

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/818**av den 20 maj 2019****om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816**

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,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ⁽²⁾, och

av följande skäl:

- (1) Kommissionen underströk i sitt meddelande av den 6 april 2016 med titeln *Starkare och smartare informationssystem för gränser och säkerhet* behovet av att förbättra unionens uppgiftshanteringsstruktur för gränsförvaltning och säkerhet. Meddelandet inledde arbetet för att uppnå interoperabilitet mellan EU-informationssystem för säkerhet, gränser och migrationshantering, i syfte att komma till rätta med de strukturella brister i systemen 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 2016 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 2017 ⁽³⁾ efterlyste Europaparlamentet förslag för att förbättra och utveckla befintliga EU-informationssystem, åtgärda luckor i informationen och gå i riktning mot interoperabilitet samt förslag om obligatoriskt informationsutbyte på EU-nivå åtföljda av de bestämmelser om dataskydd som krävs.
- (4) I sina slutsatser av den 15 december 2016 uppmanade Europeiska rådet till ansträngningar för att fortsatt tillhandahålla 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 2017 att det var nödvändigt och tekniskt genomförbart att eftersträva praktiska lösningar för interoperabilitet och att interoperabilitet i princip både kan ge operativa vinster och erhållas i överensstämmelse med dataskyddskraven.
- (6) Kommissionen presenterade i sitt meddelande av den 16 maj 2017 med titeln *Sjunde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*, 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 när det gäller gränser, säkerhet och migration där alla EU-informationssystem för säkerhet, gränsförvaltning och migrationshantering kommer att vara interoperabla på ett sätt som fullt ut respekterar de grundläggande rättigheterna.

⁽¹⁾ EUT C 283, 10.8.2018, s. 48.

⁽²⁾ Europaparlamentets ståndpunkt av den 16 april 2019 (ännu ej offentliggjord i EUT) och rådets beslut av den 14 maj 2019.

⁽³⁾ EUT C 101, 16.3.2018, s. 116.

- (7) I sina slutsatser av den 9 juni 2017 om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabiliteten mellan EU-informationssystem uppmanade rådet kommissionen att i sitt arbete följa de lösningar för interoperabilitet som expertgruppen föreslagit.
- (8) I sina slutsatser av den 23 juni 2017 underströk Europeiska rådet behovet av att förbättra interoperabiliteten mellan databaser och uppmanade kommissionen att så snart som möjligt utarbeta förslag till lagstiftning på grundval av förslagen från expertgruppen för informationssystem och interoperabilitet.
- (9) I syfte att förbättra ändamålsenligheten och effektiviteten i kontrollerna vid de yttre gränserna, bidra till att förebygga och bekämpa olaglig invandring och främja en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen – bland annat att upprätthålla den allmänna säkerheten och allmänna ordningen och trygga säkerheten inom medlemsstaternas territorier förbättra genomförandet av den gemensamma viseringsspolitiken, bistå vid prövningen av ansökningar om internationellt skydd, bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott, underlätta identifieringen av okända personer vid en naturkatastrof, en olycka eller ett terrordåd, i syfte att upprätthålla allmänhetens förtroende för unionens migrations- och asylsystem, unionens säkerhetsåtgärder och unionens förmåga att förvalta de yttre gränserna, 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 de uppgifter som de innehåller kompletterar varandra, med respekt för den enskildes grundläggande rättigheter, i synnerhet rätten till skydd av personuppgifter. 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 dessa system att komplettera varandra för att underlätta korrekt identifiering av personer, däribland okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor, bidra till att bekämpa identitetsbedrägeri, förbättra och harmonisera kvalitetskraven på uppgifterna i respektive EU-informationssystem, underlätta medlemsstaternas tekniska implementering och operativa drift av EU-informationssystem, stärka de skyddsåtgärder för datasäkerhet och dataskydd som reglerar respektive EU-informationssystem, rationalisera åtkomst till in- och utresesystemet, VIS, Etias och Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, samt stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.
- (11) Interoperabilitetskomponenterna bör omfatta in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. De bör också omfatta Europoluppgifter, men endast i den mån som krävs för att Europoluppgifter ska kunna sökas samtidigt med dessa EU-informationssystem.
- (12) Interoperabilitetskomponenterna bör behandla personuppgifterna för personer vars personuppgifter behandlas i de underliggande EU-informationssystemen och av Europol.
- (13) ESP bör inrättas för att tekniskt underlätta medlemsstaternas myndigheters och unionsbyråernas snabba, smidiga, effektiva, systematiska och kontrollerade åtkomst till EU-informationssystem, Europoluppgifter och Internationella kriminalpolisorganisationens (Interpol) databaser i den mån som krävs för att de ska kunna utföra sina uppgifter, i enlighet med deras åtkomsträttigheter. ESP bör även inrättas för att stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS, Ecris-TCN och Europoluppgifter. Genom att göra det möjligt att utföra parallella sökningar i alla relevanta EU-informationssystem, Europoluppgifter och Interpols databaser bör ESP fungera som en gemensam kontaktpunkt eller *meddelandehanterare* för att söka i de olika centrala systemen och smidigt hämta den nödvändiga informationen, med full respekt för de underliggande systemens åtkomstkontroll och dataskyddskrav.
- (14) Utformningen av ESP bör, vid en sökning i Interpols databaser, säkerställa att de uppgifter som används av en ESP-användare för att inleda en sökning inte delas med ägarna av Interpols uppgifter. Utformningen av ESP bör även säkerställa att sökningar i Interpols databaser enbart sker i enlighet med tillämplig unionsrätt och nationell rätt.

- (15) De ESP-användare som har åtkomsträtt till Europoluppgifter enligt Europaparlamentets och rådets förordning (EU) 2016/794 ⁽⁴⁾ 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 i fråga om åtkomst eller användning som dataleverantören har fastställt.
- (16) ESP bör utvecklas och konfigureras så att det endast går att göra sådana sökningar med uppgifter som rör personer eller resehandlingar som finns i ett EU-informationssystem, i Europoluppgifter eller i Interpols databaser.
- (17) För att säkerställa systematisk användning av de relevanta EU-informationssystemen bör ESP användas för att söka i CIR, in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN. En nationell uppkoppling till de olika EU-informationssystemen bör dock behållas som en teknisk reserv. ESP bör också användas av unionens byråer för att göra sökningar i 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 centrala SIS, Europoluppgifter och Interpols databaser, som ett komplement till de befintliga särskilda gränssnitten.
- (18) 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 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 har registrerats i flera databaser, genom att använda en enda teknisk komponent för att matcha den personens biometriska uppgifter mellan olika system, i stället för flera komponenter. Den gemensamma biometriska matchningstjänsten bör främja säkerhet och ge fördelar i fråga om kostnader, underhåll och drift. 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 alla dessa biometriska mallar – logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör – på ett enda ställe och därigenom underlätta jämförelser mellan systemen med användning av biometriska mallar och möjliggöra stordriftsfördelar vid utveckling och underhåll av de centrala EU-systemen.
- (19) De biometriska mallar som lagras i den gemensamma biometriska matchningstjänsten och bör bestå av uppgifter som härrör från en särdragsextraktion från faktiska biometriska prov och erhållas på ett sådant sätt att det inte går att vända på extraktionsprocessen. De biometriska mallarna bör erhållas från biometriska uppgifter, men det bör inte vara möjligt att få fram dessa biometriska uppgifter från de biometriska mallarna. Eftersom handavtryck och DNA-profiler lagras endast i SIS, och inte kan inte användas för att genomföra korskontroller mot uppgifter som finns i andra informationssystem, i enlighet med principerna om nödvändighet och proportionalitet, bör den gemensamma biometriska matchningstjänsten inte lagra DNA-profiler eller biometriska mallar som erhålls från handavtryck.
- (20) Biometriska uppgifter utgör känsliga personuppgifter. Denna förordning bör fastställa grunden och skyddsåtgärder för behandlingen av sådana uppgifter i syfte att entydigt identifiera de berörda personerna.
- (21) In- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN kräver en korrekt identifiering av de personer vars personuppgifter lagras i dem. CIR bör därför underlätta en korrekt identifiering av personer som har registrerats i dessa system.
- (22) 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. Interoperabiliteten mellan EU-informationssystem bör bidra till en korrekt identifiering av personer som är registrerade i dessa system. CIR bör lagra de personuppgifter som behövs för att göra det möjligt att mer korrekt identifiera de personer vars uppgifter lagras i de systemen, inklusive 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 automatiskt när uppgifterna har raderats i det underliggande systemet i enlighet med den logiska separeringen.

