll av om en begäran är tillåten och om uppgifter har behandlats på ett lagligt sätt samt för att säkerställa datasäkerhet i enlighet med artikel 42. Loggarna ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats, såvida de inte behövs för övervakningsförfaranden som redan har inletts. Loggarna över historiken avseende akten med identitetsbekräftelse ska raderas så snart uppgifterna i akten med identitetsbekräftelse har raderats.

KAPITEL VI

Åtgärder till stöd för interoperabilitet

Artikel 37

Uppgifternas kvalitet

1. Eu-LISA ska inrätta automatiska mekanismer och förfaranden för kontroll av uppgifternas kvalitet avseende de uppgifter som lagras i SIS, Eurodac, [Ecris-TCN-

systemet], den gemensamma biometriska matchningstjänsten, den gemensamma databasen för identitetsuppgifter (CIR) och detektorn för multipla identiteter.

2. Eu-LISA ska inrätta gemensamma indikatorer för uppgifternas kvalitet och minimikvalitetsstandarder för lagring av uppgifter i SIS, Eurodac, [Ecris-TCN-systemet], den gemensamma biometriska matchningstjänsten, CIR och detektorn för multipla identiteter.
3. Eu-LISA ska regelbundet tillhandhålla rapporter om de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet och de gemensamma indikatorerna för uppgifternas kvalitet till medlemsstaterna. Eu-LISA ska också regelbundet rapportera till kommissionen om problem som uppstått och vilka medlemsstater som berörs.
4. Detaljerna om de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma indikatorerna för uppgifternas kvalitet och minimikvalitetsstandarderna för lagring av uppgifter i SIS, Eurodac, [Ecris-TCN-systemet], den gemensamma biometriska matchningstjänsten, CIR och detektorn för multipla identiteter, särskilt vad gäller biometriska uppgifter, ska fastställas i genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 64.2.
5. Ett år efter inrättandet av de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet och de gemensamma indikatorerna för uppgifternas kvalitet och varje år därefter ska kommissionen utvärdera medlemsstaternas genomförande av uppgifternas kvalitet och lämna nödvändiga rekommendationer. Medlemsstaterna ska förse kommissionen med en handlingsplan för att avhjälpa de brister som konstaterats i utvärderingsrapporten och ska rapportera om vilka framsteg som har gjorts med denna handlingsplan till dess att den genomförts fullt ut. Kommissionen ska överlämna utvärderingsrapporten till Europaparlamentet, rådet, Europeiska datatillsynsmannen och Europeiska unionens byrå för grundläggande rättigheter som inrättades genom rådets förordning (EG) nr 168/2007⁶³.

Artikel 38

Universellt meddelandeformat

1. Härmed inrättas en standard för ett universellt meddelandeformat (UMF). Genom det universella meddelandeformatet definieras standarder för vissa innehållselement i det gränsöverskridande informationsutbytet mellan informationssystem, myndigheter och/eller organisationer på området rättsliga och inrikes frågor.
2. UMF-standarderna ska användas vid utvecklingen av [Eurodac], [Ecris-TCN-systemet], den europeiska sökportalen, CIR, detektorn för multipla identiteter och, i förekommande fall, eu-LISA:s eller andra EU-organs utveckling av nya modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor.
3. Möjligheten kan övervägas att införa UMF-standarderna i SIS och i alla befintliga eller nya gränsöverskridande modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor vilka utvecklas av medlemsstaterna eller associerade länder.

⁶³ Rådets förordning (EG) nr 168/2007 av den 15 februari 2007 om inrättande av Europeiska unionens byrå för grundläggande rättigheter (EUT L 53, 22.2.2007, s. 1).

4. Kommissionen ska anta en genomförandeakt för fastställande och utveckling av den UMF-standard som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 64.2.

Artikel 39

Den centrala databasen för rapporter och statistik

1. Det ska inrättas en central databas för rapporter och statistik (CRRS) för att stödja målen för Eurodac, SIS och [Ecris-TCN-systemet] och för att ta fram systemöverskridande statistiska uppgifter och analysrapporter för politiska och operativa syften samt för uppgiftskvaliteten.
2. Eu-LISA ska inrätta, implementera och hysa CRRS vid sina tekniska anläggningar som logiskt åtskilt innehåller de uppgifter som avses i [artikel 42.8 i Eurodacförordningen], [artikel 71 i förordningen om SIS på området brottsbekämpning] och [artikel 30 i Ecris-TCN-förordningen]. Uppgifterna i CRRS ska inte göra det möjligt att identifiera individer. Åtkomst till databasen ska beviljas via säkrad åtkomst genom nättjänsten transeuropeiska telematiktjänster för myndigheter (Testa) med åtkomstkontroll och specifika användarprofiler enbart för rapportering och statistik, till de myndigheter som avses i [artikel 42.8 i Eurodacförordningen], [artikel 71 i förordningen om SIS på området brottsbekämpning] och [artikel 30 i Ecris-TCN-förordningen].
3. Eu-LISA ska anonymisera uppgifterna och registrera de anonymiserade uppgifterna i CRRS. Förfarandet för att anonymisera uppgifterna ska vara automatiskt.
4. CRRS ska bestå av följande:
 - (a) En central infrastruktur som består av en central databas som gör det möjligt att anonymisera uppgifter.
 - (b) En säker kommunikationsinfrastruktur för att ansluta CRRS till SIS, Eurodac och [Ecris-TCN] samt de centrala infrastrukturerna för den gemensamma biometriska matchningstjänsten, CIR och detektorn för multipla identiteter.
5. Kommissionen ska fastställa detaljerade bestämmelser om driften av CRRS, inbegripet särskilda skyddsåtgärder för behandling av de personuppgifter som avses i punkt 2 och 3 och de säkerhetsregler som är tillämpliga på databasen genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 64.2.

KAPITEL VII

Dataskydd

Artikel 40

Personuppgiftsansvarig

1. När det gäller behandling av uppgifter i den gemensamma biometriska matchningstjänsten ska medlemsstaternas myndigheter som är personuppgiftsansvariga för Eurodac, SIS respektive [Ecris-TCN-systemet] också anses vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 avseende de biometriska mallar som erhållits från de uppgifter som avses i

artikel 13 och som de lägger in i respektive system och ska ansvara för behandlingen av de biometriska mallarna i den gemensamma biometriska matchningstjänsten.

2. När det gäller behandling av uppgifter i den gemensamma databasen för identitetsuppgifter (CIR) ska medlemsstaternas myndigheter som är personuppgiftsansvariga för Eurodac respektive [Ecris-TCN-systemet] också anses vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 avseende de uppgifter som avses i artikel 18 och som de lägger in i respektive system och ska ansvara för behandlingen av dessa personuppgifter i CIR.
3. När det gäller behandling av uppgifter i detektorn för multipla identiteter:
 - (a) Europeiska gräns- och kustbevakningsbyrån ska anses vara personuppgiftsansvarig i enlighet med artikel 2 b i förordning nr 45/2001 när det gäller behandling av personuppgifter som utförs av Etias centralenhet.
 - (b) Medlemsstaters myndigheter som lägger till eller ändrar uppgifter i akten med identitetsbekräftelse ska också anses vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 och ska ansvara för behandlingen av personuppgifter i detektorn för multipla identiteter.

Artikel 41 Registerförare

När det gäller behandling av personuppgifter i CIR ska eu-LISA anses vara registerförare i enlighet med artikel 2 e i förordning (EG) nr 45/2001.

Artikel 42 Säkerhet vid behandling

1. Både eu-LISA och medlemsstaternas myndigheter ska säkerställa att personuppgifter behandlas säkert enligt den här förordningen. Eu-LISA, [Etias centralenhet] och medlemsstaternas myndigheter ska samarbeta kring säkerhetsrelaterade uppgifter.
2. Utan att det påverkar tillämpningen av artikel 22 i förordning (EG) nr 45/2001 ska eu-LISA vidta nödvändiga åtgärder för att säkerställa säkerheten för interoperabilitetskomponenterna och den relaterade kommunikationsinfrastrukturen.
3. Eu-LISA ska i synnerhet vidta nödvändiga åtgärder, inbegripet en säkerhetsplan, en kontinuitetsplan och en katastrofplan, i syfte att
 - (a) fysiskt skydda uppgifter, bland annat genom att utarbeta beredskapsplaner för skydd av kritisk infrastruktur,
 - (b) hindra obehöriga från att läsa, kopiera, ändra eller avlägsna datamedier,
 - (c) hindra obehörigt införande av uppgifter och hindra obehöriga från att skaffa sig kännedom om, ändra eller radera lagrade personuppgifter,
 - (d) hindra obehörig behandling av uppgifter och hindra obehöriga från att kopiera, ändra eller radera uppgifter,
 - (e) säkerställa att personer som har åtkomstbehörighet till interoperabilitetskomponenterna endast har åtkomst till de uppgifter för vilka de är behöriga endast med hjälp av individuella användaridentiteter och skyddade åtkomstmetoder,
 - (f) säkerställa att det är möjligt att kontrollera och fastställa till vilka organ

personuppgifter får överföras via datakommunikationsutrustning,

- (g) säkerställa att det är möjligt att kontrollera och fastställa vilka uppgifter som har behandlats i interoperabilitetskomponenterna, när detta har gjorts, av vem, och i vilket syfte,
 - (h) hindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av personuppgifter till eller från interoperabilitetskomponenterna eller under transport av datamedier, särskilt med hjälp av lämplig krypteringsteknik,
 - (i) övervaka att de säkerhetsåtgärder som avses i denna punkt är ändamålsenliga och vidta nödvändiga organisatoriska åtgärder i fråga om inre övervakning för att säkerställa att denna förordning efterlevs.
4. Medlemsstaterna ska vidta åtgärder som är likvärdiga med de som avses i punkt 3 vad gäller säkerheten vid behandling av personuppgifter som utförs av de myndigheter som har åtkomsträtt till någon av interoperabilitetskomponenterna.

Artikel 43

SIS-uppgifternas konfidentialitet

1. 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 till vilka åtkomst fåtts genom någon av interoperabilitetskomponenterna. Reglerna ska gälla även efter det att personerna lämnat sin tjänst eller anställning eller efter det att organets verksamhet upphört.
2. Utan att det påverkar tillämpningen av artikel 17 i tjänsteföreskrifterna för tjänstemän i Europeiska unionen och anställningsvillkoren för övriga anställda i Europeiska unionen ska eu-LISA tillämpa lämpliga regler om tystnadsplikt eller motsvarande sekretesskrav som är jämförbara med de som anges i punkt 1 på all personal som arbetar med SIS-uppgifter. Reglerna ska gälla även efter det att personerna lämnat sin tjänst eller anställning eller upphört med sin yrkesverksamhet.

Artikel 44

Säkerhetstillbud

1. Alla händelser som har eller kan ha inverkan på interoperabilitetskomponenternas säkerhet och som kan orsaka skada på eller förlust av uppgifter lagrade i dem ska betraktas som säkerhetstillbud, särskilt om obehörig åtkomst till uppgifter kan ha inträffat eller uppgifters tillgänglighet, integritet och konfidentialitet har äventyrats eller kan ha äventyrats.
2. Säkerhetstillbud ska hanteras på ett sätt som säkerställer en snabb, effektiv och välavvägd respons.
3. Utan att det påverkar anmälan av och information om personuppgiftsincidenter i enlighet med artikel 33 i förordning (EU) 2016/679, artikel 30 i direktiv (EU) 2016/680 eller båda, ska medlemsstaterna underrätta kommissionen, eu-LISA och Europeiska datatillsynsmannen om säkerhetstillbud. Om ett säkerhetstillbud inträffar avseende interoperabilitetskomponenternas centrala infrastruktur ska eu-LISA underrätta kommissionen och Europeiska datatillsynsmannen.
4. Information om säkerhetstillbud som har eller kan ha inverkan på interoperabilitetskomponenternas drift eller på uppgifternas tillgänglighet, integritet

och konfidentialitet ska tillhandahållas medlemsstaterna och rapporteras i enlighet med den incidenthanteringsplan som eu-LISA ska tillhandahålla.

5. De berörda medlemsstaterna och eu-LISA ska samarbeta om ett säkerhetstillbud inträffar. Kommissionen ska fastställa specifikationer för detta samarbete genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 64.2.

Artikel 45 *Egenkontroll*

Medlemsstaterna och de relevanta EU-organen ska säkerställa att varje myndighet som har åtkomsträtt till interoperabilitetskomponenterna vidtar nödvändiga åtgärder för att övervaka efterlevnaden av denna förordning och vid behov samarbetar med tillsynsmyndigheterna.

De personuppgiftsansvariga som avses i artikel 40 ska vidta nödvändiga åtgärder för att övervaka att uppgiftsbehandlingen sker i enlighet med denna förordning, däribland genom frekventa kontroller av loggar, och vid behov samarbeta med de tillsynsmyndigheter som avses i artiklarna 49 och 50.

Artikel 46 *Rätt till information*

1. Utan att det påverkar den rätt till information som avses i artiklarna 11 och 12 i förordning (EG) nr 45/2001 och artiklarna 13 och 14 i förordning (EU) 2016/679, ska de personer vilkas uppgifter lagras i den gemensamma biometrisk matchningstjänsten, den gemensamma databasen för identitetsuppgifter eller detektorn för multipla identiteter, vid den tidpunkt då deras uppgifter samlas in, underrättas av den myndighet som samlar in uppgifterna om behandlingen av personuppgifter vid tillämpningen av denna förordning, inbegripet om respektive personuppgiftsansvarigs identitet och kontaktuppgifter samt förfarandena för att utöva rätten till åtkomst till, rättelse och radering av uppgifter samt om kontaktuppgifter till Europeiska datatillsynsmannen och den nationella tillsynsmyndigheten i den medlemsstat som ansvarar för insamlingen av uppgifterna.
2. De personer vilkas uppgifter registrerats i Eurodac eller [Ecris-TCN-systemet] ska underrättas om behandlingen av uppgifter vid tillämpningen av denna förordning, i enlighet med punkt 1 i följande fall:
 - (a) – (ej tillämpligt)
 - (b) – (ej tillämpligt)
 - (c) – (ej tillämpligt)
 - (d) [En ansökan om internationellt skydd skapas eller uppdateras i Eurodac i enlighet med artikel 10 i Eurodacförordningen].
 - (e) [En datapost skapas eller uppdateras i Ecris-TCN-systemet i enlighet med artikel 5 i Ecris-TCN-förordningen].

Artikel 47 *Rätt till åtkomst, korrigering och radering*

1. För att utöva sina rättigheter enligt artiklarna 13, 14, 15 och 16 i förordning (EG) 45/2001 och artiklarna 15, 16, 17 och 18 i förordning (EU) 2016/679, ska varje

person ha rätt att vända sig till den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller till en annan medlemsstat som ska pröva och besvara begäran.