⁽⁴⁾ 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).

- (23) En ny behandling, som består i lagring av sådana uppgifter i CIR i stället för lagring i vart och ett av de separata systemen är nödvändig för att det ska vara möjligt att förbättra identifieringens tillförlitlighet genom den automatiska jämförelsen och matchningen av uppgifterna. Det faktum att identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter lagras i CIR bör inte på något sätt hindra den behandling av uppgifter som sker med avseende på in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN, eftersom CIR bör vara en ny gemensam komponent i dessa underliggande system.
- (24) Det är därför nödvändigt att skapa en personakt i CIR för varje person som har registrerats i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN, för att uppnå syftet med en korrekt identifiering av personer inom Schengenområdet och för att stödja MID i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. Personakten bör lagra all den identitetsinformation som avser en person på ett enda ställe och ge vederbörligen bemyndigade slutanvändare åtkomst till den.
- (25) CIR således underlätta och rationalisera åtkomst för myndigheter med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott till de EU-informationssystem som inte har inrättats uteslutande i syfte att förebygga, förhindra, upptäcka eller utreda grov brottslighet.
- (26) CIR bör tillhandahålla en gemensam lagringsplats för identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter om personer som har registrerats i in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN. CIR bör utgöra en del av den tekniska arkitekturen i dessa system och fungera som den gemensamma komponenten mellan dem för att lagra och söka i de identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter som de behandlar.
- (27) Alla poster i CIR bör separeras logiskt genom att varje post automatiskt taggas med namnet på det underliggande system som äger den uppgiften. CIR:s åtkomstkontroller bör använda dessa taggar för att avgöra huruvida åtkomst till posten ska medges.
- (28) Om en medlemsstats polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet, eller om det föreligger tvivel om de identitetsuppgifter som lämnats av den personen eller om resehandlingens äkthet eller dess innehavares identitet eller om personen inte kan eller vägrar att samarbeta, bör polismyndigheten i fråga kunna göra en sökning i CIR för att identifiera personen. För dessa ändamål bör polisen ta fingeravtryck med hjälp av tekniker för direktscanning av fingeravtryck, under förutsättning att förfarandet inleddes i den berörda personens närvaro. Sådana sökningar i CIR bör inte tillåtas för identifiering av minderåriga under 12 år, såvida de inte görs för barnets bästa.
- (29) Om en persons biometriska uppgifter inte kan användas eller en sökning med dessa uppgifter misslyckas bör sökningen utföras med personens identitetsuppgifter i kombination med resehandlingsuppgifter. Om sökningen visar att det finns uppgifter om personen i CIR bör medlemsstaternas myndigheter ha åtkomst till CIR för att ta del av den personens identitetsuppgifter och resehandlingsuppgifter, utan att det i CIR anges vilket EU-informationssystem uppgifterna tillhör.
- (30) Medlemsstaterna bör anta nationella lagstiftningsåtgärder för att utse de myndigheter som är behöriga att utföra identitetskontroller med hjälp av CIR och fastställa förfarandena, villkoren och kriterierna för sådana kontroller, vilka bör vara förenliga 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 rätt.
- (31) Genom denna förordning bör det också införas en ny möjlighet till rationaliserad åtkomst till andra uppgifter än identitetsuppgifter och resehandlingsuppgifter i in- och utresesystemet, VIS, Etias eller Eurodac för medlemsstaternas utsedda myndigheter med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott samt för Europol. Sådana uppgifter kan vara nödvändiga för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i ett specifikt fall där det finns rimliga skäl att anta att en konsultation av dem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrotten eller andra aktuella grova brott, särskilt om det finns misstankar om att en person som misstänks för, har begått eller utsatts för ett terroristbrott eller ett annat grovt brott är en person vars uppgifter lagras i in- och utresesystemet, VIS, Etias eller Eurodac.

- (32) Fullständig åtkomst till uppgifter som finns i EU-informationssystemen som är nödvändig för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, utöver åtkomst till identitetsuppgifter eller resehandlingsuppgifter som finns i CIR, bör även i fortsättningen regleras genom de tillämpliga rättsliga instrumenten. De utsedda myndigheterna med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott samt Europol vet inte på förhand vilket EU-informationssystem som innehåller uppgifter om de personer de behöver göra sökningar om. Detta leder till förseningar och ineffektivitet. Den slutanvändare som har bemyndigats av den utsedda myndigheten bör därför ha rätt att se i vilket av dessa EU-informationssystem de uppgifter som motsvarar resultatet av en sökning är registrerade. 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).
- (33) I detta sammanhang bör ett svar från CIR inte tolkas eller användas som en grund för en slutsats om eller en anledning att vidta åtgärder med avseende på en person, utan bör användas uteslutande i syfte att lämna in begäran om åtkomst till de underliggande EU-informationssystemen, med förbehåll för de villkor och förfaranden som fastställs i respektive rättsliga instrument som reglerar sådan åtkomst. Varje sådan begäran om åtkomst bör omfattas av kapitel VII i denna förordning och i tillämpliga fall av Europaparlamentets och rådets förordning (EU) 2016/679 ⁽⁵⁾, Europaparlamentets och rådets direktiv (EU) 2016/680 ⁽⁶⁾ eller Europaparlamentets och rådets förordning (EU) 2018/1725 ⁽⁷⁾.
- (34) Som en allmän regel bör de utsedda myndigheterna eller Europol begära full åtkomst till minst ett av de berörda EU-informationssystemen, om en flaggning för träff anger att uppgifterna är registrerade i Eurodac. Om sådan full åtkomst i undantagsfall inte begärs – till exempel därför att de utsedda myndigheterna eller Europol redan har erhållit uppgifterna på annat sätt eller att erhållandet av uppgifterna inte längre är tillåtet enligt nationell rätt – bör motiveringen till att inte begära åtkomst registreras.
- (35) Loggarna över sökningarna i CIR bör visa syftet med sökningarna. 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, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.
- (36) Den sökning i CIR som görs av de utsedda myndigheterna och Europol för att få ett svar i form av en flaggning som anger att uppgifterna finns i in- och utresesystemet, VIS, Etias eller Eurodac kräver automatiserad behandling av personuppgifter. En flaggning för träff bör 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 flaggning för träff. Slut användarens åtkomst till en flaggning för träff kommer därför utgöra ett mycket begränsat ingrepp i den berörda personens rätt till skydd av personuppgifter, samtidigt som det ger de utsedda myndigheterna och Europol möjlighet att på ett mer effektivt sätt begära åtkomst till personuppgifter.
- (37) MID bör inrättas för att stödja CIR i dess funktion och för att stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. För att effektivt uppfylla sina respektive syften kräver alla dessa EU-informationssystem en korrekt identifiering av de personer vars personuppgifter lagras i dem.
- (38) För att bättre förverkliga syftena med EU-informationssystemen bör de myndigheter som använder dessa system kunna utföra en tillräckligt tillförlitlig verifiering av identiteten på de personer vars uppgifter lagras i olika system. Den uppsättning identitetsuppgifter eller resehandlingsuppgifter som lagras i ett visst enskilt system kan vara

⁽⁵⁾ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

⁽⁶⁾ Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

⁽⁷⁾ Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

inkorrekt, ofullständig eller falsk, och i dagsläget finns det inget sätt att upptäcka inkorrekta, ofullständiga eller falska identitetsuppgifter eller resehandlingsuppgifter 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 personer för dessa ändamål.

- (39) 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 uppgifter om personer som har registrerats i fler än ett EU-informationssystem. De länkade uppgifterna bör vara strikt begränsade till de uppgifter som krävs för att verifiera att en person har registrerats på ett berättigat eller oberättigat sätt med olika identiteter i olika system, eller för att klargöra att två personer med liknande identitetsuppgifter kanske inte är samma person. Behandlingen av uppgifter genom ESP och den gemensamma biometriska matchningstjänsten för att länka personakter mellan olika system bör hållas till ett absolut minimum och är således begränsad till spårning av multipla identiteter, som ska ske vid den tidpunkt då nya uppgifter läggs till i ett av de system som har uppgifter lagrade i CIR eller som lagts till i SIS. MID bör omfatta skyddsåtgärder mot potentiell diskriminering och ogynnsamma beslut mot personer som lagligen har multipla identiteter.
- (40) 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 Europeiska unionens 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 och ett effektivt genomförande av unionens asyl- och viseringspolitik.
- (41) ESP och den gemensamma biometriska matchningstjänsten bör jämföra uppgifter om personer i CIR och SIS när en nationell myndighet eller en unionsbyrå skapar eller laddar upp 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 en person 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 personen.
- (42) Den nationella myndighet eller unionsbyrå som registrerade uppgifterna i respektive EU-informationssystem bör bekräfta eller ändra länkarna. Denna nationella myndighet eller unionsbyrå bör ha åtkomst till de uppgifter som lagras i CIR eller SIS och i MID för manuell verifiering av olika identiteter.
- (43) En manuell verifiering av olika 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 lagras i ett annat EU-informationssystem. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter bör bedöma om det finns multipla identiteter som på ett berättigat eller oberättigat sätt hänvisar till en och samma person. En sådan bedömning bör om möjligt utföras i den berörda personens närvaro och när så är nödvändigt genom att begära ytterligare klargöranden eller information. Bedömningen bör göras utan dröjsmål, i enlighet med de rättsliga kraven på korrekt information enligt unionsrätten och nationell rätt.
- (44) För länkar som erhålls genom SIS med registreringar avseende personer som är efterlysta för att gripas och överlämnas eller för att utlämnas, försvunna eller utsatta personer, personer som söks för att delta i ett rättsligt förfarande och personer som omfattas av diskreta kontroller eller undersökningskontroller bör den myndighet som ansvarar för manuell verifiering av olika 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 som länkas till dem 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 Europaparlamentets och rådets förordningar (EU) 2018/1860 ⁽⁸⁾, (EU) 2018/1861 ⁽⁹⁾ och (EU) 2018/1862 ⁽¹⁰⁾.

- (45) Skapandet av sådana länkar förutsätter öppenhet gentemot berörda personer. För att underlätta genomförandet av nödvändiga skyddsåtgärder i enlighet med unionens tillämpliga dataskyddsbestämmelser bör personer som är föremål för en röd länk eller en vit länk efter manuell verifiering av olika identiteter informeras skriftligen utan att det påverkar tillämpningen av begränsningar för att trygga säkerheten och den allmänna ordningen, förebygga och förhindra brott samt garantera att nationella utredningar inte äventyras. Dessa personer bör erhålla ett enda identifikationsnummer som gör det möjligt för dem att identifiera den myndighet till vilken de bör vända sig för att utöva sina rättigheter.
- (46) Om en gul länk skapas bör den myndighet som ansvarar för manuell verifiering av olika identiteter ha åtkomst till MID. Om det finns en röd länk bör medlemsstaternas myndigheter och unionens byråer som har åtkomst till minst ett EU-informationssystem som ingår i CIR eller till SIS ha åtkomst till MID. En röd länk bör visa att en person använder olika identiteter på ett oberättigat sätt eller att en person använder någon annan persons identitet.
- (47) När det förekommer en vit eller grön länk mellan uppgifter från två EU-informationssystem bör medlemsstaternas myndigheter och unionens byråer ha åtkomst till MID, om den berörda myndigheten eller byrån har åtkomst till båda informationssystemen. Sådan åtkomst bör beviljas endast i syfte att göra det möjligt för den myndigheten eller byrån att upptäcka potentiella fall där uppgifter har länkats inkorrekt eller behandlats i MID, CIR och SIS i strid med denna förordning samt för att vidta åtgärder för att avhjälpa bristerna och uppdatera eller radera länken.
- (48) Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (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 av EU-informationssystemen. De gemensamma indikatorerna för uppgiftskvalitet bör inbegripa minimikvalitetsstandarder för lagring av uppgifter i EU-informationssystemen eller interoperabilitetskomponenter. 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.
- (49) Kommissionen bör utvärdera eu-Lisas kvalitetsrapporter och utfärda rekommendationer till medlemsstaterna när så är lämpligt. 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.
- (50) Det universella meddelandeformatet (UMF) bör utgöra en standard för strukturerat, gränsöverskridande informationsutbyte mellan informationssystem, myndigheter 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 utbytets innehåll på ett konsekvent och semantiskt likvärdigt sätt.
- (51) Möjligheten kan övervägas att införa UMF-standarderna i VIS, SIS och alla andra befintliga eller nya gränsöverskridande modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor vilka utvecklas av medlemsstaterna.

⁽⁸⁾ Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna (EUT L 312, 7.12.2018, s. 1).

⁽⁹⁾ Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006 (EUT L 312, 7.12.2018, s. 14).

⁽¹⁰⁾ Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU (EUT L 312, 7.12.2018, s. 56).