2. Den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter enligt artikel 29 eller den medlemsstat till vilken begäran har ställts ska besvara denna inom 45 dagar från mottagandet.
3. Om en begäran om korrigerig eller raderig av personuppgifter ställs till en annan medlemsstat än den ansvariga medlemsstaten ska myndigheterna i den medlemsstat till vilken begäran ställts inom sju dagar kontakta myndigheterna i den ansvariga medlemsstaten och den ansvariga medlemsstaten ska inom 30 dagar från en sådan kontakt kontrollera om uppgifterna är korrekta och om de har behandlats på ett lagligt sätt.
4. Om det, efter en prövning, visar sig att de uppgifter som lagrats i detektorn för multipla identiteter är oriktiga eller har registrerats på ett olagligt sätt, ska den ansvariga medlemsstaten eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts korrigera eller radera dessa uppgifter.
5. Om uppgifter i detektorn för multipla identiteter ändras av den ansvariga medlemsstaten under giltighetstiden, ska den ansvariga medlemsstaten utföra den behandling som avses i artikel 27 och, i förekommande fall, artikel 29 för att avgöra huruvida de ändrade uppgifterna ska länkas. Om behandlingen inte ger någon träff, ska den ansvariga medlemsstaten eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts radera uppgifterna från akten med identitetsbekräftelse. Om den automatiska behandlingen ger en eller flera träffar ska den ansvariga medlemsstaten skapa eller uppdatera den relevanta länken i enlighet med de relevanta bestämmelserna i denna förordning.
6. Om den ansvariga medlemsstaten eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts inte instämmer i att uppgifter som lagrats i detektorn för multipla identiteter är oriktiga eller har registrerats på ett olagligt sätt ska medlemsstaten utan dröjsmål anta ett administrativt beslut med en skriftlig förklaring till den berörda personen om varför den inte är beredd att korrigera eller radera uppgifter som rör honom eller henne.
7. Detta beslut ska även ge den berörda personen information om möjligheten att invända mot det beslut som fattats med avseende på den begäran som avses i punkt 3 och, i tillämpliga fall, information om hur talan kan väckas vid eller klagomål inges till behöriga myndigheter eller domstolar samt möjligheterna till bistånd, även från behöriga nationella tillsynsmyndigheter.
8. En begäran som ställs enligt punkt 3 ska innehålla den information som behövs för att den berörda personen ska kunna identifieras. Denna information ska endast användas för att de rättigheter som avses i punkt 3 ska kunna utövas och ska sedan omedelbart raderas.
9. Den ansvariga medlemsstaten eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts ska spara dokumentation i form av en skriftlig handling om att en begäran som avses i punkt 3 gjorts och hur den behandlats, och ska utan dröjsmål tillhandahålla denna handling till de behöriga nationella tillsynsmyndigheterna med ansvar för dataskydd.

Artikel 48

Överföring av personuppgifter till tredjeländer, internationella organisationer eller privata parter

Personuppgifter som lagras i interoperabilitetskomponenterna eller till vilka interoperabilitetskomponenterna fått åtkomst får inte överföras till eller göras tillgängliga för tredjeländer, internationella organisationer eller privata parter.

Artikel 49

Den nationella tillsynsmyndighetens övervakning

1. Den tillsynsmyndighet eller de tillsynsmyndigheter som utsetts enligt artikel 49 i förordning (EU) 2016/679 ska säkerställa att en granskning av den uppgiftsbehandling som utförs av de ansvariga nationella myndigheterna genomförs i enlighet med relevanta internationella revisionsstandards minst vart fjärde år.
2. Medlemsstaterna ska säkerställa att deras tillsynsmyndighet har de resurser som krävs för att fullgöra de uppgifter som den åläggs enligt denna förordning.

Artikel 50

Europeiska datatillsynsmannens övervakning

Europeiska datatillsynsmannen ska säkerställa att en revision av eu-LISA:s behandling av personuppgifter genomförs i enlighet med relevanta internationella revisionsstandards minst vart fjärde år. En rapport om revisionen ska sändas till Europaparlamentet, rådet, eu-LISA, kommissionen och medlemsstaterna. Eu-LISA ska ges tillfälle att yttra sig innan rapporterna antas.

Artikel 51

Samarbete mellan de nationella tillsynsmyndigheterna och Europeiska datatillsynsmannen

1. Europeiska datatillsynsmannen ska agera i nära samarbete med nationella tillsynsmyndigheter med avseende på särskilda frågor som kräver nationellt deltagande, i synnerhet om Europeiska datatillsynsmannen eller en nationell tillsynsmyndighet upptäcker stora skillnader mellan praxis i medlemsstaterna eller upptäcker eventuellt olagliga överföringar genom interoperabilitetskomponenternas kommunikationskanaler, eller i samband med frågor rörande genomförande och tolkning av denna förordning som tas upp av en eller flera nationella tillsynsmyndigheter.
2. I de fall som avses i punkt 1 ska en samordnad tillsyn säkerställas i enlighet med artikel 62 i förordning (EU) XXXX/2018 [reviderad förordning 45/2001].

KAPITEL VIII

Skyldigheter

Artikel 52

Eu-LISA:s skyldigheter under utformnings- och utvecklingsfasen

1. Eu-LISA ska säkerställa att interoperabilitetskomponenternas centrala infrastrukturer drivs i enlighet med denna förordning.

2. Interoperabilitetskomponenterna ska hysas av eu-LISA vid dess tekniska anläggningar och ska tillhandahålla de funktioner som fastställs i denna förordning i enlighet med de krav på säkerhet, tillgänglighet, kvalitet och hastighet som anges i artikel 53.1.
3. Eu-LISA ska ansvara för interoperabilitetskomponenternas utveckling, för de anpassningar som krävs för att upprätta interoperabilitet mellan de centrala systemen för in- och utresesystemet, VIS, [Etias], SIS, Eurodac och [Ecris-TCN-systemet] och den europeiska sökportalen, den gemensamma biometriska matchningstjänsten, den gemensamma databasen för identitetsuppgifter och detektorn för multipla identiteter.

Eu-LISA ska fastställa utformningen av interoperabilitetskomponenternas fysiska arkitektur inbegripet deras kommunikationsinfrastrukturer och de tekniska specifikationerna och deras utveckling vad gäller den centrala infrastrukturen och den säkra kommunikationsinfrastrukturen, som ska antas av styrelsen, med förbehåll för ett positivt yttrande från kommissionen. Eu-LISA ska också göra alla nödvändiga anpassningar av SIS, Eurodac eller [Ecris-TCN-systemet] som följer av upprättandet av interoperabilitet och som föreskrivs i denna förordning.

Eu-LISA ska utveckla och implementera interoperabilitetskomponenterna så snart som möjligt efter ikraftträdandet av denna förordning och kommissionens antagande av de åtgärder som föreskrivs i artiklarna 8.2, 9.7, 28.5 och 28.6, 37.4, 38.4, 39.5 och 44.5.

Utvecklingen ska bestå i att utarbeta och genomföra de tekniska specifikationerna, testerna och den övergripande projektsamordningen.
4. En förvaltningsgrupp för programmet bestående av högst tio medlemmar ska inrättas under utformnings- och utvecklingsfasen. Den ska bestå av sju medlemmar som eu-LISA:s styrelse utser bland sina ledamöter eller suppleanter, ordföranden för den rådgivande grupp för interoperabilitet som avses i artikel 65, en medlem som företräder eu-LISA och som utses av dess verkställande direktör och en medlem som utses av kommissionen. De medlemmar som utses av eu-LISA:s styrelse ska väljas enbart från de medlemsstater som enligt unionsrätten fullt ut omfattas av de lagstiftningsinstrument som reglerar utveckling, inrättande, drift och användning av samtliga stora it-system som förvaltas av eu-LISA och som kommer att delta i interoperabilitetskomponenterna.
5. Förvaltningsgruppen för programmet ska sammanträda regelbundet och minst tre gånger i kvartalet. Den ska säkerställa en lämplig förvaltning av interoperabilitetskomponenternas utformnings- och utvecklingsfas.

Förvaltningsgruppen för programmet ska varje månad lämna skriftliga rapporter till styrelsen om projektets framsteg. Förvaltningsgruppen för programmet ska varken ha befogenhet att fatta beslut eller mandat att företräda ledamöterna i eu-LISA:s styrelse.
6. Eu-LISA:s styrelse ska fastställa arbetsordningen för förvaltningsgruppen för programmet, vilken särskilt ska innehålla bestämmelser om följande:
 - (a) Ordförandeskap.
 - (b) Mötesplatser.
 - (c) Mötesförberedelser.
 - (d) Tillträde för experter till mötena.

- (e) Kommunikationsplaner som säkerställer fullständig information till icke deltagande ledamöter i styrelsen.

Ordförandeskapet ska innehas av en medlemsstat som enligt unionsrätten fullt ut omfattas av de lagstiftningsinstrument som reglerar utveckling, inrättande, drift och användning av samtliga stora it-system som förvaltas av eu-LISA.

Medlemmarna i förvaltningsgruppen för programmet ska få alla sina utgifter för resa och uppehålle ersatta av byrån, och artikel 10 i eu-LISA:s arbetsordning ska gälla i tillämpliga delar. Eu-LISA ska tillhandahålla ett sekretariat för förvaltningsgruppen.

Den rådgivande grupp för interoperabilitet som avses i artikel 65 ska sammanträda regelbundet till dess att interoperabilitetskomponenterna tas i drift. Den ska rapportera till förvaltningsgruppen för programmet efter varje möte. Den ska tillhandahålla teknisk expertis till stöd för förvaltningsgruppens uppgifter och följa upp medlemsstaternas förberedelser.

Artikel 53

Eu-LISA:s skyldigheter före och efter idrifttagandet

1. Efter det att respektive interoperabilitetskomponent tagits i drift ska eu-LISA ansvara för den tekniska förvaltningen av den centrala infrastrukturen och de enhetliga nationella gränssnitten. I samarbete med medlemsstaterna ska byrån ständigt säkerställa bästa tillgängliga teknik med förbehåll för en kostnads-nyttanalys. Eu-LISA ska också ansvara för den tekniska förvaltningen av den kommunikationsinfrastruktur som avses i artiklarna 6, 12, 17, 25 och 39.

Den tekniska förvaltningen av interoperabilitetskomponenterna ska bestå av alla de arbetsuppgifter som krävs för att interoperabilitetskomponenterna ska kunna fungera dygnet runt alla dagar i veckan i enlighet med denna förordning, särskilt det underhåll och den tekniska utveckling som krävs för att säkerställa att komponenterna fungerar med tillfredsställande teknisk kvalitet, särskilt vad gäller svarstiden vid sökningar i de centrala infrastrukturerna i enlighet med de tekniska specifikationerna.

2. Utan att det påverkar tillämpningen av artikel 17 i tjänsteföreskrifterna för tjänstemän vid Europeiska unionen ska eu-LISA tillämpa lämpliga regler avseende tystnadsplikt eller motsvarande sekretesskrav på all personal som arbetar med uppgifter som lagrats i interoperabilitetskomponenterna. Denna skyldighet ska också gälla efter det att den anställde i fråga lämnat sin tjänst eller anställning eller upphört med sin yrkesverksamhet.
3. Eu-LISA ska utveckla och underhålla en mekanism och förfaranden för att genomföra kvalitetskontroller av de uppgifter som lagras i den gemensamma biometrisk matchningstjänsten och den gemensamma databasen för identitetsuppgifter i enlighet med artikel 37.
4. Eu-LISA ska också utföra uppgifter avseende tillhandahållandet av utbildning om interoperabilitetskomponenternas tekniska användning.

Artikel 54

Medlemsstaternas skyldigheter

1. Varje medlemsstat ska ansvara för följande:
 - (a) Anslutning av den europeiska sökportalen och den gemensamma databasen för

identitetsuppgifter (CIR) till kommunikationsinfrastrukturen.

- (b) Integration av de befintliga nationella systemen och infrastrukturerna med den europeiska sökportalen, den gemensamma biometriska matchningstjänsten, CIR och detektorn för multipla identiteter.
 - (c) Organisation, förvaltning, drift och underhåll av den befintliga nationella infrastrukturen och dess anslutning till interoperabilitetskomponenterna.
 - (d) Förvaltning av och föreskrifter för åtkomst för vederbörligen bemyndigad och vederbörligen befullmäktigad personal vid behöriga nationella myndigheter till den europeiska sökportalen, CIR och detektorn för multipla identiteter i enlighet med denna förordning och upprättandet och regelbunden uppdatering av en förteckning över denna personal och deras profiler.
 - (e) Antagande av de lagstiftningsåtgärder som avses i artikel 20.3 för att få åtkomst till CIR i identifieringssyfte.
 - (f) Den manuella verifiering av olika identiteter som avses i artikel 29.
 - (g) Genomförande av kraven på uppgiftskvalitet i EU-informationssystemen och interoperabilitetskomponenterna.
 - (h) Avhjälpa eventuella brister som konstaterats i kommissionens utvärderingsrapport om uppgifternas kvalitet som avses i artikel 37.5.
2. Varje medlemsstat ska ansluta sina utsedda nationella myndigheter som avses i artikel 4.24 till CIR.

Artikel 54a *Europols skyldigheter*

- 1. Europol ska säkerställa att den europeiska sökportalen behandlar Europoluppgifter i sökningarna och ska i enlighet med detta anpassa sitt gränssnitt Querying Europol Systems (QUEST) till uppgifter med en grundläggande skyddsnivå.
- 2. Europol ska ansvara för förvaltningen av, och föreskrifterna för, vederbörligen bemyndigad personal att använda och få åtkomst till den europeiska sökportalen respektive CIR i enlighet med denna förordning samt upprättandet och regelbunden uppdatering av en förteckning över denna personal och deras profiler.

Artikel 55 *Etias centralenhets skyldigheter*

Etias centralenhet ska ansvara för följande:

- (a) Den manuella verifiering av olika identiteter som avses i artikel 29.
- (b) Genomförande av en spårning av multipla identiteter bland de uppgifter som lagras i VIS, Eurodac och SIS som avses i artikel 59.

KAPITEL IX

Slutbestämmelser

Artikel 56

Rapportering och statistik

1. Den vederbörligen bemyndigade personalen vid medlemsstaternas behöriga myndigheter, kommissionen och eu-LISA ska ha åtkomst för att söka på följande uppgifter avseende den europeiska sökportalen, dock endast för rapporterings- och statistikändamål och utan möjlighet att identifiera enskilda personer:
 - (a) Antalet sökningar per användare av den europeiska sökportalen.
 - (b) – (Ej tillämpligt).
2. Den vederbörligen bemyndigade personalen vid medlemsstaternas behöriga myndigheter, kommissionen och eu-LISA ska ha åtkomst för att söka på följande uppgifter avseende den gemensamma databasen för identitetsuppgifter, dock endast för rapporterings- och statistikändamål och utan möjlighet att identifiera enskilda personer:
 - (a) Antalet sökningar för de syften som avses i artiklarna 20, 21 och 22.
 - (b) Personens medborgarskap, kön och födelseår.
 - (c) Typ av resehandling och kod på tre bokstäver för det utfärdande landet.
 - (d) Antalet sökningar som utförts med och utan biometriska uppgifter.
3. Den vederbörligen bemyndigade personalen vid medlemsstaternas behöriga myndigheter, kommissionen och eu-LISA ska ha åtkomst för att söka på följande uppgifter avseende detektorn för multipla identiteter, dock endast för rapporterings- och statistikändamål och utan möjlighet att identifiera enskilda personer:
 - (a) Personens medborgarskap, kön och födelseår.
 - (a) Typ av resehandling och kod på tre bokstäver för det utfärdande landet.
 - (b) Antalet sökningar som utförts med och utan biometriska uppgifter.
 - (c) Antal länkar per typ.
4. Den vederbörligen bemyndigade personalen vid Europeiska gräns- och kustbevakningsbyrån inrättad genom Europaparlamentets och rådets förordning (EU) 2016/1624⁶⁴ ska ha åtkomst för att söka på de uppgifter som avses i punkterna 1, 2 och 3 i syfte att utföra de riskanalyser och sårbarhetsanalyser som avses i artiklarna 11 och 13 i den förordningen.
5. Vid tillämpningen av punkt 1 i denna artikel ska eu-LISA lagra de uppgifter som avses i punkt 1 i denna artikel i den centrala databas för rapporter och statistik som avses i kapitel VII i denna förordning. De uppgifter som ingår i databasen ska inte möjliggöra identifiering av individer, men de ska göra det möjligt för de myndigheter som förtecknas i punkt 1 i denna artikel att erhålla anpassade rapporter och anpassad statistik för att effektivisera in- och utresekontroller, hjälpa myndigheternas

⁶⁴ 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.

handläggning av viseringsansökningar och stödja evidensbaserat beslutsfattande om migration och säkerhet i unionen.

Artikel 57

Övergångsperiod för användning av den europeiska sökportalen

Under en tvåårsperiod från och med den dag då den europeiska sökportalen tas i drift ska de skyldigheter som avses i artikel 7.2 och 7.4 inte tillämpas och det ska vara frivilligt att använda den europeiska sökportalen.