- (52) En central databas för rapporter och statistik (CRRS) bör inrättas för att generera systemöverskridande statistiska uppgifter och analytisk rapportering för verksamhetsstyrande och operativa syften samt för uppgiftskvalitet i enlighet med tillämpliga rättsliga instrument. eu-Lisa bör inrätta, implementera och hysa CRRS i sina tekniska anläggningar. Den bör innehålla anonymiserade statistiska uppgifter från EU-informationssystemen, CIR, MID och den gemensamma biometrisk matchningstjänsten. Uppgifterna i CRRS bör inte möjliggöra identifiering av enskilda personer. eu-Lisa bör automatiskt anonymisera uppgifterna och registrera de anonymiserade uppgifterna i CRRS. Anonymiseringsprocessen bör vara automatisk, och eu-Lisas personal bör inte beviljas direkt åtkomst till några personuppgifter som lagras i EU-informationssystemen eller i interoperabilitetskomponenterna.
- (53) Förordning (EU) 2016/679 är tillämplig på de nationella myndigheternas behandling av personuppgifter i interoperabilitetssyfte inom ramen för denna förordning, förutom om behandlingen görs av medlemsstaternas utsedda myndigheter eller centrala kontaktpunkter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.
- (54) Direktiv (EU) 2016/680 är tillämpligt i de fall medlemsstaternas behandling av personuppgifter utförs av de behöriga myndigheterna i interoperabilitetssyfte i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.
- (55) Förordning (EU) 2016/679 förordning (EU) 2018/1725 eller, i tillämpliga fall, direktiv (EU) 2016/680 tillämpas på överföringar av personuppgifter till tredjeländer eller internationella organisationer som utförs enligt den här förordningen. Utan att det påverkar grunderna för överföring enligt kapitel V i förordning (EU) 2016/679 eller, i tillämpliga fall, direktiv (EU) 2016/680, bör en dom i en domstol eller ett beslut av en administrativ myndighet i ett tredjeland som kräver att en personuppgiftsansvarig eller ett personuppgiftsbiträde ska överföra eller offentliggöra personuppgifter erkännas eller verkställas på något sätt endast om domen eller beslutet grundar sig på ett internationellt avtal som är i kraft mellan det begärande tredjelandet och unionen eller en medlemsstat.
- (56) De särskilda bestämmelserna om dataskydd i Europaparlamentets och rådets förordning (EU) 2018/1862 och Europaparlamentets och rådets förordning (EU) 2019/816 ⁽¹⁾ är tillämpliga på behandlingen av personuppgifter i de system som regleras genom dessa förordningar.
- (57) Förordning (EU) 2018/1725 är tillämplig på behandling av personuppgifter som utförs av eu-Lisa och unionens andra institutioner och organ när de fullgör sina skyldigheter enligt den här förordningen, utan att det påverkar tillämpningen av förordning (EU) 2016/794, som är tillämplig på Europols behandling av personuppgifter.
- (58) De tillsynsmyndigheter som avses i förordning (EU) 2016/679 eller direktiv (EU) 2016/680 bör övervaka lagligheten i medlemsstaternas behandling av personuppgifter. Europeiska datatillsynsmannen, bör övervaka unionsinstitutionernas och unionsorganens behandling av personuppgifter. Europeiska datatillsynsmannen och tillsynsmyndigheterna bör samarbeta med varandra vid övervakningen av interoperabilitetskomponenternas behandling av personuppgifter. För att Europeiska datatillsynsmannen ska kunna utföra sina uppgifter enligt den här förordningen krävs tillräckliga både personella och ekonomiska resurser.
- (59) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ⁽²⁾ och avgav ett yttrande den 16 april 2018 ⁽³⁾.
- (60) Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (artikel 29-gruppen) avgav ett yttrande den 11 april 2018.
- (61) 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. eu-Lisas skyldigheter i detta avseende bör

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2019/816 av den 17 april 2019 om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN) för att komplettera och stödja det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726 (se sidan 1 i detta nummer av EUT).

⁽²⁾ 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).

⁽³⁾ EUT C 233, 4.7.2018, s. 12.

omfatta antagande av nödvändiga åtgärder för att förhindra åtkomst för obehöriga personer, såsom personal hos externa tjänsteleverantörer, till personuppgifter som behandlas genom interoperabilitetskomponenterna. Vid tilldelning av kontrakt för tillhandahållande av tjänster bör medlemsstaterna och eu-Lisa överväga alla de åtgärder som krävs för att säkerställa efterlevnaden av lagar eller andra författningar om skydd av personuppgifter och den enskildes integritet eller för att skydda väsentliga säkerhetsintressen i enlighet med Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046⁽¹⁴⁾ och tillämpliga internationella konventioner. eu-Lisa bör tillämpa principerna om inbyggt integritetsskydd och integritetsskydd som standard under utvecklingen av interoperabilitetskomponenterna.

- (62) Till stöd för statistik och rapportering är det nödvändigt att bevilja bemyndigad personal vid de behöriga myndigheter, unionsinstitutioner och unionsbyråer som avses i denna förordning åtkomst till vissa uppgifter som rör vissa interoperabilitetskomponenter utan att möjliggöra identifiering av enskilda personer.
- (63) För att medlemsstaternas myndigheter och unionsbyråerna ska kunna anpassa sig till de nya kraven beträffande användningen av ESP är det nödvändigt att föreskriva en övergångsperiod. Likaledes bör övergångsåtgärder fastställas för driftsättningen av MID för att den ska fungera konsekvent och optimalt.
- (64) Eftersom målet för denna förordning, nämligen att inrätta en ram för interoperabilitet mellan EU-informationssystem, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.
- (65) Det återstående beloppet i den budget som öronmärkts för smarta gränser i Europaparlamentets och rådets förordning (EU) nr 515/2014⁽¹⁵⁾ bör omfördelas till den här förordningen, i enlighet med artikel 5.5 b i förordning (EU) nr 515/2014, för att täcka kostnaderna för utveckling av interoperabilitetskomponenterna.
- (66) 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 (EUF-fördraget) delegeras till kommissionen med avseende på
- förlängning av övergångsperioden för användning av ESP,
 - förlängning av övergångsperioden för spårning av multipla identiteter som utförs av Etias centralenhet,
 - förfarandena för att fastställa de fall där identitetsuppgifterna kan betraktas som desamma eller liknande samt
 - reglerna för driften av CRRS, däribland särskilda skyddsåtgärder för behandling av personuppgifter och säkerhetsregler tillämpliga på databasen,
 - samt närmare regler om driften av webbportalen.

Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning⁽¹⁶⁾. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

- (67) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter att fastställa de datum då ESP, den gemensamma biometrisk matchningstjänsten, CIR, MID och CRRS ska tas i drift.

⁽¹⁴⁾ Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (EU) nr 1296/2013, (EU) nr 1301/2013, (EU) nr 1303/2013, (EU) nr 1304/2013, (EU) nr 1309/2013, (EU) nr 1316/2013, (EU) nr 223/2014, (EU) nr 283/2014 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012 (EUT L 193, 30.7.2018, s. 1).

⁽¹⁵⁾ 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).

⁽¹⁶⁾ EUT L 123, 12.5.2016, s. 1.