Artikel 58

Övergångsperiod som är tillämplig på bestämmelserna om åtkomst till den gemensamma databasen för identitetsuppgifter för brottsbekämpande ändamål

Artikel 22 ska tillämpas från och med den dag för idrifttagandet som avses i artikel 62.1.

Artikel 59

Övergångsperiod för spårning av multipla identiteter

1. Under en ettårsperiod efter det att eu-LISA har anmält slutförandet av det test som avses i artikel 62.1 b vad gäller detektorn för multipla identiteter och innan detektorn tagits i drift, ska Etias centralenhet som avses i [artikel 33 a i förordning (EU) 2016/1624] ansvara för att utföra en spårning av multipla identiteter mellan de uppgifter som lagrats i VIS, Eurodac och SIS. Spårningarna av multipla identiteter ska utföras endast med hjälp av biometriska uppgifter i enlighet med artikel 27.2 i denna förordning.
2. Om sökningen ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är identiska eller liknande, ska en vit länk skapas i enlighet med artikel 33.

Om sökningen ger en eller flera träffar och identitetsuppgifterna i de länkade akterna inte kan anses vara liknande, ska en gul länk skapas i enlighet med artikel 30 och det förfarande som avses i artikel 29 ska tillämpas.

Vid flera träffar ska en länk skapas till varje uppgift som gett upphov till träffen.
3. Om en gul länk skapas i enlighet med punkt 3 ska detektorn för multipla identiteter bevilja Etias centralenhet åtkomst till de identitetsuppgifter som finns i de olika informationssystemen.
4. Om det skapas en länk till en registrering i SIS, utom en registrering om nekad inresa eller en registrering om en resehandling som anmälts som försvunnen, stulen eller ogiltig i enlighet med artikel 24 i förordningen om SIS på området in- och utresekontroller respektive artikel 38 i förordningen om SIS på området brottsbekämpning, ska detektorn för multipla identiteter bevilja Sirenekontoret i den medlemsstat som skapade registreringen åtkomst till de identitetsuppgifter som finns i de olika informationssystemen.
5. Etias centralenhet eller Sirenekontoret i den medlemsstat som skapade registreringen ska ha åtkomst till de uppgifter som finns i akten med identitetsbekräftelse och ska bedöma de olika identiteterna samt uppdatera länken i enlighet med artiklarna 31, 32 och 33 och lägga till den i akten med identitetsbekräftelse.
6. Eu-LISA ska vid behov bistå Etias centralenhet med att utföra den spårning av multipla identiteter som avses i denna artikel.

Artikel 60

Kostnader

1. Kostnaderna i samband med inrättandet och driften av den europeiska sökportalen, den gemensamma biometriska matchningstjänsten, den gemensamma databasen för identitetsuppgifter (CIR) och detektorn för multipla identiteter ska belasta unionens allmänna budget.
2. Kostnaderna i samband med integreringen av befintliga nationella infrastrukturer och deras anslutning till de enhetliga nationella gränssnitten samt i samband med förvaltandet av de enhetliga nationella gränssnitten ska belasta unionens allmänna budget.

Följande kostnader ska vara undantagna:

 - (a) Medlemsstaternas projektledningskontor (möten, tjänsteresor, kontor).
 - (b) Hysande av nationella it-system (lokaler, implementering, elektricitet, kylning).
 - (c) Drift av nationella it-system (operatörs- och supportavtal).
 - (d) Utformning, utveckling, implementering, drift och underhåll av nationella kommunikationsnätverk.
3. Kostnaderna för de myndigheter som utsetts i enlighet med artikel 4.24 ska belasta de enskilda medlemsstaterna respektive Europol. Kostnaderna för anslutningen av de utsedda myndigheterna till CIR ska belasta de enskilda medlemsstaterna respektive Europol.

Artikel 61

Underrättelser

1. Medlemsstaterna ska underrätta eu-LISA om de myndigheter som avses i artiklarna 7, 20, 21 och 26 och som får använda eller ha åtkomst till den europeiska sökportalen, CIR respektive detektorn för multipla identiteter.

En konsoliderad förteckning över dessa myndigheter ska offentliggöras i *Europeiska unionens officiella tidning* inom tre månader efter den dag då respektive interoperabilitetskomponent togs i drift i enlighet med artikel 62. Om förteckningen ändras ska eu-LISA en gång om året offentliggöra en uppdaterad konsoliderad förteckning.
2. Eu-LISA ska underrätta kommissionen om att det test som avses i artikel 62.1 b har slutförts på ett framgångsrikt sätt.
3. Etias centralenhet ska underrätta kommissionen om att den övergångsåtgärd som avses i artikel 59 har slutförts på ett framgångsrikt sätt.
4. Kommissionen ska tillhandahålla medlemsstaterna och allmänheten de uppgifter som anmälts enligt punkt 1 genom en ständigt uppdaterad offentlig webbplats.

Artikel 62

Driftsstart

1. Kommissionen ska fastställa vilken dag varje interoperabilitetskomponent ska tas i drift så snart följande villkor har uppfyllts:

- (a) De åtgärder som avses i artiklarna 8.2, 9.7, 28.5 och 28.6, 37.4, 38.4, 39.5 och 44.5 har antagits.
 - (b) Eu-LISA har förklarat att ett övergripande test av den relevanta interoperabilitetskomponenten, vilket ska utföras av eu-LISA i samarbete med medlemsstaterna, har slutförts på ett framgångsrikt sätt.
 - (c) Eu-LISA har godkänt de tekniska och rättsliga föreskrifter som ska gälla för insamling och överföring av de uppgifter som avses i artiklarna 8.1, 13, 19, 34 och 39 och anmält dessa till kommissionen.
 - (d) Medlemsstaterna har underrättat kommissionen i enlighet med artikel 61.1.
 - (e) Vad gäller detektorn för multipla identiteter har Etias centralenhet underrättat kommissionen i enlighet med artikel 61.3.
- 2. Kommissionen ska underrätta Europaparlamentet och rådet om resultaten av de tester som genomförts i enlighet med punkt 1 b.
 - 3. Det kommissionsbeslut som avses i punkt 1 ska offentliggöras i *Europeiska unionens officiella tidning*.
 - 4. Medlemsstaterna och Europol ska börja använda interoperabilitetskomponenterna från och med den dag som fastställts av kommissionen i enlighet med punkt 1.

Artikel 63

Utövande av delegeringen

- 1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
- 2. Den befogenhet att anta delegerade akter som avses i artiklarna 8.2 och 9.7 ska ges till kommissionen tills vidare från och med [*den dag då denna förordning träder i kraft*].
- 3. Den delegering av befogenhet som avses i artiklarna 8.2 och 9.7 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
- 4. Innan kommissionen antar en delegerad akt, ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.
- 5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
- 6. En delegerad akt som antas enligt artiklarna 8.2 och 9.7 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på [två månader] från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med [två månader] på Europaparlamentets eller rådets initiativ.

Artikel 64
Kommittéförfarande

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

Artikel 65
Rådgivande grupp

Eu-LISA ska inrätta en rådgivande grupp som ska bistå byrån med sakkunskap om interoperabilitet, särskilt i samband med utarbetandet av det årliga arbetsprogrammet och den årliga verksamhetsrapporten. Under utformnings- och utvecklingsfasen av interoperabilitetsinstrumenten ska artikel 52.4–6 vara tillämplig.

Artikel 66
Utbildning

Eu-LISA ska utföra uppgifter vad gäller tillhandahållandet av utbildning i den tekniska användningen av interoperabilitetskomponenterna i enlighet med förordning (EU) nr 1077/2011.

Artikel 67
Handbok

Kommissionen ska i nära samarbete med medlemsstaterna, eu-LISA och andra relevanta byråer tillhandahålla en handbok om implementeringen och förvaltningen av interoperabilitetskomponenterna. Handboken ska innehålla tekniska och operativa riktlinjer, rekommendationer och bästa praxis. Kommissionen ska anta handboken i form av en rekommendation.

Artikel 68
Övervakning och utvärdering

1. Eu-LISA ska säkerställa att det finns förfaranden för att övervaka utvecklingen av interoperabilitetskomponenterna mot bakgrund av målen för planering och kostnader samt för att övervaka interoperabilitetskomponenternas funktion mot bakgrund av målen för tekniska resultat, kostnadseffektivitet, säkerhet och tjänsternas kvalitet.
2. Inom [sex månader efter det att denna förordning har trätt i kraft — Publikationsbyrån, ersätt med aktuellt datum] och därefter var sjätte månad under interoperabilitetskomponenternas utvecklingsfas ska eu-LISA lämna en rapport till Europaparlamentet och rådet om hur interoperabilitetskomponenternas utveckling framskrider. Så snart utvecklingsarbetet har slutförts ska en rapport lämnas till Europaparlamentet och rådet med en ingående redogörelse för hur målen för framför allt planering och kostnader har uppfyllts samt vad eventuella avvikelser beror på.
3. Eu-LISA ska ha åtkomst till nödvändig information om den uppgiftsbehandling som utförs i interoperabilitetskomponenterna, vilken behövs för det tekniska underhållet.

4. Fyra år efter det att respektive interoperabilitetskomponent har tagits i drift, och därefter vart fjärde år, ska eu-LISA rapportera till Europaparlamentet, rådet och kommissionen om interoperabilitetskomponenternas tekniska funktion, inbegripet ur säkerhetssynpunkt.
5. Dessutom ska kommissionen ett år efter varje rapport från eu-LISA utarbeta en övergripande utvärdering av komponenterna, inbegripet följande:
 - (a) En bedömning av tillämpningen av denna förordning.
 - (b) En granskning av uppnådda resultat i relation till målen och deras inverkan på de grundläggande rättigheterna.
 - (c) En bedömning av huruvida de förutsättningar som ligger till grund för interoperabilitetskomponenterna fortfarande är giltiga.
 - (d) En bedömning av säkerheten i interoperabilitetskomponenterna.
 - (e) En bedömning av eventuella konsekvenser, inbegripet eventuell oproportionellt stor inverkan på trafikflödet vid gränsövergångsställena, samt budgetkonsekvenser för unionens budget.

Utvärderingen ska omfatta eventuella nödvändiga rekommendationer. Kommissionen ska överlämna utvärderingsrapporten till Europaparlamentet, rådet, Europeiska datatillsynsmannen och Europeiska unionens byrå för grundläggande rättigheter som inrättades genom rådets förordning (EG) nr 168/2007⁶⁵.
6. Medlemsstaterna och Europol ska ge eu-LISA och kommissionen den information som de behöver för att kunna utarbeta de rapporter som avses i punkterna 4 och 5. Denna information får inte äventyra arbetsmetoder eller innehålla uppgifter som röjer de utsedda myndigheternas källor, personal eller utredningar.
7. Eu-LISA ska ge kommissionen den information som den behöver för att kunna utarbeta de utvärderingar som avses i punkt 5.
8. Varje medlemsstat och Europol ska, med respekt för bestämmelserna i nationell rätt om offentliggörande av känsliga uppgifter, utarbeta årliga rapporter om hur effektiv åtkomsten till de uppgifter som lagrats i den gemensamma databasen för identitetsuppgifter varit för brottsbekämpande ändamål, däribland information och statistik om
 - (a) det närmare syftet med sökningarna, däribland vilken typ av terroristbrott eller grovt brott det gällt,
 - (b) välgrundade misstankar om att en person som misstänks för, har begått eller utsatts för ett brott omfattas av Eurodacförordningen,
 - (c) antal begäranden om åtkomst till den gemensamma databasen för identitetsuppgifter för brottsbekämpande ändamål,
 - (d) antalet och den typ av ärenden som har lett till identifieringar,
 - (e) behovet och utnyttjandet av möjligheten att åberopa brådskande undantagsfall, inklusive de fall där brådskande inte godtogs som skäl vid den verifiering i efterhand som genomfördes av den centrala åtkomstpunkten.

⁶⁵ Rådets förordning (EG) nr 168/2007 av den 15 februari 2007 om inrättande av Europeiska unionens byrå för grundläggande rättigheter (EUT L 53, 22.2.2007, s. 1).

Medlemsstaternas och Europols årsrapporter ska översändas till kommissionen senast den 30 juni påföljande år.

Artikel 69
Ikraftträdande och tillämplighet

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

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

Utfärdad i Strasbourg den

På Europaparlamentets vägnar
Ordförande

På rådets vägnar
Ordförande

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

- 1.1. Förslagets eller initiativets beteckning
- 1.2. Berörda politikområden
- 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 av interoperabilitet mellan Europeiska unionens informationssystem för säkerhet, gränser och migrationshantering.

1.2. Berörda politikområden

Inrikes frågor (Avdelning 18)

1.3. Typ av förslag eller initiativ

☒ Ny åtgärd

☐ Ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd⁶⁶

☐ 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*

Gränsförvaltning – att rädda liv och säkra de yttre gränserna

Interoperabilitetskomponenterna skapar möjligheten att bättre använda den information som finns i de befintliga EU-systemen för säkerhet, gränser och migrationshantering. Dessa åtgärder syftar främst till att undvika att samma person registreras i olika system med olika identiteter. För närvarande är det möjligt att göra en unik identifiering av en person inom ett visst system, men inte i flera olika system. Detta kan leda till att myndigheterna fattar felaktiga beslut och det kan utnyttjas av resenärer med oärligt uppsåt för att dölja deras verkliga identitet.

Ett bättre informationsutbyte

De föreslagna åtgärderna gör det också möjligt för brottsbekämpande myndigheter att få en smidigare – men fortfarande begränsad – åtkomst till dessa uppgifter. Här fastställs en enda uppsättning villkor för åtkomst snarare än olika villkor för varje uppgiftssamling, som i dagens läge.

1.4.2. *Specifika mål och specifikt mål nr []*

Inrättandet av interoperabilitetskomponenterna har följande allmänna syften:

- (a) Att förbättra förvaltningen av de yttre gränserna.
- (b) Att bidra till att förebygga och bekämpa irreguljär migration.
- (c) Att bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, bland annat genom att upprätthålla den allmänna säkerheten och allmänna ordningen och trygga säkerheten på medlemsstaternas territorier.

⁶⁶

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

Målet att säkerställa interoperabilitet ska uppnås genom att

- a) säkerställa en korrekt identifiering av personer,
- b) bidra till att bekämpa identitetsbedrägeri,
- c) förbättra och harmonisera EU-informationssystemens krav på uppgiftskvalitet,
- d) underlätta medlemsstaternas tekniska implementering och operativa drift av befintliga och framtida EU-informationssystem,
- e) skärpa, förenkla och enhetliggöra de villkor för datasäkerhet och dataskydd som reglerar respektive EU-informationssystem,
- f) förenkla och enhetliggöra villkoren för åtkomst i brottsbekämpningssyfte till in- och utresesystemet, VIS, Etias och Eurodac,
- g) stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN-systemet.

Berörda verksamheter enligt den verksamhetsbaserade förvaltningen och budgeteringen

Kapitlet Säkerhet och skydd av friheter: inre säkerhet

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.

De allmänna syftena med detta initiativ härstammar från två fördragsbaserade mål:

1. Att förbättra förvaltningen av Schengenområdets yttre gränser, på grundval av den europeiska migrationsagendan och efterföljande meddelanden, bland annat meddelandet om bevarande och stärkande av Schengenområdet.

2. Att bidra till den inre säkerheten i Europeiska unionen, på grundval av den europeiska säkerhetsagendan och kommissionens arbete för en effektiv och verklig säkerhetsunion.

De specifika politiska syftena med detta interoperabilitetsinitiativ anges nedan.

De specifika syftena med detta förslag är följande:

1. Säkerställa att slutanvändare, framför allt gränskontrolltjänstemän, brottsbekämpande tjänstemän, immigrationstjänstemän och rättsliga myndigheter, får snabb, smidig, systematisk och kontrollerad åtkomst till den information de behöver för att utföra sina uppgifter.

2. Tillhandahålla en metod för att spåra multipla identiteter som används med samma biometriska uppgifter, vilket har det dubbla syftet att säkerställa en korrekt identifiering av personer med ärligt uppsåt och bekämpa identitetsbedrägeri.