- (68) Kommissionen bör även tilldelas genomförandebefogenheter med avseende på antagande av närmare bestämmelser om tekniska detaljer i användarprofilerna för ESP, specifikationer för den tekniska lösningen som gör det möjligt att utföra sökningar i EU-informationssystemen, Europoluppgifter och Interpols databaser genom ESP samt formatet för svaren från ESP, tekniska regler för att skapa länkar i MID mellan uppgifter från olika EU-informationssystem, innehållet i och utformningen av det formulär som ska användas för att informera den registrerade när en röd länk skapas, prestandakrav och prestandaövervakning för den gemensamma biometrisk matchningstjänsten, mekanismer, förfaranden och indikatorer för automatiserad kontroll av uppgiftskvalitet, utveckling av UMF-standarden, det samarbetsförfarande som ska användas i händelse av säkerhetsincidenter, samt specifikationerna för den tekniska lösningen för medlemsstaternas hantering av åtkomstbegäranden från användare. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ⁽¹⁷⁾.
- (69) Eftersom interoperabilitetskomponenterna kommer att medföra behandling av betydande mängder känsliga personuppgifter är det viktigt att personer vars uppgifter behandlas genom dessa komponenter i praktiken kan utöva sina rättigheter som registrerade i enlighet med förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725. De registrerade bör få tillgång till en webbplats som gör det lättare för dem att utöva sin rätt till åtkomst till och rättelse, radering och begränsning av behandlingen av deras personuppgifter. eu-Lisa bör inrätta och förvalta en sådan webbplats.
- (70) En av huvudprinciperna i samband med dataskydd är uppgiftsminimering. Enligt artikel 5.1 c i förordning (EU) 2016/679 ska de personuppgifter som behandlas vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Interoperabilitetskomponenterna bör därför inte lagra några nya personuppgifter, med undantag för de länkar som kommer att lagras i MID och som utgör det minimum som krävs för tillämpningen av den här förordningen.
- (71) Denna förordning bör innehålla tydliga bestämmelser om ansvar och rätten till ersättning vid otillåten behandling av personuppgifter och vid någon annan åtgärd som är oförenlig med den. Sådana bestämmelser bör inte påverka rätten till ersättning från samt ansvaret för den personuppgiftsansvarige eller personuppgiftsbiträdet enligt förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725. eu-Lisa bör vara ansvarig för skada som den orsakat i sin egenskap av personuppgiftsbiträde om byrån inte har fullgjort de skyldigheter som den specifikt har ålagts enligt den här förordningen eller om den har agerat utanför eller i strid med lagenliga instruktioner från den medlemsstat som är personuppgiftsansvarig.
- (72) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2004/38/EG ⁽¹⁸⁾.
- (73) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, deltar Danmark inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Danmark. Eftersom denna förordning, i den utsträckning som dess bestämmelser rör SIS såsom det regleras genom förordning (EU) 2018/1862, är en utveckling av Schengenregelverket ska Danmark, i enlighet med artikel 4 i det protokollet, inom sex månader efter det att rådet har beslutat i fråga om den här förordningen, besluta huruvida landet ska genomföra den i sin nationella rätt.
- (74) I den utsträckning som dess bestämmelser rör SIS såsom det regleras genom förordning (EU) 2018/1862, deltar Förenade kungariket i den här förordningen, i enlighet med artikel 5.1 i protokoll nr 19 om Schengenregelverket införlivat inom Europeiska unionens ramar, fogat till EU-fördraget och EUF-fördraget och artikel 8.2 i rådets beslut 2000/365/EG ⁽¹⁹⁾. I den utsträckning som dess bestämmelser rör Eurodac och Ecris-TCN 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, har Förenade kungariket dessutom genom en skrivelse av den 16 maj 2018 meddelat att det önskar delta i antagandet och tillämpningen av denna förordning.

⁽¹⁷⁾ 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).

⁽¹⁸⁾ Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier, och om ändring av förordning (EEG) nr 1612/68 och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG (EUT L 158, 30.4.2004, s. 77).

⁽¹⁹⁾ Rådets beslut 2000/365/EG av den 29 maj 2000 om en begäran från Förenade konungariket Storbritannien och Nordirland om att få delta i vissa bestämmelser i Schengenregelverket (EGT L 131, 1.6.2000, s. 43).

- (75) I den utsträckning som dess bestämmelser rör SIS såsom det regleras genom förordning (EU) 2018/1862, kunde Irland i princip delta i denna förordning i enlighet med artikel 5.1 i protokoll nr 19 om Schengenregelverket införlivat inom Europeiska unionens ramar, fogat till EU-fördraget och EUF-fördraget, och artikel 6.2 i rådets beslut 2002/192/EG ⁽²⁰⁾. I den utsträckning som dess bestämmelser rör Eurodac och Ecris-TCN, i enlighet med artiklarna 1 och 2 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, och utan att det påverkar tillämpningen av artikel 4 i det protokollet, deltar Irland inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Irland. Eftersom det under dessa omständigheter inte är möjligt att säkerställa att denna förordning i alla delar är tillämplig på Irland, såsom krävs enligt artikel 288 i EUF-fördraget, deltar Irland inte i antagandet av denna förordning, utan att det påverkar Irlands rättigheter enligt protokollen nr 19 och nr 21.
- (76) När det gäller Island och Norge utgör denna förordning, i den utsträckning den rör SIS såsom det regleras genom förordning (EU) 2018/1862, i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ⁽²¹⁾, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1 G i rådets beslut 1999/437/EG ⁽²²⁾.
- (77) När det gäller Schweiz utgör denna förordning, i den utsträckning den rör SIS såsom det regleras genom förordning (EU) 2018/1862, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ⁽²³⁾, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1 G i rådets beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2008/149/RIF ⁽²⁴⁾.
- (78) När det gäller Liechtenstein utgör denna förordning, i den utsträckning den rör SIS såsom det regleras genom förordning (EU) 2018/1862, i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ⁽²⁵⁾, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1 G i rådets beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2011/350/EU ⁽²⁶⁾.
- (79) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns i synnerhet i Europeiska unionens stadga om de grundläggande rättigheterna, och bör tillämpas i enlighet med dessa rättigheter och principer.
- (80) För att denna förordning ska passa in i den befintliga rättsliga ramen bör Europaparlamentets och rådets förordningar (EU) 2018/1726 ⁽²⁷⁾, (EU) 2018/1862 och (EU) 2019/816 ändras i enlighet med detta.

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

⁽²¹⁾ EUT L 176, 10.7.1999, s. 36.

⁽²²⁾ Rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtal som har ingåtts mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 176, 10.7.1999, s. 31).

⁽²³⁾ EUT L 53, 27.2.2008, s. 52.

⁽²⁴⁾ Rådets beslut 2008/149/RIF av den 28 januari 2008 om ingående på Europeiska unionens vägnar av avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 53, 27.2.2008, s. 50).

⁽²⁵⁾ EUT L 160, 18.6.2011, s. 21.

⁽²⁶⁾ Rådets beslut 2011/350/EU av den 7 mars 2011 om ingående på Europeiska unionens vägnar av protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, om avskaffande av kontroller vid de inre gränserna och om personers rörlighet (EUT L 160, 18.6.2011, s. 19).

⁽²⁷⁾ Europaparlamentets och rådets förordning (EU) 2018/1726 av den 14 november 2018 om Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-Lisa), om ändring av förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF och om upphävande av förordning (EU) nr 1077/2011 (EUT L 295, 21.11.2018, s. 99).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. Genom denna förordning tillsammans med Europaparlamentets och rådets förordning (EU) 2019/817 ⁽²⁸⁾ 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).
2. Denna ram ska omfatta följande interoperabilitetskomponenter:
 - a) En europeisk sökportal (ESP).
 - b) En gemensam biometrisk matchningstjänst.
 - c) En gemensam databas för identitetsuppgifter (CIR).
 - d) En detektor för multipla identiteter (MID).
3. Denna förordning innehåller också bestämmelser om kraven på uppgifternas kvalitet, ett universellt meddelandeformat (UMF), en central databas för rapporter och statistik (CRRS) 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, utvecklingen och driften av interoperabilitetskomponenterna.
4. Genom denna förordning anpassas också förfarandena och villkoren för att de utsedda myndigheterna och Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) ska få åtkomst till in- och utresesystemet, VIS, Etias och Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.
5. I denna förordning fastställs också ramar för verifiering av personers identitet och för identifiering av personer.

Artikel 2

Mål

1. Genom att säkerställa interoperabilitet har denna förordning följande mål:
 - a) Förbättra ändamålsenligheten och effektiviteten hos in- och utresekontrollerna vid de yttre gränserna.
 - b) Bidra till att förebygga och bekämpa olaglig invandring.
 - c) Bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, bland annat 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.
 - f) Bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott.
 - g) Underlätta identifieringen av okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor vid en naturkatastrof, olycka eller ett terrordåd.
2. De mål som avses i punkt 1 ska uppnås genom att:
 - a) säkerställa en korrekt identifiering av personer,
 - b) bidra till kampen mot identitetsbedrägerier,

⁽²⁸⁾ Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF (se sidan 27 i detta nummer av EUT).

- c) förbättra uppgiftskvaliteten och harmonisera kvalitetskraven på uppgifter som lagras i EU-informationssystemen, samtidigt som kraven avseende uppgiftsbehandling i de rättsliga instrument som reglerar de enskilda systemen samt normerna och principerna för dataskydd respekteras,
- d) underlätta och stödja medlemsstaternas tekniska implementering och operativa drift av EU-informationssystem,
- e) skärpa och förenkla de villkor för datasäkerhet och dataskydd som reglerar de respektive EU-informationssystemen och göra dem mer enhetliga, utan att det påverkar det särskilda skyddet och de särskilda skyddsåtgärderna för vissa kategorier av uppgifter,
- f) rationalisera villkoren för utsedda myndigheters åtkomst till in- och utresesystemet, VIS, Etias och Eurodac, samtidigt som nödvändiga och proportionella villkor för denna åtkomst säkerställs,
- g) stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

Artikel 3

Tillämpningsområde

1. Denna förordning ska tillämpas på Eurodac, SIS och Ecris-TCN.
2. Denna förordning ska också tillämpas på Europoluppgifter i en utsträckning som gör det möjligt att söka i dem samtidigt som i de EU-informationssystem som avses i punkt 1.
3. Denna förordning ska tillämpas på personer vars 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 avses med

1. *yttre gränser*: yttre gränser enligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2016/399 ⁽²⁹⁾,
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 avses i artikel 51.1 i förordning (EU) 2016/679 och den tillsynsmyndighet som avses i 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. *alfanumeriska uppgifter*: uppgifter som återges med bokstäver, siffror, specialtecken, mellanslag och skiljetecken,
8. *identitetsuppgifter*: de uppgifter som avses i artikel 27.3 a–e,
9. *fingeravtrycksuppgifter*: bilder av fingeravtryck och bilder av fingeravtrycksspår som på grund av sin unika karaktär och de referenspunkter som de innefattar möjliggör exakta och entydiga jämförelser för att fastställa en persons identitet,

⁽²⁹⁾ Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna) (EUT L 77, 23.3.2016, s. 1).

10. *ansiktsbild*: digitala bilder av en persons ansikte,
11. *biometriska uppgifter*: fingeravtrycksuppgifter eller ansiktsbilder, eller båda,
12. *bietrisk 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,
13. *resehandling*: pass eller motsvarande handling som ger innehavaren rätt att passera de yttre gränserna och i vilken en visering kan föras in,
14. *resehandlingsuppgifter*: resehandlingens typ, nummer och utfärdandeland samt sista giltighetsdag och koden på tre bokstäver för det land som utfärdat resehandlingen,
15. *EU-informationssystem*: in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN,
16. *Europoluppgifter*: de personuppgifter som behandlas av Europol för det syfte som avses i artikel 18.2 a, b och c i förordning (EU) 2016/794,
17. *Interpols databaser*: Interpols databas över stulna och förkomna resehandlingar (SLTD-databasen) och Interpols databas för resehandlingar som är föremål för ett meddelande (TDAWN-databasen),
18. *träff*: förekomsten av en motsvarighet till följd av en automatisk jämförelse mellan personuppgifter som har registrerats eller håller på att registreras i ett informationssystem eller en databas,
19. *polismyndighet*: behörig myndighet enligt definitionen i artikel 3.7 i direktiv (EU) 2016/680,
20. *utsedda myndigheter*: medlemsstaternas utsedda myndigheter enligt definitionen i artikel 3.1.26 i Europaparlamentets och rådets förordning (EU) 2017/2226 ⁽³⁰⁾, artikel 2.1 e i rådets beslut 2008/633/RIF ⁽³¹⁾ och artikel 3.1.21 i Europaparlamentets och rådets förordning (EU) 2018/1240 ⁽³²⁾,
21. *terroristbrott*: ett brott enligt nationell rätt som motsvarar eller är likvärdigt med ett av de brott som avses i Europaparlamentets och rådets direktiv (EU) 2017/541 ⁽³³⁾,
22. *grovt brott*: ett brott som motsvarar eller är likvärdigt med ett av de brott som avses i artikel 2.2 i rådets rambeslut 2002/584/RIF ⁽³⁴⁾ om det enligt nationell rätt kan leda till fängelse eller annan frihetsberövande åtgärd under en maximal tidsperiod på minst tre år,
23. *in- och utresesystemet*: det in- och utresesystem som inrättats genom förordning (EU) 2017/2226,
24. *Informationssystemet för viseringar* eller *VIS*: det informationssystem för viseringar som inrättats genom Europaparlamentets och rådets förordning (EG) nr 767/2008 ⁽³⁵⁾,
25. *EU-systemet för reseuppgifter och resetillstånd* eller *Etias*: det EU-system för reseuppgifter och resetillstånd som inrättats genom förordning (EU) 2018/1240,

⁽³⁰⁾ 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) nr 1077/2011 (EUT L 327, 9.12.2017, s. 20).

⁽³¹⁾ Rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott (EUT L 218, 13.8.2008, s. 129).

⁽³²⁾ Europaparlamentets och rådets förordning (EU) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226 (EUT L 236, 19.9.2018, s. 1).

⁽³³⁾ Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017, s. 6).

⁽³⁴⁾ Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (EGT L 190, 18.7.2002, s. 1).

⁽³⁵⁾ 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).

26. *Eurodac*: Eurodac som inrättats genom Europaparlamentets och rådets förordning (EU) nr 603/2013 ⁽³⁶⁾,
27. *Schengens informationssystem* eller *SIS*: Schengens informationssystem som inrättats genom Europaparlamentets och rådets förordning (EU) 2018/1860, (EU) 2018/1861 och (EU) 2018/1862,
28. *Ecris-TCN*: det centraliserade system för identifiering av medlemsstater som innehåller uppgifter ur kriminalregister avseende tredjelandsmedborgare och statslösa personer som inrättats genom förordning (EU) 2019/816.

Artikel 5

Icke-diskriminering och grundläggande rättigheter

Behandling av personuppgifter enligt denna förordning får inte leda till diskriminering av personer på någon grund, såsom kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till en nationell minoritet, förmögenhet, börd, funktionsnedsättning, ålder eller sexuell läggning. Den ska ske med fullständig respekt för mänsklig värdighet och integritet samt grundläggande rättigheter, inbegripet rätten till respekt för privatlivet och skydd av personuppgifter. Särskild hänsyn ska tas till barn, äldre, personer med funktionsnedsättning och personer i behov av internationellt skydd. Barnets bästa ska komma i främsta rummet.