3. Underlätta polismyndigheternas identitetskontroller av tredjelandsmedborgare på en medlemsstats territorium.

4. Underlätta och rationalisera de brottsbekämpande myndigheternas åtkomst till EU:s informationssystem som inte är utformade för brottsbekämpning, när det är nödvändigt för att förebygga, utreda, upptäcka eller lagföra grov brottslighet och terrorism.

För att uppfylla specifikt mål nr 1 kommer den europeiska sökportalen (ESP) att utvecklas.

För att uppfylla specifikt mål nr 2 kommer detektorn för multipla identiteter (MID) att införas, med stöd av den gemensamma databasen för identitetsuppgifter (CIR) och den gemensamma biometriska matchningstjänsten.

För att uppfylla specifikt mål nr 3 kommer bemyndigade tjänstemän att beviljas åtkomst till CIR för identifiering.

För att uppfylla specifikt mål nr 4 kommer CIR att innehålla en flaggfunktion vid träff som möjliggör en tvåstegsstrategi för åtkomst i brottsbekämpningssyfte till gränsförvaltningssystemen.

Utöver dessa fyra interoperabilitetskomponenter kommer de mål som beskrivs i avsnitt 1.4.2 ytterligare att understödjas genom inrättandet och förvaltningen av det universella meddelandeformatet (UMF) som en EU-standard för utvecklingen av informationssystem på området rättsliga och inrikes frågor samt inrättandet av en central databas för rapporter och statistik (CRRS).

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.

Var och en av de föreslagna åtgärderna kräver utveckling, och därefter underhåll och drift, av den komponenten.

Utvecklingsfasen

Utvecklingen av varje komponent kommer att ske så snart förutsättningarna för detta är uppfyllda, dvs. medlagstiftarna har antagit lagstiftningsförslaget och de tekniska förutsättningarna är uppfyllda, eftersom vissa komponenter endast kan byggas när en annan är tillgänglig.

Specifikt mål: redo för drift senast måldatumet

Förslaget lämnas till medlagstiftarna för antagande i slutet av 2017. Det antas att antagningsprocessen slutförs under 2018, baserat på den tid det tagit för andra förslag.

Utgående från detta antagande anges början av 2019 (= T0) som start för utvecklingsfasen för att ha en referenspunkt från vilken perioder räknas och inte exakta datum. Om medlagstiftarna antar förslaget vid en senare tidpunkt framskjuts hela tidsplanen i enlighet med detta. Å andra sidan måste den gemensamma biometriska matchningstjänsten vara tillgänglig innan CIR och MID kan färdigställas. Utvecklingsperioderna anges i tabellen nedan.

	2019	2020	2021	2022	2023	2024	2025	2026	2027
	Lagstiftnings förslag antaget		Jan 2021 in- och utresesystemets biometriska matchningstjänst tillgänglig						
Programförvaltning									
CRRS									
ESP (Europeiska sökportalen)									
Den gemensamma biometriska matchningstjänsten									
migrering av Eurodac, SIS, Ecris									
CIR (gemensam databas för identitetsuppgifter)									
inkorporering av Eurodac, Ecris i CIR									
MID (detektor för multipla identiteter)									
manuell validering av länkar									

(Gul ruta avser en specifik Eurodacrelaterad uppgift.)

- Den centrala databasen för rapporter och statistik (CRRS): tidsplan: T0 + 12 månader (2019–2020)

- Den europeiska sökportalen (ESP): tidsplan: T0 + 36 månader (2019–2021)

- Den gemensamma biometriska matchningstjänsten skapas först för in- och utresesystemet. När detta delmål uppnåtts måste de applikationer som kommer att använda den gemensamma biometriska matchningstjänsten uppdateras och uppgifterna i SIS automatiska fingeravtrycksidentifieringssystem (Afis), Eurodacs Afis och Ecris-TCN migreras till tjänsten. Målet är att den ska vara klar i slutet av 2023.

- Den gemensamma databasen för identitetsuppgifter (CIR) skapas först under implementeringen av in- och utresesystemet. När in- och utresesystemet är klart införlivas uppgifterna från Eurodac och Ecris i CIR. Målet är att den ska vara klar i slutet av 2022 (tillgång till den gemensamma biometriska matchningstjänsten + 12 månader).

- Detektorn för multipla identiteter (MID) skapas efter det att CIR har tagits i drift. Målet är att den ska vara klar i slutet av 2022 (tillgång till den gemensamma biometriska matchningstjänsten + 24 månader), men sedan följer en mycket

resurskrävande period då länkar mellan identiteter som föreslås av MID ska valideras. Varje potentiell länk måste valideras manuellt. Detta pågår till slutet av 2023.

Detektorn tas i drift när utvecklingsfasen har slutförts.

Driftsfasen

Indikatorer som avser varje specifikt mål som anges i 1.4.3 är följande:

1. Specifikt mål: Snabb, smidig och systematisk bemyndigad åtkomst till datakällor
 - Antal användningsfall som utförts (= antal sökningar som kan hanteras av ESP) per tidsperiod.
 - Antal sökningar som hanterats av ESP jämfört med det totala antalet sökningar (via ESP och direkt i systemen) per tidsperiod.
2. Specifikt mål: Upptäcka multipla identiteter
 - Antal identiteter länkade till samma uppsättning biometriska uppgifter jämfört med antalet identiteter med biografiska uppgifter per tidsperiod.
 - Antal upptäckta fall av identitetsbedrägeri jämfört med antalet länkade identiteter och det totala antalet identiteter per tidsperiod.
3. Specifikt mål: Underlätta identifiering av tredjelandsmedborgare
 - Antal identitetskontroller som gjorts jämfört med det totala antalet transaktioner per tidsperiod.
4. Specifikt mål: Underlätta bemyndigad åtkomst till datakällor för brottsbekämpande ändamål
 - Antal åtkomster i steg 1 (= kontroll av förekomst av uppgifter) för brottsbekämpande ändamål per tidsperiod.
 - Antal åtkomster i steg 2 (= faktiskt konsultering av uppgifter från EU-systemen inom tillämpningsområdet) för brottsbekämpande ändamål per tidsperiod.
5. Övergripande, ytterligare mål: Förbättra kvaliteten på och användningen av uppgifter för bättre beslutsfattande
 - Regelbundet utarbetande av rapporter om kvalitetskontroll av uppgifter.
 - Antal särskilda ansökningar om statistiska uppgifter per tidsperiod.

1.5. Motivering till förslaget eller initiativet

1.5.1. Behov som ska tillgodoses på kort eller lång sikt

Som förklaras i den konsekvensbedömning som åtföljer detta lagstiftningsförslag är varje föreslagen komponent nödvändig för att uppnå interoperabilitet:

- För att uppfylla målet att ge bemyndigade användare snabb, smidigt, systematisk och kontrollerad åtkomst till relevanta informationssystem bör man inrätta en europeisk sökportal (ESP) som bygger på en gemensam biometrisk matchningstjänst så att alla databaser beaktas.
- För att uppfylla målet att underlätta bemyndigade tjänstemäns kontroller av tredjelandsmedborgares identitet på en medlemsstats territorium bör man inrätta en

gemensam databas för identitetsuppgifter (CIR) som innehåller en minimiuppsättning av identitetsuppgifter och som bygger på samma gemensamma biometriska matchningstjänst.

- För att uppfylla målet att spåra multipla identiteter som används med samma biometriska uppgifter, i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri, bör man bygga en detektor för multipla identiteter (MID) som innehåller länkar mellan olika identiteter mellan systemen.
- För att uppfylla målet att underlätta och rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning, i syfte att förebygga, utreda, upptäcka eller lagföra grov brottslighet och terrorism, bör en flaggfunktion vid träff inkluderas i den gemensamma databasen för identitetsuppgifter (CIR).

Eftersom alla målen ska uppfyllas är den kompletta lösningen en kombination av ESP, CIR (med flagga vid träff) och MID, som alla bygger på den gemensamma biometriska matchningstjänsten.

- 1.5.2. *Mervärdet av en åtgärd på unionsnivå (som kan beror på flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökat effektivitet eller komplementaritet). Med "mervärdet av en åtgärd på unionsnivå" menas det värde en unionsinsats tillför som går utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.*

Det krävs åtgärder på unionsnivå eftersom de system som föreslås bli interoperabla används av flera medlemsstater; antingen alla medlemsstater (Eurodac) eller alla medlemsstater som ingår i Schengenområdet (in- och utresesystemet, VIS, Etias och SIS). Per definition kan åtgärder helt enkelt inte vidtas på någon annan nivå.

Det största mervärdet förväntas i fråga om att undanröja fall av identitetsbedrägeri, kartlägga fall där en person har använt olika identiteter för att resa in i EU och undvika att personer med ärligt uppsåt förväxlas med personer med samma namn och oärligt uppsåt. Ett ytterligare mervärde ligger i att den interoperabilitet som föreslås här underlättar implementeringen och underhållet av stora it-system på EU-nivå. För de brottsbekämpande myndigheterna torde de föreslagna åtgärderna leda till att de oftare får faktisk åtkomst till specifika uppgifter i EU:s stora it-system. På operativ nivå kan uppgifternas kvalitet endast upprätthållas och förbättras om den övervakas. För politik och beslutsfattande finns det dessutom ett behov av att kunna göra ad hoc-sökningar i anonymiserade uppgifter.

Enligt den kostnads-nyttoanalys som ingår i konsekvensbedömningen kan de förväntade fördelarna, om man bara räknar sådana som kan kvantifieras, rimligen uppskattas till omkring 77,5 miljoner EUR per år och främst tillfalla medlemsstaterna. Dessa fördelar härrör framför allt från följande:

- Minskade kostnader för ändringar i de nationella applikationerna när det centrala systemet är i drift (uppskattningsvis 6 miljoner EUR per år för medlemsstaternas it-avdelningar).
- Kostnadsbesparingar som följer av att endast ha en central gemensam biometrisk matchningstjänst snarare än en sådan för varje centralt system som innehåller biometriska uppgifter (uppskattningsvis 1,5 miljoner EUR per år och en engångsbesparing på 8 miljoner EUR för eu-LISA).

- Kostnadsbesparingar för identifiering av multipla identiteter jämfört med en situation där samma resultat skulle uppnås utan de föreslagna verktygen. Detta skulle innebära en kostnadsbesparing på åtminstone 50 miljoner EUR per år för medlemsstaternas myndigheter för gränsförvaltning, migration och brottsbekämpning.
- Inbesparade utbildningskostnader för en stor grupp av slutanvändare jämfört med en situation som kräver utbildning på återkommande basis; uppskattningsvis 20 miljoner EUR per år för medlemsstaternas myndigheter för gränsförvaltning, migration och brottsbekämpning.

1.5.3. *Huvudsakliga erfarenheter från liknande försök eller åtgärder*

Utvecklingen av andra generationen av Schengens informationssystem (SIS II) och Informationssystemet för viseringar (VIS) har gett följande erfarenheter:

1. För att skydda sig mot merkostnader och förseningar till följd av ändrade krav bör arbetet med att utveckla nya informationssystem på området frihet, säkerhet och rättvisa, särskilt om det rör sig om ett stort it-system, inte starta förrän man slutgiltigt har antagit de underliggande rättsliga instrument som fastställer systemets syfte, tillämpningsområde och funktioner samt de tekniska detaljerna.
2. För SIS II och VIS kunde medlemsstaternas nationella utvecklingsarbete medfinansieras inom Fonden för yttre gränser (EBF), men detta var inte obligatoriskt. Det gick därför inte att få någon överblick över hur långt arbetet kommit i de medlemsstater som inte hade planerat sin verksamhet i en flerårsplanering eller som inte varit tillräckligt precisa i sin planering. Mot denna bakgrund föreslås det nu att kommissionen ska ersätta medlemsstaternas samtliga integrationskostnader för att därmed också kunna följa hur utvecklingen framskrider.
3. I syfte att underlätta den allmänna samordningen av implementeringen kommer alla föreslagna utbyten av meddelanden mellan de nationella och centrala systemen att återanvända befintliga nätverk och det enhetliga nationella gränssnittet.

1.5.4. *Förenlighet med andra finansieringsformer och eventuella synergieffekter*

Förenlighet med den gällande fleråriga budgetramen

Förordningen om fonden för inre säkerhet och stödet för yttre gränser är det finansieringsinstrument som innehåller budgeten för genomförande av interoperabilitetsinitiativet.

I artikel 5 b anges att 791 miljoner EUR ska användas genom ett program för utveckling av it-system på grundval av befintliga och/eller nya system som stöd för hanteringen av migrationsströmmar över de yttre gränserna, med förbehåll för att de relevanta unionslagstiftningsakterna antas och på de villkor som avses i artikel 15. Av dessa 791 miljoner EUR är 480,2 miljoner EUR avsatta för utvecklingen av in- och utresesystemet, 210 miljoner EUR för Etias och 67,9 miljoner EUR för översynen av SIS II. Återstoden (32,9 miljoner EUR) ska omfördelas genom mekanismerna inom fonden för inre säkerhet – gränser och viseringar. Det föreliggande förslaget kräver 32,1 miljoner EUR för den nuvarande fleråriga budgetramperioden, vilket är förenligt med den återstående budgeten.

Det föreliggande förslaget kräver totalt 424,7 miljoner EUR i budgetmedel (inklusive rubrik 5) under perioden 2019–2027. Den nuvarande fleråriga budgetramen sträcker sig bara över de två åren 2019 och 2020. Kostnaderna har dock uppskattats ända

fram till 2027 för att ge en bättre bild av förslaget ekonomiska konsekvenser, utan att föregripa nästa fleråriga budgetram.

Den budget som begärts för nio år uppgår till 424,7 miljoner EUR eftersom även följande punkter ingår:

- 1) 136,3 miljoner EUR till medlemsstaterna för att täcka de ändringar i deras nationella system som krävs för att använda interoperabilitetskomponenterna, det enhetliga nationella gränssnitt som eu-LISA levererar och en budget för utbildning av det betydande antalet slutanvändare. Detta påverkar inte den nuvarande fleråriga budgetramen då finansieringen tillhandahålls från och med 2021.
- 2) 4,8 miljoner EUR till Europeiska gräns- och kustbevakningsbyrån för att ta emot en grupp specialister som under ett år (2023) kommer att validera länkarna mellan identiteter vid den tidpunkt då detektorn för multipla identiteter tas i bruk. Gruppens verksamhet motsvarar den dubbelkontroll av identitet som åläggs Europeiska gräns- och kustbevakningsbyrån i förslaget om Etias. Detta påverkar inte den nuvarande fleråriga budgetramen då finansieringen tillhandahålls från och med 2021.
- 3) 48,9 miljoner EUR till Europol för att täcka uppgraderingen av kapaciteten hos byråns it-system att hantera mängden meddelanden och den ökande prestandanivån. Interoperabilitetskomponenterna kommer att användas av Etias för att konsultera Europoluppgifter. Europolis nuvarande kapacitet att hantera information är emellertid inte förenlig med de betydande volymerna (i genomsnitt 100 000 sökningar per dag) och den kortare svarstiden. 9,1 miljoner EUR spenderas under den nuvarande fleråriga budgetramen.
- 4) 2,0 miljoner EUR till Cefop för att täcka utarbetande och tillhandahållande av utbildning för operativ personal. 0,1 miljon EUR beräknas för 2020.
- 5) 225,0 miljoner EUR till eu-LISA, vilket täcker de totala programkostnaderna för utvecklingen av de fem interoperabilitetskomponenterna (68,3 miljoner EUR), underhållskostnaderna från leveransen av komponenterna fram till 2027 (56,1 miljoner EUR), en särskild budget på 25 miljoner EUR för migrering av uppgifter från befintliga system till den gemensamma biometrisk matchningstjänsten och de extra kostnaderna för uppdateringen av det enhetliga nationella gränssnittet, nätverk, utbildning och möten. En särskild budget på 18,7 miljoner EUR täcker kostnaderna för uppgradering och drift av Ecris-TCN med hög tillgänglighet från och med 2022. Av det totala beloppet spenderas 23,0 miljoner EUR under den nuvarande fleråriga budgetramen.
- 6) 7,7 miljoner EUR till GD Migration och inrikes frågor för att täcka en begränsad personalökning och därmed sammanhängande kostnader under utvecklingen av de olika komponenterna, eftersom kommissionen också tar ansvaret för det utskott som sköter det universella meddelandeformatet. Denna budget som faller under rubrik 5 kommer inte att täckas av budgeten för fonden för inre säkerhet. Till kännedom ska 2,0 miljoner EUR betalas under perioden 2019–2020.

Förenlighet med tidigare initiativ

Detta initiativ är förenligt med följande:

I april 2016 lade kommissionen fram sitt **meddelande Starkare och smartare informationssystem för gränser och säkerhet**, för att lyfta fram ett antal strukturella brister i informationssystemen. Detta har lett till följande tre åtgärder:

För det första har kommissionen vidtagit **åtgärder för att stärka och maximera fördelarna med de befintliga informationssystemen**. I december 2016 antog kommissionen förslag för att ytterligare stärka Schengens informationssystem (SIS) i dess nuvarande form. Under tiden har förhandlingarna framskridit om kommissionens förslag från maj 2016 om en översyn av den rättsliga grunden för Eurodac – EU:s databas för fingeravtryck från asylsökande. Ett förslag till en ny rättslig grund för Informationssystemet för viseringar (VIS) håller också på att utarbetas och kommer att läggas fram under andra kvartalet 2018.

För det andra har kommissionen föreslagit **ytterligare informationssystem för att komma till rätta med de konstaterade luckorna** i EU:s uppgiftshanteringsstruktur. Förhandlingarna om kommissionens förslag från april 2016 om att inrätta ett in- och utresesystem⁶⁷ – för att förbättra gränskontrollförfarandena för tredjelandsmedborgare som reser till EU – slutfördes redan i juli 2017, då medlagstiftarna nådde en politisk överenskommelse, som bekräftades av Europaparlamentet i oktober 2017 och formellt antogs av rådet i november 2017. I november 2016 lade kommissionen också fram ett förslag om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias)⁶⁸. Förslaget syftar till att stärka säkerhetskontrollerna av viseringsbefriade resande genom att möjliggöra förhandskontroll av irreguljär migration och säkerhetsrisker. Medlagstiftarnas förhandlingar pågår som bäst. I juni 2017 föreslogs även det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN-systemet)⁶⁹ för att åtgärda den lucka som konstaterats när det gäller informationsutbyte mellan medlemsstaterna om dömda tredjelandsmedborgare.

För det tredje har kommissionen arbetat för att **uppnå interoperabilitet mellan informationssystem**, med inriktning på de fyra alternativen i meddelandet från april 2016⁷⁰. Tre av de fyra alternativen är faktiskt den europeiska sökportalen (ESP), den gemensamma databasen för personuppgifter (CIR) och den gemensamma biometriska matchningstjänsten. I efterhand blev det tydligt att en åtskillnad måste göras mellan CIR som en databas över identiteter och en ny komponent som identifierar multipla identiteter som är kopplade till samma biometriska kännetecken (MID). De fyra komponenterna är därmed nu ESP, CIR, MID och den gemensamma biometriska matchningstjänsten.

Synergier

Med synergier avses här de fördelar som vinnas genom att man återanvänder befintliga lösningar och undviker nya investeringar på alla plan.

Det finns betydande synergier mellan dessa initiativ och utvecklingen av in- och utresesystemet och Etias.

För att in- och utresesystemet ska fungera skapas en personakt för varje tredjelandsmedborgare som reser in i Schengenområdet för en kortare vistelse. För detta ändamål ska det nuvarande system som används för biimetrisk matchning i VIS och som innehåller fingeravtrycksmallar för alla resenärer som måste ha visering utvidgas till att även omfatta biometriska uppgifter från viseringsbefriade resenärer.

⁶⁷ COM(2016) 194 av den 6 april 2016.

⁶⁸ COM(2016) 731 av den 16 november 2016.

⁶⁹ COM(2017) 344 av den 29 juni 2017.

⁷⁰ COM(2016) 205 av den 6 april 2016.

Den gemensamma biometriska matchningstjänsten är alltså konceptuellt sett en ytterligare generalisering av den biometriska matchningsfunktion som kommer att byggas som en del av in- och utresesystemet. De biometriska mallar som ingår i den biometriska matchningsfunktionen för SIS och Eurodac kommer sedan att migreras (detta är den tekniska termen för att överföra data från ett system till ett annat) till den gemensamma biometriska matchningstjänsten. Enligt leverantörens uppgifter kostar lagring i separata databaser i genomsnitt 1 EUR per biometrisk uppsättning (det finns potentiellt 200 miljoner datauppsättningar totalt) medan de genomsnittliga kostnaderna sjunker till 0,35 EUR per biometrisk uppsättning när en gemensam biometrisk matchningstjänst skapas. De högre kostnaderna för den maskinvara som krävs för en stor datavolym utjämnar delvis dessa fördelar, men i slutändan beräknas kostnaderna för en gemensam biometrisk matchningstjänst vara 30 % lägre än när samma uppgifter lagras i flera mindre biometriska matchningssystem.

För att Etias ska fungera måste en komponent finnas tillgänglig för sökningar i flera EU-system. Antingen används ESP eller så byggs en specifik komponent som en del av förslaget om ESP. Förslaget om interoperabilitet gör det möjligt att bygga en komponent i stället för två.

Synergi uppnås även genom återanvändning av samma enhetliga nationella gränssnitt som används för in- och utresesystemet och Etias. Det enhetliga nationella gränssnittet måste uppdateras men kommer att användas även i fortsättningen.

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**

– Efter en utvecklingsfas under 2019–2023 beräknas genomförandetakten nå en stabil nivå.

– Därför anges att åtgärden kommer att pågå och påverka resursanvändningen under perioden 2019–2027.

1.7. Planerad metod för genomförandet⁷¹

☒ **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

Block	Utvecklingsfas	Driftsfas	Förvaltningsmetod	Aktör
-------	----------------	-----------	-------------------	-------

⁷¹

Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb:

<https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

Block	Utvecklingsfas	Driftsfas	Förvaltningsmetod	Aktör
Utveckling och underhåll (av interoperabilitetskomponenter för de centrala systemen, systemutbildning)	X	X	Indirekt	eu-LISA Europol Cepol
Datamigrering (migrering av biometriska mallar till en gemensam biometrisk matchningstjänst), nätverkskostnader, uppdatering av det enhetliga nationella gränssnittet, möten och utbildning	X	X	Indirekt	eu-LISA
Validering av länkar när MID skapas	X	-	Indirekt	Europeiska gräns- och kustbevakningen
Anpassning av det enhetliga nationella gränssnittet, integration av nationella system och utbildning av slutanvändare	X	X	Delad (eller direkt) (1)	Kommissionen + Medlemsstaterna

(1) Inga belopp ingår i detta instrument för driftsfasen.

Utvecklingsperioden börjar 2019 och pågår fram till leveransen av varje komponent, från 2019 till 2023 (se avsnitt 1.4.4).

1. Direkt förvaltning som sköts av GD Migration och inrikes frågor: Under utvecklingsperioden kan åtgärder vid behov också vidtas direkt av kommissionen. Detta kan framför allt gälla unionens ekonomiska stöd till verksamhet i form av bidrag (inklusive bidrag till medlemsstaternas nationella myndigheter), offentlig upphandling och/eller återbetalning av kostnader som externa experter ådrar sig.

2. Delad förvaltning: Under utvecklingsfasen kommer medlemsstaterna att behöva anpassa sina nationella system för åtkomst till den europeiska sökportalen i stället för de enskilda systemen (för utgående meddelanden från medlemsstaterna) och för ändringar av svaren på deras begäranden om sökningar (inkommande meddelanden till medlemsstaterna). Även det enhetliga nationella gränssnitt som införts för in- och utresesystemet och Etias kommer att uppdateras.

3. Indirekt förvaltning: Eu-LISA kommer att sköta utvecklingen av alla it-delar av projektet, dvs. interoperabilitetskomponenterna, uppdateringen av det enhetliga nationella gränssnittet i varje medlemsstat, uppdateringen av infrastrukturen för kommunikation mellan de centrala systemen och de enhetliga nationella gränssnitten, migreringen av biometriska mallar från de

befintliga biometriska matchningssystemen i SIS och Eurodac till den gemensamma biometriska matchningstjänsten samt den uppgiftsrensning som hör samman med detta.

Under driftperioden kommer eu-LISA att sköta all teknisk verksamhet som hör samman med underhållet av komponenterna.

Europeiska gräns- och kustbevakningsbyrån kommer att inrätta ett nytt team som ansvarar för att validera länkar så snart MID tas i drift. Denna uppgift gäller en begränsad tid.

Europol kommer att sköta utvecklingen och underhållet av sina system för att säkerställa interoperabilitet mellan ESP och Etias.

Cepol utformar och tillhandahåller utbildning till de operativa avdelningarna genom fortbildningskurser för utbildare.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder

Övervaknings- och rapporteringsregler för utveckling och underhåll av andra system:

1. Eu-LISA ska säkerställa att det finns förfaranden för att övervaka utvecklingen av interoperabilitetskomponenterna mot bakgrund av målen för planering och kostnader samt för att övervaka komponenternas funktion mot bakgrund av målen för tekniska resultat, kostnadseffektivitet, säkerhet och tjänsternas kvalitet.

2. Inom sex månader efter det att denna förordning har trätt i kraft och därefter var sjätte månad under komponenternas utvecklingsfas ska eu-LISA lämna en rapport till Europaparlamentet och rådet om hur utvecklingen av varje komponent framskrider. Så snart utvecklingsarbetet har slutförts ska en rapport lämnas till Europaparlamentet och rådet med en ingående redogörelse för hur målen för framför allt planering och kostnader har uppfyllts samt vad eventuella avvikelser beror på.

3. Eu-LISA ska ha åtkomst till den information om uppgiftsbehandling i komponenterna som behövs för det tekniska underhållet.

4. Fyra år efter driftsättningen av den sista komponent som implementerats, och vart fjärde år därefter, ska eu-LISA tillstålla Europaparlamentet, rådet och kommissionen en rapport om komponenternas tekniska funktion.

5. Fem år efter driftsättningen av den sista komponent som implementerats, och vart fjärde år därefter, ska kommissionen utarbeta en övergripande utvärdering och lämna nödvändiga rekommendationer. Denna övergripande utvärdering ska omfatta de resultat som uppnåtts med hjälp av komponenterna avseende målet med interoperabilitet, underhållsmässighet, prestanda och ekonomiska konsekvenser samt deras inverkan på de grundläggande rättigheterna.

Kommissionen ska överlämna utvärderingsrapporten till Europaparlamentet och rådet.

6. Medlemsstaterna och Europol ska förse eu-LISA och kommissionen med de uppgifter som krävs för att de rapporter som avses i punkterna 4 och 5 ska kunna utarbetas i enlighet med de kvantitativa indikatorer som fastställts på förhand av kommissionen och/eller eu-LISA. Denna information får inte äventyra arbetsmetoder eller innehålla uppgifter som röjer källor, personalens identitet eller de utsedda myndigheternas utredningar.

7. Eu-LISA ska ge kommissionen den information som den behöver för att kunna utarbeta de övergripande utvärderingar som avses i punkt 5.

8. Varje medlemsstat och Europol ska, med iakttagande av bestämmelserna i nationell rätt om offentliggörande av känsliga uppgifter, utarbeta årliga rapporter om hur effektiv åtkomsten till EU-system har varit för brottsbekämpande ändamål, vilka ska innehålla information och statistik om

- det närmare syftet med sökningarna, däribland vilken typ av terroristbrott eller grovt brott det gällt,

- välgrundade misstankar om att en person som misstänks för, har begått eller utsatts för ett brott omfattas av denna förordning,

- antal begäranden om åtkomst till komponenterna för brottsbekämpande ändamål,
- antalet och den typ av ärenden som har lett till identifieringar,
- behovet och utnyttjandet av möjligheten att åberopa brådskande undantagsfall, inklusive de fall där brådskande inte godtogs som skäl vid den kontroll i efterhand som genomfördes av den centrala åtkomstpunkten.

Medlemsstaternas och Europols årsrapporter ska översändas till kommissionen senast den 30 juni påföljande år.

2.2. Administrations- och kontrollsystem

2.2.1. Risker som identifierats

Riskerna är de som hänger samman med it-utvecklingen av fem komponenter verkställd av en extern entreprenör under översyn av eu-LISA. De är typiska projektrisker:

1. Risken för att projektet inte slutförs i tid.
2. Risken för att projektet inte slutförs inom budgeten.
3. Risken för att projektets hela omfattning inte förverkligas.

Den första risken är den mest betydande, eftersom en försening leder till högre kostnader då de flesta kostnader har en koppling till varaktighet, såsom personalkostnader, licenskostnader per år osv.

Dessa risker kan minskas genom att tillämpa projektledningsmetoder, beakta omkostnader i utvecklingsprojekt och ha tillräcklig personal för att kunna absorbera arbetstoppar. Beräkningen av insatser görs vanligen genom att man antar att arbetsbördan fördelas jämnt över en längre tid, medan det vid projekt i praktiken är så att ojämn arbetsbelastning absorberas av högre resurstilldelning.

Det finns flera risker med att använda en extern entreprenör för detta utvecklingsarbete.

1. Framför allt finns det en risk för att entreprenören inte anslår tillräckliga resurser till projektet eller utformar och utvecklar ett system som inte är tillräckligt modernt.
2. Det finns risk för att förvaltningsförfaranden och metoder för att hantera stora it-projekt inte respekteras fullt ut på grund av att entreprenören försöker minska kostnaderna.
3. Det går slutligen inte heller att utesluta att entreprenören kan komma att drabbas av ekonomiska svårigheter som inte har med projektet att göra.

Dessa risker minskas genom att tilldela kontrakt på grundval av hållbara kvalitetskriterier, kontrollera entreprenörernas referenser och upprätthålla starka förbindelser med dem. Som en sista utväg kan slutligen kraftiga sanktions- och uppsägningsklausuler införas och tillämpas vid behov.

2.2.2. Uppgifter om det interna kontrollsystemet

Det är meningen att eu-LISA ska vara ett kompetenscentrum på området utveckling och förvaltning av stora it-system. Byrån ska sköta den verksamhet som hänger samman med utvecklingen och driften av de olika interoperabilitetskomponenterna, bland annat underhåll av det enhetliga nationella gränssnittet i medlemsstaterna.

Under utvecklingsfasen kommer allt utvecklingsarbete att utföras av eu-LISA. Detta täcker utvecklingen av alla delar av projektet. De kostnader som härrör från integration av systemen i medlemsstaterna under utvecklingen kommer att hanteras av kommissionen via delad förvaltning eller via bidrag.

Under driftsfasen kommer eu-LISA att ha ansvaret för den tekniska och ekonomiska förvaltningen av de komponenter som används centralt, i synnerhet tilldelningen och förvaltningen av kontrakt. Kommissionen kommer att hantera bidragen till medlemsstaterna för kostnader avseende de nationella enheterna via fonden för inre säkerhet – gränser (nationella program).

För att undvika förseningar på nationell nivå ska en effektiv styrning planeras mellan alla berörda aktörer före inledningen av utvecklingsfasen. Kommissionen utgår från en interoperabilitetsarkitektur som ska fastställas i början av projektet för att användas i projekten in- och utresesystemet och Etias, eftersom dessa projekt resulterar i och utnyttjar den gemensamma biometrisk matchningstjänsten, den gemensamma databasen för identitetsuppgifter och den europeiska sökportalen. En medlem av ledningsgruppen för interoperabilitetsprojektet bör ingå i styrningsstrukturen för projekten in- och utresesystemet och Etias.

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

Ingen beräkning anges, eftersom riskkontroll och begränsning av risker ingår i projektledningsstrukturen.