KAPITEL II

Den europeiska sökportalen

Artikel 6

Den europeiska sökportalen

1. En europeisk sökportal (ESP) ska inrättas för att underlätta medlemsstaternas myndigheters och unionsbyråernas möjligheter att få snabb, kontinuerlig, effektiv, systematisk och kontrollerad åtkomst till EU-informationssystemen, Europoluppgifter och Interpols databaser som krävs för att de ska kunna utföra sina uppgifter, i enlighet med sina åtkomsträttigheter och målen för och syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.
2. ESP 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 och Ecris-TCN samt i Europoluppgifter och Interpols databaser.
 - b) En säker kommunikationskanal mellan ESP, medlemsstaterna och de unionsbyråer som har rätt att använda sökportalen.
 - c) En säker kommunikationsinfrastruktur mellan ESP och in- och utresesystemet, VIS, Etias, Eurodac, centrala SIS, Ecris-TCN, Europoluppgifter och Interpols databaser samt mellan ESP och de centrala infrastrukturerna för CIR och MID.
3. eu-Lisa ska utveckla ESP och säkerställa dess tekniska förvaltning.

Artikel 7

Användning av den europeiska sökportalen

1. Användningen av ESP ska förbehållas de myndigheter i medlemsstaterna och de unionsbyråer som har åtkomst till åtminstone ett av EU-informationssystemen i enlighet med de rättsliga instrument som reglerar dessa EU-informationssystem, till CIR och MID i enlighet med denna förordning, till Europoluppgifter i enlighet med förordning (EU) 2016/794 eller till Interpols databaser i enlighet med unionsrätten eller nationell rätt avseende sådan åtkomst.

Dessa myndigheter i medlemsstaterna och unionsbyråer får använda ESP och de uppgifter som tillhandahålls genom den endast för de mål och syften som fastställs i de rättsliga instrument som reglerar dessa EU-informationssystem, i förordning (EU) 2016/794 och i denna förordning.

⁽³⁶⁾ Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 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 och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 180, 29.6.2013, s. 1).

2. De myndigheter i medlemsstaterna och de unionsbyråer som avses i punkt 1 ska använda ESP för att söka uppgifter om personer eller deras resehandlingar i Eurodacs och Ecris-TCN:s centrala system i enlighet med sina åtkomsträttigheter enligt de rättsliga instrument som reglerar dessa EU-informationssystem och nationell rätt. De ska också använda ESP 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 ESP för att söka på uppgifter om personer eller deras resehandlingar i det centrala SIS som avses i förordningarna (EU) 2018/1860 och (EU) 2018/1861.
4. När så föreskrivs enligt unionsrätten ska de unionsbyråer som avses i punkt 1 använda ESP för att söka på uppgifter om personer eller deras resehandlingar i centrala SIS.
5. De myndigheter i medlemsstaterna och de unionsbyråer som avses i punkt 1 får använda ESP för att söka på uppgifter om personer eller deras resehandlingar i Europoluppgifter i enlighet med sina åtkomsträttigheter enligt unionsrätten och nationell rätt.

Artikel 8

Profiler för användarna av ESP

1. För att det ska vara möjligt att använda ESP ska eu-Lisa i samarbete med medlemsstaterna skapa en profil för varje kategori av ESP användare och på, det syfte som de har med sökningarna, i enlighet med de tekniska detaljer och åtkomsträttigheter som avses i punkt 2. Varje profil ska, i enlighet med unionsrätten och nationell rätt, inbegripa följande information:
 - a) De uppgiftsfält som ska användas vid sökningar.
 - b) De EU-informationssystem, Europoluppgifter och Interpols databaser som ska vara föremål för sökningar, de som kan vara föremål för sökningar och de som ska tillhandahålla användaren ett svar.
 - c) De specifika uppgifter i EU-informationssystemen, Europoluppgifterna och Interpols databaser som får vara föremål för sökningar.
 - d) De kategorier av uppgifter som får tillhandahållas i varje svar.
2. Kommissionen ska anta genomförandeakter för att närmare ange de tekniska detaljerna för de profiler som avses i punkt 1 ESP i enlighet med ESP-användarnas åtkomsträttigheter enligt de rättsliga instrument som reglerar EU-informationssystemen och nationell rätt. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.
3. De profiler som avses i punkt 1 ska regelbundet ses över av eu-Lisa i samarbete med medlemsstaterna, minst en gång om året, och vid behov uppdateras.

Artikel 9

Sökningar

1. Användarna av ESP ska inleda en sökning genom att mata in alfanumeriska eller biometriska uppgifter i ESP. När en sökning har inletts ska ESP samtidigt söka i in- och utresesystemet, Etias, VIS, SIS, Eurodac, Ecris-TCN och CIR samt i Europoluppgifter och Interpols databaser med de uppgifter som användaren matat in och i enlighet med användarprofilen.
2. De kategorier av uppgifter som används för att inleda en sökning via ESP ska motsvara de kategorier av uppgifter i fråga om personer eller resehandlingar som kan användas för att söka i de olika EU-informationssystemen, Europoluppgifter och Interpols databaser i enlighet med de rättsliga instrument som reglerar dem.
3. eu-Lisa ska i samarbete med medlemsstaterna ta fram ett dokument för gränssnittskontroll för ESP på grundval av det universella UMF som avses i artikel 38.
4. När en sökning inleds av en ESP-användare ska in- och utresesystemet, Etias, VIS, SIS, Eurodac, Ecris-TCN, CIR och MID samt Europoluppgifter och Interpols databaser som svar på sökningen tillhandahålla uppgifter som de innehåller.

Utan att det påverkar tillämpningen av artikel 20 ska det i svaret från ESP anges vilket av EU-informationssystemen eller vilken databas som uppgifterna tillhör.

ESP får inte tillhandahålla någon information om uppgifter i EU-informationssystemen, Europoluppgifter och Interpols databaser som användaren saknar åtkomst till enligt tillämplig unionsrätt och nationell rätt.

5. Alla sökningar i Interpols databaser genom ESP ska göras på ett sådant sätt att ingen information röjs för ägaren av Interpolregistreringen.
6. ESP ska så snart som uppgifter finns tillgängliga tillhandahålla användaren svar från något av EU-informationssystemen, Europoluppgifterna eller Interpols databaser. Dessa svar får endast innehålla de uppgifter som användaren har åtkomst till enligt unionsrätten och nationell rätt.
7. Kommissionen ska anta en genomförandeakt för att specificera det tekniska förfarandet för ESP:s sökningar i EU-informationssystemen, Europoluppgifterna och Interpols databaser och formatet för ESP:s svar. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 10

Registerföring av loggar

1. Utan att det påverkar tillämpningen av artiklarna 12 och 18 i förordning (EU) 2018/1862, artikel 29 i förordning (EU) 2019/816 och artikel 40 i förordning (EU) 2016/794, ska eu-Lisa föra logg över all uppgiftsbehandling i ESP. Dessa loggar ska innehålla följande:
 - a) Den medlemsstat eller unionsbyrå som inlett sökningen och den ESP-profil som används.
 - b) Datum och tidpunkt för sökningen.
 - c) De EU-informationssystem och Europoluppgifter som varit föremål för sökning.
2. Varje medlemsstat ska föra logg över sökningar som utförs av dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda ESP. Varje unionsbyrå ska föra logg över sökningar som utförs av dess vederbörligen bemyndigade personal.
3. De loggar som avses i punkterna 1 och 2 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 och dataintegritet. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats. För det fall de behövs för övervakningsförfaranden som redan har inletts ska de emellertid raderas så snart loggarna i fråga inte längre behövs för övervakningsförfarandena.