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 bedrägeri, korruption och andra rättsstridiga handlingar ska förordning (EG) nr 1073/1999 gälla.
2. Byråerna 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 byråerna.
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 byråerna 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 HOME:s strategi för bekämpning och upptäckt av bedrägerier kommer att tillämpas.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

DE BERÄKNADE KONSEKVENSERNA PÅ UTGIFTER OCH PERSONAL FÖR ÅR 2021 OCH FRAMÅT INKLUDERAS I DENNA FINANSIERINGSÖVERSIKT I ILLUSTRERANDE SYFTE OCH FÖREGRIPER INTE NÄSTA FLERÅRIGA BUDGETRAM.

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			
	Nummer [Beteckning.....]	Diff./Icke-diff. ⁷²	från Efta-länder ⁷³	från kandidat-länder ⁷⁴	från tredje-länder	enligt artikel 21.2 b i budget-förordningen
3	18.02.01.03 – Smarta gränser	Diff.	Nej	Nej	Ja	Nej
3	18.02.03 – Europeiska gräns- och kustbevakningsbyrå (Frontex)	Diff.	Nej	Nej	Ja	Nej
3	18.02.04 – Europol	Diff.	Nej	Nej	Nej	Nej
3	18.02.05 – Cepol	Icke-diff.	Nej	Nej	Nej	Nej
3	18.02.07 – Europeiska byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA)	Diff.	Nej	Nej	Ja	Nej

⁷² Differentierade respektive icke-differentierade anslag.

⁷³ Efta: Europeiska frihandelssammanslutningen.

⁷⁴ Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad inverkan på utgifterna

[Dessa uppgifter ska anges på [databladet för budgetuppgifter av administrativ natur](#) (andra dokumentet i bilagan till denna finansieringsöversikt), vilket ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.]

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	3	Säkerhet och medborgarskap
------------------------------------	---	----------------------------

GD Migration och inrikes frågor			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	År 2028	TO TALT
• Driftsanslag													
18.02.01.03 – Smarta gränser	Åtaganden	(1)	0	0	43,150	48,150	45,000	0	0	0	0	0	136,300
	Betalningar	(2)	0	0	34,520	47,150	45,630	9,000	0	0	0	0	136,300
Anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program ⁷⁵													
Budgetrubrik (nr)		(3)											
TOTALA anslag för GD Migration och inrikes frågor	Åtaganden	=1+1a +3	0	0	43,150	48,150	45,000	0	0	0	0	0	136,300
	Betalningar	=2+2a +3	0	0	34,520	47,150	45,630	9,000	0	0	0	0	136,300

Utgifterna ska täcka kostnader för följande:

⁷⁵ Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

- Kostnaderna för att anpassa det enhetliga nationella gränssnittet, vars utveckling finansieras inom ramen för förslaget om in- och utresesystemet, ett budgeterat belopp för ändringar av systemen i medlemsstaterna för att ta hänsyn till ändringarna av de centrala systemen och ett budgeterat belopp för utbildning av slutanvändare.

18.0203 – Europeiska gräns- och kustbevakningen			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
Rubrik 1: Personalkostnader	Åtaganden	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Betalningar	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Rubrik 2: Infrastruktur och driftsutgifter	Åtaganden	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Betalningar	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Rubrik 3: Driftsutgifter	Åtaganden	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Betalningar	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
TOTALA anslag för Europol	(summa åtaganden = summa betalningar)	= 1+1a +3a	0	0	0	0,776	4,744	0,402	0	0	0	5,923

- Budgeten för Europeiska gräns- och kustbevakningen täcker utgifterna för ett team som ska validera länkar som genererats av MID (detektorn för multipla identiteter) utgående från befintliga uppgifter (omkring 14 miljoner uppgifter). Det uppskattas att omkring 550 000 länkar ska valideras manuellt. Det särskilda team som inrättas för detta ändamål läggs till det team som inrättades för Etias inom Europeiska gräns- och kustbevakningen, eftersom de har liknande funktioner och man därigenom undviker kostnaderna för att inrätta ett helt nytt team. Arbetet förväntas utföras under 2023. Kontraktsanställda rekryteras därför upp till tre månader i förväg och deras kontrakt avslutas upp till två månader efter att migreringen är klar. En annan del av de resurser som krävs rekryteras enligt planerna inte som kontraktsanställda utan anställs som konsulter. Detta förklarar kostnaderna under rubrik 3 för 2023. Tanken är att de anställs en månad i förväg. Närmare uppgifter om bemanningen tillhandahålls senare.
- Rubrik 1 inbegriper därför kostnaderna för 20 internt anställda och en förstärkning av lednings- och stödpersonal.
- Rubrik 2 inbegriper ytterligare kostnader för att ta emot de 10 extra anställda från entreprenören.

- Rubrik 3 inbegriper utgifterna för de 10 extra anställda från entreprenören. Inga andra typer av kostnader ingår.

18.0204 – Europol			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
Rubrik 1: Personalkostnader	Åtaganden	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Betalningar	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Rubrik 2: Infrastruktur och driftsutgifter	Åtaganden	(1a)	0	0	0	0	0	0	0	0	0	0
	Betalningar	(2a)	0	0	0	0	0	0	0	0	0	0
Rubrik 3: Driftsutgifter	Åtaganden	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Betalningar	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
TOTALA anslag för Europol	(summa åtaganden = summa betalningar)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Europols utgifter täcker uppgraderingen av IKT-systemens kapacitet att hantera volymen av meddelanden som ska hanteras och den ökade prestanda som krävs (svarstid).

Personalutgifterna under rubrik 1 täcker kostnaderna för den ytterligare IKT-personal som ska rekryteras för att stärka Europols informationssystem av de orsaker som beskrivs ovan. Närmare detaljer om fördelningen av tjänster mellan tillfälligt anställda och kontraktsanställda och deras sakkunskap anges nedan.

Rubrik 3 omfattar kostnader för den maskinvara och programvara som behövs för att stärka Europols informationssystem. För närvarande används Europols it-system av en begränsad användargrupp inom Europol, Europols sambandsmän och utredare i medlemsstaterna för analys och utredning. I och med implementeringen av Quest (systemgränssnittet som gör det möjligt för ESP att söka i Europoluppgifter) på grundläggande skyddsnivå (för närvarande är Europols informationssystem ackrediterade upp till nivåerna RESTREINT UE/EU RESTRICTED och CONFIDENTIEL UE/EU CONFIDENTIAL) kommer Europols informationssystem att bli tillgängliga för en mycket större grupp bemyndigade inom brottsbekämpning. Utöver dessa ökningar kommer ESP att användas av Etias för att automatiskt söka Europoluppgifter vid hantering av resetillstånd. Detta ökar antalet sökningar mot Europoluppgifter från de nuvarande omkring 107 000 sökningarna per månad till mer än 100 000 förfrågningar per dag, och det kommer också att kräva att Europols informationssystem är tillgängliga dygnet runt varje dag med mycket korta svarstider för att uppfylla kraven i Etiasförordningen. De flesta kostnaderna är begränsade till perioden innan

interoperabilitetskomponenterna tas i drift, men vissa löpande åtaganden behövs för att säkerställa hög och kontinuerlig tillgänglighet för Europol's informationssystem. Ett visst utvecklingsarbete behövs också för att införa interoperabilitetskomponenterna med Europol som användare.

18.0205 – Cepol			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
Rubrik 1: Personalkostnader	Åtaganden	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Betalningar	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Rubrik 2: Infrastruktur och driftsutgifter	Åtaganden	(1a)	0	0	0	0	0	0	0	0	0	0
	Betalningar	(2a)	0	0	0	0	0	0	0	0	0	0
Rubrik 3: Driftsutgifter	Åtaganden	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Betalningar	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
TOTALA anslag för Cepol	(summa åtaganden = summa betalningar)	=1+1a +3a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

En centralt samordnad utbildning på EU-nivå gör genomförandet av kurser på nationell nivå mer enhetligt och säkerställer därmed en korrekt och lyckad implementering och användning av interoperabilitetskomponenterna. Cepol – i egenskap av EU:s byrå för utbildning av tjänstemän inom brottsbekämpning – är väl lämpad att tillhandahålla central utbildning på EU-nivå. Dessa utgifter täcker förberedelserna för den ”utbildning av medlemsstaternas utbildare” som krävs för att använda de centrala systemen när de väl är interoperabla. Kostnaderna inbegriper kostnader för en liten personalökning inom Cepol för att samordna, administrera, organisera och uppdatera kurserna samt kostnader för att tillhandahålla ett antal kurstillfällen per år och utarbeta en nätkurs. Närmare detaljer om dessa kostnader redovisas nedan. Utbildningsverksamheten fokuseras på perioderna strax innan driftsättningen. Ett fortlöpande arbete krävs även efter detta då interoperabilitetskomponenterna underhålls och det inte alltid är samma personer som ger utbildningarna, utgående från erfarenheterna av befintliga utbildningar om Schengens informationssystem.

18.0207 – eu-LISA			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTAL T
--------------------------	--	--	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------

Rubrik 1: Personalkostnader	Åtaganden	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Betalningar	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Rubrik 2: Infrastruktur och driftsutgifter	Åtaganden	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Betalningar	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Rubrik 3: Driftsutgifter	Åtaganden	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Betalningar	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
TOTALA anslag för eu-LISA	(summa åtaganden = summa betalningar)	=1+1a +3a	5,830	17,031	51,743	44,749	29,653	20,370	18,609	18,529	18,529	225,041

Utgifterna täcker följande:

- Utveckling och underhåll av de fyra interoperabilitetskomponenter – den europeiska sökportalen (ESP), den gemensamma biometriska matchningstjänsten, den gemensamma databasen för identitetsuppgifter (CIR) och detektorn för multipla identiteter (MID) – som ingår i lagstiftningsförslaget samt den centrala databasen för rapporter och statistik (CRRS). Eu-LISA kommer att fungera som företrädare för projektägaren och använda sin egen personal för att utarbeta specifikationer, välja entreprenörer, leda arbetet, lämna in resultat på ett antal tester och godkänna det arbete som utförts.
- De kostnader som rör datamigreringen från de befintliga systemen till de nya komponenterna. Eu-LISA har dock ingen direkt roll vid den första datainmatningen i MID (validering av länkar), eftersom den handlar om själva datainnehållet. Migreringen av biometriska uppgifter från befintliga system rör uppgifternas format och märkning och inte datainnehållet.
- Kostnaderna för Ecris-TCN-systemets uppgradering till och drift som ett högtillgängligt system från och med 2022. Ecris-TCN är det centrala system som innehåller uppgifter ur brottsregister om tredjelandsmedborgare. Systemet planeras bli tillgängligt senast 2020. Interoperabilitetskomponenterna planeras ha åtkomst även till det systemet, som därför också bör bli ett högtillgängligt system. De operativa utgifterna inbegriper de ytterligare kostnaderna för att uppnå denna höga tillgänglighet. Under 2021 uppstår betydande utvecklingskostnader,

och därefter kostnader för löpande underhåll och drift. Dessa kostnader ingår inte i finansieringsöversikten för översynen av förordningen om inrättande av eu-LISA⁷⁶, som endast inbegriper budgetar från 2018 till 2020 och därför inte överlappar detta budgetäskande.

- Utgiftsmönstret är resultatet av att projekten sker i sekvens. Eftersom de olika komponenterna är beroende av varandra sträcker sig utvecklingsperioden från 2019 till 2023. Emellertid börjar underhåll och drift av de första tillgängliga komponenterna redan 2020. Detta förklarar varför utgifterna är låga i början, för att sedan öka och därefter minska igen till ett konstant värde.
- Utgifterna under rubrik 1 (personalkostnader) följer projektens ordningsföljd: mer personal krävs för att förverkliga projektet med entreprenören (vars utgifter ingår under rubrik 3). När projektet har levererats övergår några ur leveransteamet till utveckling och underhåll. Samtidigt ökar den personal som sköter driften av de nylevererade systemen.
- Utgifterna under rubrik 2 (infrastruktur och driftsutgifter) täcker ytterligare kontorsutrymmen för den tillfälliga inhysningen av de entreprenörsteam som ansvarar för utvecklings-, underhålls- och driftsuppgifter. Utgiftsmönstren över tiden följer därför också personalnivåns utveckling. Kostnaderna för att hysa ytterligare utrustning har redan inkluderats i eu-LISA:s budget. Inga extra kostnader tillkommer för emottagandet av personal från eu-LISA eftersom detta ingår i de ordinära personalkostnaderna.
- Utgifterna under rubrik 3 (driftsutgifter) inbegriper entreprenörens kostnader för att utveckla och underhålla systemet samt anskaffningen av den specifika maskinvaran och programvaran.
Entreprenörskostnaderna gäller inledningsvis studier för att specificera komponenterna och utvecklingen av endast en komponent (CRRS). Under perioden 2020–2022 ökar kostnaderna vartefter som fler komponenter utvecklas parallellt. Kostnaderna minskar inte efter det att toppnivån nåtts, eftersom denna projektporfölj inbegriper särskilt stora datamigreringsuppgifter. Entreprenörskostnaderna minskar sedan när komponenterna levererats och tagits i drift, vilket kräver ett stabilt finansieringsmönster.
Samtidigt med utgifterna under rubrik 3 ökar utgifterna 2020 kraftigt jämfört med föregående år på grund av initiala investeringskostnader för maskinvara och programvara under utvecklingsfasen. Utgifterna under rubrik 3 (driftsutgifter) ökar väsentligen under 2021 och 2022 eftersom investeringskostnaderna för maskinvara och programvara för den operativa it-miljön (produktion och förproduktion både för den centrala enheten och dess backup) uppkommer året innan driftsättningen av respektive interoperabilitetskomponent (CIR och MID) med höga krav på programvara och maskinvara. När komponenterna väl är i drift gäller kostnaderna för maskinvara och programvara främst underhåll.
- Närmare detaljer följer.

⁷⁶

Förslag till Europaparlamentets och rådets förordning om Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, om ändring av förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF och om upphävande av förordning (EU) nr 1077/2011, COM(2017) 352 final, 2017/0145 (COD).

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

Miljoner euro (avrundat till tre decimaler)

		År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
GD HOME											
• Personalresurser Budgetrubrik 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Övriga administrativa kostnader (möten o.dyl.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
GD HOME TOTALT	Anslag	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
---	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Miljoner euro (avrundat till tre decimaler)

		År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	År 2028	TOTAL T
TOTALA anslag för RUBRIKERNÄ 1–5 i den fleråriga budgetramen	Åtaganden	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	0	424,738
	Betalningar	7,533	26,569	96,042	97,591	83,993	34,256	28,088	28,008	22,658	0	424,738

3.2.2. Beräknad inverkan på driftanslagen

3.2.2.1. Beräknad inverkan på Europeiska gräns- och kustbevakningsbyråns anslag

- ☐ Förslaget/initiativet kräver inte att driftanslag tas i anspråk
- ☒ Förslaget/initiativet kräver att driftanslag tas i anspråk enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Mål- och resultatbeteckning Europeiska gräns- och kustbevaknings byrån ⇓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT								
	Typ ⁷⁷	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1 ⁷⁸ Validering av länkar																				
Antal anställda som rekryteras som experter för att validera länkar	Entreprenörskostnader	0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0	2,383
Delsumma för specifikt mål nr 1			0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0	2,383

Utgifterna täcker följande:

- Rekrytering av tillräcklig ytterligare personal (uppskattningsvis omkring tio experter) till den befintliga interna personalen (uppskattningsvis omkring 20 personer) som utplaceras vid Europeiska gräns- och kustbevakningsbyrån för att validera länkar. Endast en månads rekrytering före startdatum planeras för att uppnå den personalnivå som krävs.

⁷⁷ 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).

⁷⁸ Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål...”.

- Inga andra entreprenörskostnader beräknas. Den programvara som krävs är en del av licenskostnaderna för den gemensamma biometriska matchningstjänsten. Ingen särskild maskinvaruprocesskapacitet krävs. Entreprenörens personal antas inhysas av Europeiska gräns- och kustbevakningsbyrån. Därför tilläggs en årlig kostnad på 12 kvadratmeter i genomsnitt per person under utgifterna under rubrik 2.

3.2.2.2. Beräknad inverkan på Europol's anslag

- ☐ 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 Europol ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT										
	Typ ⁷⁹	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1 ⁸⁰ Utveckling och underhåll av (Europol's) system																						
It-miljö	Infrastruktur				1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096	
It-miljö	Maskinvara				3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144	
It-miljö	Programvara				0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948	

⁷⁹

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).

⁸⁰

Mål som redovisats under punkt 1.4.2: "Specifikt/specifika mål...".

Utvecklingsarbet e	Entreprenör			0,360	0,360									0,720
Delsumma			0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908		

Dessa utgifter täcker behovet av att stärka Europol's informationssystem och infrastruktur för att hantera det ökade antalet sökningar. Dessa kostnader omfattar följande:

- Uppgradering av säkerhets- och nätverksinfrastrukturen, maskinvara (servrar och lagring) och programvara (licenser). Dessa uppgraderingar måste vara klara innan den europeiska sökportalen och Etias tas i drift 2021 och kostnaderna har fördelats jämnt mellan 2020 och 2021. Från och med 2022 har en årlig underhållssats på 20 % använts som grund för beräkningen av underhållskostnader. Dessutom har man beaktat standardcykeln på fem år för ersättning av föråldrad maskinvara och infrastruktur.
- Entreprenörskostnader för utvecklingsarbete för implementering av Quest med grundläggande skyddsnivå.

3.2.2.3. Beräknad inverkan på Cepols anslag

- ☐ 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 Cepol ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT										
	Typ ⁸¹	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1 ⁸² Utveckling och tillhandahållande av utbildning																						
Antal kurser med närutbildning	0,34 per kurs	0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788	
Onlinekurs	0,02		0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052	
Delsumma				0		0,040		0,176		0,274		0,070		0,070		0,070		0,070		0,070		0,840

⁸¹ 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).
⁸² Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål...”.

För att säkerställa enhetlig implementering och användning av interoperabilitetslösningarna kommer utbildningen att organiseras både centralt på EU-nivå av Cepol och av medlemsstaterna. Utgifterna för utbildning på EU-nivå omfattar följande:

- Utveckling av en gemensam läroplan som medlemsstaterna ska använda när de genomför nationell utbildning.
- Närutbildning för utbildare. Utbildningen är tänkt att genomföras i större skala under de två åren genast efter att interoperabilitetslösningarna tagits i drift och senare upprätthållas genom två kurser närutbildning per år.
- Nätkurs för att komplettera närutbildningen på EU-nivå och i medlemsstaterna.

3.2.2.4. Beräknad inverkan på eu-LISA:s anslag

- ☐ 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 eu-LISA ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT									
	Typ ⁸³	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad	
SPECIFIKT MÅL nr 1 ⁸⁴ Utveckling av interoperabilitetskomponenterna																					
Byggda system	Entreprenör		1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Programvaruprodukter	Programvara		0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Maskinvaruprodukter	Maskinvara		0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
It-utbildning	Utbildning & övrigt		0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340

⁸³ 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).

⁸⁴ Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål...”.

Delsumma för specifikt mål nr 1	2,390	11,151	28,879	16,131	6,830	1,815	0,415	0,335	0,335	68,281
---------------------------------	-------	--------	--------	--------	-------	-------	-------	-------	-------	--------

- Detta mål omfattar endast kostnaderna för att leverera de fyra interoperabilitetskomponenterna och CRRS.
- Kostnadsberäkningen för den gemensamma biometriska matchningstjänsten förutsätter att det in- och utresesystem som håller på att utvecklas används som kärnsystem för utvecklingen. Därför planerar man att återanvända de biometriska programvarulicenser som inkluderas för in- och utresesystemet (36 miljoner EUR).
- I denna budget hanteras den gemensamma biometriska matchningstjänsten budgetmässigt som en vidareutvidgning av den biometriska matchningstjänsten för in- och utresesystemet. Därför omfattar denna finansieringsöversikt marginalkostnaderna för programvarulicenser (6,8 miljoner EUR) för att lägga till de omkring 20 miljoner biometriska datauppsättningar som finns i SIS Afis (Afis är det automatiska fingeravtrycksidentifieringssystemet, dvs. SIS motsvarighet till en biometrisk matchningstjänst), Eurodacs Afis och det framtida Ecris-TCN (det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare) till den biometriska matchningstjänst som levereras för in- och utresesystemet. Kostnaderna för att integrera de olika systemen (SIS, Eurodac och Ecris-TCN) med den gemensamma biometriska matchningstjänsten ingår i denna finansieringsöversikt.
- Som en del av arbetet under 2019 och 2020 kommer eu-LISA att få i uppgift att utarbeta en precis teknisk lösning som inte kan fastställas vid tidpunkten för inlämnande av lagstiftningsförslaget och att beräkna hur mycket det skulle kosta att införa den valda tekniska lösningen. Detta kan kräva en ändring av den kostnadsberäkning som anges här.
- Alla komponenter levereras senast i slutet av 2023, varför entreprenörskostnaderna minskar till nära noll vid den tidpunkten. Endast en restpost för fortlöpande uppdatering av CRRS kvarstår.
- Under perioden 2019–2021 ökar programvarukostnaderna avsevärt eftersom programvarulicenskostnader uppkommer för de olika miljöer som behövs för produktion, förproduktion och tester; både för centralanläggningen och backupanläggningen. Dessutom prissätts vissa specifika och nödvändiga programvarukomponenter enligt antalet referensobjekt (t.ex. datavolym). Eftersom databasen i slutändan kommer att innehålla omkring 220 miljoner identiteter står programvarupriset i proportion till detta värde.

Mål- och resultatbeteckning eu-LISA ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT										
	Typ ⁸⁵	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad		
SPECIFIKT MÅL nr 2 Underhåll och drift av interoperabilitetskomponenterna																						
System i drift	Entreprenör		0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501	
Programvaruprodukter	Programvara		0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032	
Maskinvaruprodukter	Maskinvara		0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423	
It-utbildning	Utbildning		0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150	
Delsumma för specifikt mål nr 2				0		0,325		0,325		3,567		10,034		10,464		10,464		10,464		10,464		56,105

- Underhållet inleds så snart en komponent har levererats. Därför inkluderas anslag för en entreprenör som sköter underhållet från och med den tidpunkt då ESP levereras (2021). Underhållsbudgeten ökar vartefter som fler komponenter levereras och når sedan en mer eller mindre konstant nivå som motsvarar en viss procentandel (15–22 %) av den ursprungliga investeringen.
- Underhåll av maskinvara och programvara börjar från och med året för idrifttagandet: utvecklingen av kostnaderna motsvarar utvecklingen för entreprenörskostnader.

⁸⁵ 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).

Mål- och resultatbeteckning eu-LISA ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT										
	Typ ⁸⁶	Geno msnit tliga kostn ader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 3 ⁸⁷ Datamigrering																						
Migrerade uppgifter från befintliga biometriska matchningssyste m	Till den gemensamma biometriska matchningstjäns ten		0		0		0		7,000		3,000		0		0		0		0			10,000
Befintliga Eurodacuppgifte r redo för migrering	Ny utformning och ombyggnad av Eurodac		0		0		7,500		7,500				0		0		0		0			15,000
Delsumma för specifikt mål nr 3				0		0		7,500		14,500		3,000										25,000

- När det gäller den gemensamma biometriska matchningstjänsten måste uppgifter migreras till den från de andra biometriska sökmotorerna, eftersom detta gemensamma system operativt sett är effektivare och även ger en ekonomisk fördel jämfört med en situation där man även i fortsättningen skulle upprätthålla flera mindre biometriska matchningssystem.
- Eurodacs nuvarande verksamhetslogik är inte tydligt åtskild från den biometriska matchningsmekanismen, till skillnad från den biometriska matchningstjänst som används med VIS. Eurodacs inre funktion och hur verksamhetstjänsterna anropar den underliggande biometriska matchningstjänsten är en svart låda för betraktaren och bygger på teknik med begränsad tillgänglighet. Det är inte möjligt att helt enkelt

⁸⁶ 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).

⁸⁷ Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål...”.

migrera uppgifterna till en gemensam biometrisk matchningstjänst och behålla det befintliga verksamhetslagret. Därför innebär migreringen av uppgifter betydande kostnader när det gäller att ändra utbytesmekanismerna med Eurodacs centrala applikation.

Mål- och resultatbeteckning eu-LISA ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT								
	Typ ⁸⁸	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 4 ⁸⁹ Nätverk																				
Nätverksanslutningar	Inrättande av nätverk		0		0		0		0,505									0		0,505
Hanterad nätverkstrafik	Nätverksverksamhet		0		0				0,246		0,246		0,246		0,246		0,246		0,246	1,230
Delsumma för specifikt mål nr 4				0		0		0,505		0,246		0,246		0,246		0,246		0,246		1,735

- Interoperabilitetskomponenterna har endast en marginell effekt på nätverkstrafiken. När det gäller uppgifter skapas endast länkar mellan befintliga uppgifter, vilket är en liten post. De kostnader som ingår här är endast den marginella budgetökning som krävs utöver budgetarna för in- och utresesystemet och Etias för inrättande av nätverk och nätverkstrafik.

⁸⁸ 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).

⁸⁹ Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål...”.

Mål- och resultatbeteckning eu-LISA ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT										
	Typ ⁹⁰	Gensnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 5 ⁹¹ Uppdatera det enhetliga nationella gränssnittet																						
Uppdaterat enhetligt	Entreprenör		0		0		0		0,505		0,505									0		1,010
Delsumma för specifikt mål nr 5				0		0		0		0,505		0,505										1,010

- I förslaget om in- och utresesystemet infördes konceptet med ett enhetligt nationellt gränssnitt som ska utvecklas och upprätthållas av eu-LISA. Tabellen ovan innehåller budgeten för uppdatering av det enhetliga nationella gränssnittet för ytterligare en typ av informationsutbyte. Inga ytterligare kostnader tillkommer för driften av det enhetliga nationella gränssnittet, som redan ingår i budgeten i förslaget om in- och utresesystemet.

⁹⁰ 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).

⁹¹ Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål...”.

Mål- och resultatbeteckning eu-LISA ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT										
	Typ 92	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 6 Möten och utbildning																						
Möten om månatliga framsteg (Utveckling)	0,021 per möte x 10 per år		10	0,210	10	0,210	10	0,210	10	0,210											40	0,840
Kvartalsvisa möten (drift)	0,021 x 4 per år		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Rådgivande grupper	0,021 x 4 per år		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Medlemsstaternas utbildning	0,025 per kurs		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Delsumma för specifikt mål			20	0,428	22	0,478	22	0,478	24	0,528	14	0,318	14	0,318	1	0,318	1	0,318	1	0,318		3,502

92

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).

nr 6									4	4	4		
------	--	--	--	--	--	--	--	--	---	---	---	--	--

- Delsumman för mål 6 omfattar förvaltningsmyndighetens (i detta fall eu-LISA) kostnader för att anordna möten för projektstyrningen. Detta är kostnaderna för extra möten för leveransen av interoperabilitetskomponenterna.
- Delsumman för mål 6 inbegriper kostnaderna för eu-LISA:s möten med medlemsstaternas personal som arbetar med utveckling, underhåll och drift av interoperabilitetskomponenterna och med att organisera och hålla utbildning för medlemsstaternas it-personal.
- Under utvecklingsfasen budgeteras för tio projektmöten per år. När driften förbereds (från och med 2019) hålls fyra möten per år. På en högre nivå inrättas en rådgivande grupp från början för att genomföra kommissionens genomförandebeslut. Fyra möten per år planeras, såsom för de befintliga rådgivande grupperna. Vidare förbereder och håller eu-LISA utbildning för medlemsstaternas it-personal. Detta är utbildning om interoperabilitetskomponenternas tekniska aspekter.

Mål- och resultatbeteckning eu-LISA ⇓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT										
	Typ ⁹³	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 7 ⁹⁴ Hög tillgänglighet för Ecris-TCN																						
Högtillgängligt system	Systemets utformning			0		0		8,067											0		8,067	

⁹³ 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).

⁹⁴ Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål...”.

Drift med hög tillgänglighet	Underhåll och drift av system	0	0	0	1,768	1,768	1,768	1,768	1,768	1,768	10,608
Delsumma för specifikt mål nr 4		0	0	8,067	1,768	1,768	1,768	1,768	1,768	1,768	18,675

- Mål nr 7 är att uppgradera Ecris-TCN från ett system med standardtillgänglighet till ett system med hög tillgänglighet. Den uppgraderingen skulle ske 2021, vilket i huvudsak kräver att ytterligare maskinvara anskaffas. Eftersom Ecris-TCN planeras vara färdigt 2020 är det frestande att bygga systemet som högtillgängligt redan från början och integrera det med interoperabilitetskomponenterna. Eftersom många projekt emellertid blir beroende av varandra bör man vara försiktig med att göra ett sådant antagande utan budgetera för separata åtgärder. Denna budget är en tilläggsbudget till kostnaderna för utveckling, underhåll eller drift av Ecris-TCN under 2019 och 2020.

3.2.2.5. 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:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Mål- och resultatbeteckning GD Migration och inrikes frågor ↓			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT								
	Typ ⁹⁵	Genomsnittliga kostnader	Antal	Kost n.	Antal	Kost n.	Antal	Kostn.	Antal	Kostn.	Antal	Kost n.	Antal	Kost n.	Antal	Kost n.	Antal	Kost n.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1 Integrering av (medlemsstaternas) nationella system																				
Enhetliga nationella gränssnitt klara för användning	Anpassning av det enhetliga nationella gränssnittet – utveckling					30	3,150	30	3,150										30	6,300
Medlemsstaternas system anpassade för interoperabilitet	Integrationskostnader					30	40,000	30	40,000	30	40,000								30	120,000

⁹⁵

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).

Utbildade slutanvändare	10 000 kurstillfällen för slutanvändare totalt, 1 000 euro per tillfälle					5 000	5 000	5 000	5 000									10,000	10,000
Delsumma för specifikt mål nr 1						43,150	48,150		45,000										136,300

- Specifikt mål nr 1 rör medel som gjorts tillgängliga för medlemsstaterna för att dra fördelar av interoperabla centrala system. Det enhetliga nationella gränssnittet anpassas både när ESP implementeras och när MID tas i drift. Varje medlemsstat har därefter en relativt måttlig förändring att göra (uppskattningsvis 150 persondagar) för att anpassa dessa uppdaterade meddelandeutbyten till de centrala systemen. Den förändring av innehållet i uppgifterna som interoperabiliteten kommer att införa är större, och tas upp under ”integrationskostnader”. Dessa medel rör förändringar av den typ av meddelanden som skickas till det centrala systemet och hanteringen av de svar som fås tillbaka. För beräkningen av kostnaderna för dessa ändringar har en budget på 4 miljoner EUR anslagits per medlemsstat. Detta belopp är detsamma som för in- och utresesystemet, eftersom motsvarande mängd arbete krävs för att anpassa integrationen av de nationella systemen med det enhetliga nationella gränssnittet.
- Slut användarna måste utbildas för systemen. Denna utbildning av ett mycket stort antal slutanvändare ska finansieras genom 1 000 EUR per kurstillfälle med 10–20 slutanvändare för de uppskattningsvis 10 000 tillfällen som ska organiseras av samtliga medlemsstater i deras egna lokaler.

3.2.3. Beräknad påverkan på personalbehov

3.2.3.1. Sammanfattning för Europeiska gräns- och kustbevakningsbyrån

- ☐ 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 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
--	------------	------------	------------	------------	------------	------------	------------	------------	------------	--------

Tjänstemän (lönegrad AD)										
Tjänstemän (lönegrad AST)	0									
Kontraktsanst ällda	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Tillfälligt anställda	0	0	0	0	0	0	0	0	0	0
Utstationerade nationella experter										

TOTALT	0,0	0,0	0,0	0,350	1,400	0,233	0,0	0,0	0,0	1,983
---------------	------------	------------	------------	--------------	--------------	--------------	------------	------------	------------	--------------

Det arbete som denna extrapersonal vid den europeiska gräns- och kustbevakningen förväntas utföra är tidsbegränsat (2023) och inleds mer specifikt 24 månader efter det att den biometrisk sökmotorn för in- och utresesystemet är tillgänglig. Personalen måste dock rekryteras i förväg (tre månader i genomsnitt har beräknats), vilket förklarar beloppet för 2022. Det arbete som utförs följs av avslutande uppgifter under två månader, vilket förklarar personalnivån 2024.

Själva personalnivån bygger på att 20 personer krävs för det arbete som ska utföras (plus tio personer som tillhandahålls av en entreprenör och som återges under rubrik 3). Uppgifterna väntas också utföras under förlängda arbetstider och inte bara under vanlig kontorstid. Det antas att stöd- och ledningspersonal tillhandahålls genom byråns resurser.

Personalantalet bygger på antagandet att omkring 550 000 fingeravtryck måste bedömas, vilket tar i genomsnitt 5–10 minuter styck (17 000 kontrollerade fingeravtryck per år)⁹⁶.

⁹⁶

Uppgifterna om personal för år 2020 och framåt är endast vägledande och en bedömning måste göras av om de ska läggas till de ursprungliga planerna för personal vid Europeiska gräns- och kustbevakningen i COM(2015) 671 eller ej.

Antal anställda	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt
Personal för manuell hantering av länkar och beslut	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Totalt rubrik 1 - kontraktsanställda	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Totalt rubrik 1 - tillfälligt anställda	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Totalt rubrik 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

3.2.3.2. Sammanfattning för Europol

- ☐ 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 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
--	------------	------------	------------	------------	------------	------------	------------	------------	------------	--------

Tjänstemän (lönegrad AD)										
Tjänstemän (lönegrad AST)	0									
Kontraktsanställda	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Tillfälligt anställda	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Utstationerade nationella experter										

TOTALT	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
---------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

Kostnaderna beräknas på grundval av följande personalnivåer:

Antal heltidsekvivalenter för IKT	2019	2020	2021	2022	2023	2024	2025	2026	2027	TOTALT
Kontraktsanställda	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Tillfälligt anställda	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Anställda totalt (heltidsekvivalenter)	5,0	15,0	15,0	12,5	12,5	11,0	11,0	11,0	11,0	104,0

Ytterligare IKT-personal för Europol planeras för att stärka Europol's informationssystem i syfte att ta hänsyn till det ökade antalet sökningar från ESP och Etias och senare att underhålla systemen dygnet runt alla dagar.

- För ESP:s implementeringsfas (2020 och 2021) finns det ett ytterligare behov av tekniska experter (arkitekter, ingenjörer, utvecklare och testare). Ett minskat antal tekniska experter behövs för åren 2022 framåt för att implementera resten av interoperabilitetskomponenterna och underhålla systemen.
- Från och med andra halvåret 2021 måste IKT-systemövervakning finnas dygnet runt alla dagar för att säkerställa ESP:s och Etias servicenivåer. Detta görs av två kontraktsanställda som arbetar i fyra skift dygnet runt alla dagar.
- I möjligaste mån har profilerna uppdelats mellan tillfälligt anställda och kontraktsanställda. Det måste dock noteras att på grund av höga säkerhetskrav är det för flera tjänster endast möjligt att använda tillfälligt anställda. Äskandet om tillfälligt anställda kommer att beakta resultatet av förlikningen om budgetförfarandet 2018.

3.2.3.3. Sammanfattning för Ceph

- ☐ 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 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
--	------------	------------	------------	------------	------------	------------	------------	------------	------------	--------

Tjänstemän (lönegrad AD)										
Tjänstemän (lönegrad AST)										
Kontraktsanställda			0,070	0,070						0,140
Tillfälligt anställda		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Utstationerade nationella experter										

TOTALT		0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
---------------	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Ytterligare personal krävs eftersom utbildningen för utbildare i medlemsstaterna måste utvecklas specifikt i syfte att använda interoperabilitetskomponenterna i operativa sammanhang.

- Utvecklingen av en läroplan och utbildningsmoduler bör inledas minst 8 månader innan systemet tas i drift. Under de två första åren efter driftsättningen är utbildningen som mest intensiv. Den måste dock bibehållas under en längre period för att säkerställa enhetlig användning, utgående från erfarenheterna av Schengens informationssystem.
- Extra personal behövs för att utarbeta, samordna och genomföra läroplanen, närutbildning och nätkurser. Dessa kurser kan endast genomföras utöver Cepols befintliga kurskatalog, och därför behövs extra personal.
- Enligt planen arbetar en kursledare som tillfälligt anställd under hela utvecklings- och underhållsperioden och får stöd av en kontraktsanställd under den mest intensiva organisationsperioden för utbildningen.

3.2.3.4. Sammanfattning för eu-LISA

- ☐ 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 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
--	------------	------------	------------	------------	------------	------------	------------	------------	------------	--------

Tjänstemän (lönegrad AD)										
Tjänstemän (lönegrad AST)										
Kontraktsanställda	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Tillfälligt anställda	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Utstationerade nationella experter										

TOTALT	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
---------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

- Personalbehovet är fastställt med hänsyn till att de fyra komponenterna och CRRS utgör en portfölj av projekt som är beroende av varandra (dvs. ett program). För att hantera beroendeförhållandena mellan projekten skapas ett programförvaltningsteam som består av programansvariga, projektledare och de profiler (ofta kallade arkitekter) som behövs för att fastställa de gemensamma delarna mellan dem. Förverkligandet av programmet/projektet kräver också profiler för program- och projektstöd.
- Personalbehovet per projekt har beräknats genom jämförelser med tidigare projekt (Informationssystemet för viseringar) och särskiljande mellan projektets avslutande fas och driftsfasen.

- De profiler som behöver stanna kvar även under driftsfasen rekryteras som tillfälligt anställda. De profiler som krävs under programmets/projektets genomförande rekryteras som kontraktsanställda. För att säkerställa den förväntade kontinuiteten för uppgifter och hålla kvar kunskap inom byrån är antalet tjänster som tillfälligt anställda och kontraktsanställda nästan lika många.
- Det antas att ingen extra personal krävs för projektet med att uppgradera Ecris-TCN till hög tillgänglighet och att eu-LISA:s projektpersonal utgörs av befintlig personal från projekt som avslutas under denna period.

Dessa uppskattningar bygger på följande personalnivåer:

Kontraktsanställda:

3.2.1. utgifter eu-LISA (motsvarar rubrik 1) i antal personer	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt (formel)
Kontraktsanställda										
Program-/projektförvaltning	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS	1,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	1,5
MID	0,0	0,5	0,5	0,5	0,5	0,0	0,0	0,0	0,0	2,0
Program-/projektkontor	2,0	2,0	2,0	2,0	2,0	1,0	1,0	1,0	1,0	14,0
Kvalitetssäkring	1,0	2,0	3,0	3,0	2,0	2,0	2,0	2,0	2,0	19,0
Finansiering och upphandling	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Ekonomisk förvaltning										0,0
Budgetplanering och kontroll										0,0
Upphandling/kontraktsförvaltning	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Tekniska experter	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	3,0	3,0	3,0	3,0	2,0	2,0	2,0	2,0	2,0	22,0
ESP	4,0	4,0	4,0	4,0	4,0	3,0	3,0	3,0	3,0	32,0
Gemensamma biometriska matchningstjänsten	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CIR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CIR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Testning	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	1,0	1,0	1,0	0,5	0,5	0,5	0,5	0,5	0,5	6,0
ESP	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gemensamma biometriska matchningstjänsten	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CIR	0,5	1,0	2,0	2,5	2,5	1,5	1,0	1,0	1,0	13,0
MID	0,0	1,0	1,0	1,0	1,0	1,0	0,5	0,5	0,5	6,5
Systemövervakning	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Allmän (dygnet runt)	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Allmän samordning	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Personalresurser	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Delsumma Kontraktsanställda	12,5	20,0	26,5	36,5	34,5	31,0	30,0	30,0	30,0	251,0

Tillfälligt anställda:

Tillfälligt anställda										
Program-/projektförvaltning	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Programförvaltning	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	9,0
Projektförvaltning	0,0	0,0	1,0	1,0	2,0	2,0	2,0	2,0	2,0	12,0
Program-/projektkontor	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	9,0
ESP	0,5	1,0	1,0	0,5	0,0	0,0	0,0	0,0	0,0	3,0
Gemensamma biometriska matchningstjänsten	0,5	0,5	0,5	1,0	1,0	0,5	0,0	0,0	0,0	4,0
CIR	0,0	0,5	1,0	1,0	0,5	0,0	0,0	0,0	0,0	3,0
MID	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Finansiering och upphandling	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Ekonomisk förvaltning	0,0	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	7,0
Budgetplanering och kontroll	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	9,0
Upphandling/kontraktförvaltning	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	18,0
Tekniska experter	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
ESP	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gemensamma biometriska matchningstjänsten	2,0	3,0	5,0	5,0	5,0	3,0	3,0	3,0	3,0	32,0
CIR	2,0	5,0	5,0	5,0	3,0	3,0	3,0	3,0	3,0	32,0
Säkerhet	1,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	17,0
MID	0,0	2,0	2,0	2,0	2,0	1,0	1,0	1,0	1,0	12,0
Arkitekter	1,0	2,0	3,0	3,0	3,0	2,0	1,0	1,0	1,0	17,0
Testning	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
ESP	0,5	1,0	1,0	1,0	1,0	0,5	0,5	0,5	0,5	6,5
Gemensamma biometriska matchningstjänsten	2,0	2,0	3,0	3,0	3,0	2,0	1,5	1,5	1,5	19,5
CIR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MID	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Systemövervakning	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
ESP	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gemensamma biometriska matchningstjänsten	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CIR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MID	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Utbildning	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Utbildning	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Personalresurser	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Övrigt	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Dataskyddsspecialist	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Delsumma Tillfälligt anställda	14,5	25,0	31,5	31,5	30,5	24,0	22,0	22,0	22,0	223,0
Totalt	27,0	45,0	58,0	68,0	65,0	55,0	52,0	52,0	52,0	474,0

3.2.4. Beräknad inverkan på anslag av administrativ natur

3.2.4.1. GD Migration och inrikes frågor: 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 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTALT
--	------------	------------	------------	------------	------------	------------	------------	------------	------------	--------

RUBRIK 5 i den fleråriga budgetramen										
Personalresurser GD HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Övriga administrativa utgifter	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Delsumma RUBRIK 5 i den fleråriga budgetramen	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Belopp utanför RUBRIK 5 i den fleråriga budgetramen	(Används inte)									
Personalresurser										
Andra utgifter av administrativ natur										
Delsumma för belopp utanför RUBRIK 5 i den fleråriga budgetramen										

TOTALT	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
---------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------

⁹⁷

Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.4.2. 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 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	TOTAL T
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)										
18 01 01 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna) GD HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
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 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	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0

18 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:

Övervakning och uppföljning av projekt. Tre tjänstemän för uppföljning. Personalen sköter kommissionens uppgifter vid genomförandet av programmet: kontrollerar överensstämmelse med lagstiftningsförslaget, tar itu med problem avseende efterlevnaden, utarbetar rapporter till Europaparlamentet och rådet samt bedömer medlemsstaternas framsteg. Eftersom programmet är en extra uppgift utöver den befintliga arbetsbördan krävs ytterligare personal. Personalökningen gäller en begränsad tid och omfattar endast utvecklingsperioden.

Förvaltning av det universella meddelandeformatet (UMF)

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).

Kommissionen kommer att sköta den dagliga förvaltningen av UMF-standarden. Två tjänstemän krävs för detta syfte: en person med sakkunskap inom brottsbekämpning och en annan person med god kunskap om verksamhetsmodellering och IKT-kunskaper.

Det universella meddelandeformatet (UMF) utgör en standard för strukturerat gränsöverskridande informationsutbyte mellan informationssystem, myndigheter och/eller organisationer på området rättsliga och inrikes frågor. UMF definierar en gemensam vokabulär och logiska strukturer för information som ofta utbyts i syfte att underlätta interoperabilitet genom att möjliggöra skapande och läsning av utbytets innehåll på ett konsekvent och semantiskt likvärdigt sätt.

För att säkerställa enhetliga villkor för genomförandet av det universella meddelandeformatet föreslås att kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med 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.

3.2.5. *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

Förklara i förekommande fall vilka ändringar i planeringen som krävs, och ange berörda budgetrubriker och belopp.

Förordningen om fonden för inre säkerhet och stödet för yttre gränser är det finansieringsinstrument som innehåller budgeten för genomförande av interoperabilitetsinitiativet.

I artikel 5 b anges att 791 miljoner EUR ska användas genom ett program för utveckling av it-system på grundval av befintliga och/eller nya system som stöd för hanteringen av migrationsströmmar över de yttre gränserna, med förbehåll för att de relevanta unionslagstiftningsakterna antas och på de villkor som avses i artikel 15. Av dessa 791 miljoner EUR är 480,2 miljoner EUR avsatta för utvecklingen av in- och utresesystemet, 210 miljoner EUR för Etias och 67,9 miljoner EUR för översynen av SIS II. Återstoden (32,9 miljoner EUR) ska omfördelas genom mekanismerna inom fonden för inre säkerhet – gränser och viseringar. **Det föreliggande förslaget kräver 32,1 miljoner EUR för den nuvarande fleråriga budgetramperioden vilket är förenligt med den återstående budgeten.**

Totalbeloppet på 32,1 miljoner EUR i rutan ovan är ett resultat av följande beräkning:

ÅTAGANDEN										
3.2. Beräknad inverkan på utgifterna för GD HOME										
	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt (horis.)
18.02.01.03 - Smarta gränser (inkl. stöd till medlemsstaterna)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Totalt (1)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
18.02.07 3.2. eu-LISA										
	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt (formel)
Rubrik 1: Personalkostnader	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Rubrik 2: Infrastruktur och driftsutgifter	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Rubrik 3: Driftsutgifter	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Totalt (2)	5,830	17,031	51,743	44,749	29,653	20,370	18,609	18,529	18,529	225,041
		22,861							202,181	225,041
18.02.04 3.2. Europol										
	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt (formel)
Rubrik 1: Personalkostnader	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Rubrik 2: Infrastruktur och driftsutgifter	0	0	0	0	0	0	0	0	0	0
Rubrik 3: Driftsutgifter	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Totalt (3)	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860
		9,072							39,788	48,860
18.02.05 3.2. Cefpol										
	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt (formel)
Rubrik 1: Personalkostnader	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Rubrik 2: Infrastruktur och driftsutgifter	0	0	0	0	0	0	0	0	0	0
Rubrik 3: Driftsutgifter	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Totalt (4)	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050
		0,144							1,906	2,050
18.02.0-3.2. Frontex - Europeiska gräns- och kustbevakningsbyrån										
	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt (formel)
Rubrik 1: Personalkostnader	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Rubrik 2: Infrastruktur och driftsutgifter	0	0	0	0,075	0,300	0,050	0	0	0	0,425
Rubrik 3: Driftsutgifter	0	0	0	0,183	2,200	0	0	0	0	2,383
Totalt (5)	0	0	0	0,608	3,900	0,283	0	0	0	4,792
		0							4,792	4,792
TOTALT (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. GD HOME Rubrik 5 "Administrativa utgifter"										
	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totalt
Totalt (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTALT (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

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

3.2.6. Bidrag från tredje part

- Det ingår **inga** bidrag från tredje part i det aktuella förslaget eller initiativet

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 inkomst del:	Belopp som förts in för det innevarande budgetåret	Förslagets eller initiativets inverkan på inkomsterna ¹⁰⁰			År 2019	År 2020	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027
Artikel 6313													
-													
Bidrag från Schengenassocierade länder (Schweiz, Norge, Liechtenstein, Island)		pm	pm	pm	pm	pm	pm	pm	pm	pm	pm	pm	pm

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

18.0207

Ange med vilken metod inverkan på inkomsterna har beräknats.

Budgeten ska omfatta ett bidrag från de länder som är associerade till genomförandet, tillämpningen och utvecklingen av Schengenregelverket och de Eurodac-relaterade åtgärderna i enlighet med vad som fastställs i respektive avtal.

¹⁰⁰

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