Artikel 11

Reservförfaranden om det är tekniskt omöjligt att använda den europeiska sökportalen

1. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera av de EU-informationssystem eller i CIR, på grund av ett fel i ESP, ska ESP:s användare automatiskt underrättas av eu-Lisa.
2. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera EU-informationssystem eller i CIR, på grund av ett fel i en medlemsstats nationella infrastruktur, ska den medlemsstaten automatiskt underrätta eu-Lisa och kommissionen.
3. I de fall som avses i punkterna 1 och 2 i denna artikel 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 ska ha åtkomst till EU-informationssystem eller till CIR direkt när så krävs enligt unionsrätten eller nationell rätt.
4. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera EU-informationssystem eller i CIR, på grund av ett fel i en unionsbyrås infrastruktur, ska den byrå automatiskt underrätta eu-Lisa och kommissionen.

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 som erhållits från de biometriska uppgifter som avses i artikel 13, vilka är lagrade i CIR och SIS, och för möjliggörande av sökningar med biometriska uppgifter i flera EU-informationssystem för att stödja CIR och MID och målen för in- och utresesystemet, VIS, Eurodac, SIS och Ecris-TCN.

2. Den gemensamma biometriska matchningstjänsten ska bestå av följande:
 - a) En central infrastruktur som ska ersätta de centrala systemen för in- och utresesystemet, VIS, SIS, Eurodac respektive Ecris-TCN i den mån den ska lagra biometriska mallar och möjliggöra sökning med biometriska uppgifter.
 - b) En säker kommunikationsinfrastruktur mellan den gemensamma biometriska matchningstjänsten, centrala SIS och CIR.
3. eu-Lisa ska utveckla den gemensamma biometriska matchningstjänsten och säkerställa den tekniska förvaltningen.

Artikel 13

Lagring av biometriska mallar 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 20.3 w och y i förordning (EU) 2018/1862, med undantag för uppgifter om handavtryck.
- b) de uppgifter som avses i artikel 5.1 b och 5.2 i förordning (EU) 2019/816.

De biometriska mallarna ska lagras i den gemensamma biometriska matchningstjänsten i logiskt åtskild form enligt det EU-informationssystem från vilket uppgifterna härrör.

2. För varje uppsättning uppgifter som avses i punkt 1 ska varje biometrisk mall i den gemensamma biometriska matchningstjänsten innehålla en hänvisning till de EU-informationssystem i vilka de motsvarande biometriska uppgifterna lagras– och en hänvisning till de konkreta posterna i de EU-informationssystemen.

3. Biometriska mallar ska registreras i den gemensamma biometriska matchningstjänsten endast efter en automatisk kvalitetskontroll av de biometriska uppgifter som läggs in i ett av EU-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.

5. Kommissionen ska genom en genomförandeakt fastställa prestandakrav och praktiska arrangemang för att övervaka den gemensamma biometriska matchningstjänstens prestanda i syfte att säkerställa att effektiviteten i de biometriska sökningarna är förenlig med tidskritiska förfaranden, såsom in- och utresekontroller och identifieringar. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 14

Sökning på biometriska uppgifter med den gemensamma biometriska matchningstjänsten

För att söka på de biometriska uppgifter som lagrats i CIR 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 förordningarna (EG) nr 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 och (EU) 2019/816.

Artikel 15

Lagring av uppgifter i den gemensamma biometriska matchningstjänsten

De uppgifter som avses i artikel 13.1 och 13.2 ska endast lagras i den gemensamma biometriska matchningstjänsten under den tid som motsvarande biometriska uppgifter lagras i CIR eller SIS. Uppgifterna ska automatiskt raderas i den gemensamma biometriska matchningstjänsten.

*Artikel 16***Registerföring av loggar**

1. Utan att det påverkar tillämpningen av artiklarna 12 och 18 i förordning (EU) 2018/1862 och artikel 29 i förordning (EU) 2019/816 ska eu-Lisa föra logg över all uppgiftsbehandling i den gemensamma biometriska matchningstjänsten. Dessa loggar ska innehålla följande:

- a) Den medlemsstat eller unionsbyrå som inlett sökningen.
- b) Historiken för skapandet och lagringen av biometriska mallar.
- c) De EU-informationssystem som varit föremål för sökning med de biometriska mallar som lagrats i den gemensamma biometriska matchningstjänsten.
- d) Datum och tidpunkt för sökningen.
- e) Den typ av biometriska uppgifter som används för att inleda sökningen.
- f) Resultaten av sökningen och datum och tidpunkt för resultatet.

2. Varje medlemsstat ska föra logg över sökningar som utförs av dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda den gemensamma biometriska matchningstjänsten. Varje unionsbyrå ska föra logg över sökningar som utförs av dess vederbörligen bemyndigade personal.

3. De loggar som avses i punkterna 1 och 2 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 och dataintegritet. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats. För det fall de behövs för övervakningsförfaranden som redan har inletts ska de emellertid raderas så snart loggarna i fråga inte längre behövs för övervakningsförfarandena.

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 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 i enlighet med artikel 20, stödja funktionen av MID i enlighet med artikel 21 och underlätta och rationalisera de utsedda myndigheternas och Europols åtkomst till in- och utresesystemet, VIS, Etias och Eurodac, om det är nödvändigt för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i enlighet med artikel 22.

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 i den mån den ska lagra de uppgifter som avses i artikel 18.
- b) En säker kommunikationskanal mellan CIR, medlemsstaterna och de unionsbyråer som har rätt att använda CIR i enlighet med unionsrätten och nationell rätt.
- c) En säker kommunikationsinfrastruktur mellan CIR och in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN samt de centrala infrastrukturerna för ESP, den gemensamma biometriska matchningstjänsten och MID.

3. eu-Lisa ska utveckla CIR och säkerställa den tekniska förvaltningen.

4. Om det på grund av ett fel i CIR är tekniskt omöjligt att söka i CIR i syfte att identifiera en person i enlighet med artikel 20, för att spåra multipla identiteter i enlighet med artikel 21 eller i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i enlighet med artikel 22, ska CIR-användarna automatiskt underrättas av eu-Lisa.

5. eu-Lisa ska i samarbete med medlemsstaterna ta fram ett dokument för gränssnittskontroll för CIR på grundval av det universella meddelandeformat som avses i artikel 38.

*Artikel 18***Uppgifter i den gemensamma databasen för identitetsuppgifter**

1. CIR ska lagra följande uppgifter, logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör: De uppgifter som avses i artikel 5.1 b och 5.2 och följande uppgifter i artikel 5.1 a i förordning (EU) 2019/816: efternamn, förnamn, födelsedatum, födelseort (ort och land), medborgarskap (ett eller flera), kön, tidigare namn, i förekommande fall, pseudonymer eller alias samt, i förekommande fall, information om resehandlingar.
2. För varje uppsättning uppgifter som avses i punkt 1 ska CIR innehålla en hänvisning till de EU-informationssystem som uppgifterna tillhör.
3. De myndigheter som har åtkomst till CIR ska handla i enlighet med sina åtkomsträttigheter enligt de rättsliga instrument som reglerar EU-informationssystemen och enligt nationell rätt och i enlighet med sina åtkomsträttigheter enligt denna förordning för de syften som avses i artiklarna 20, 21 och 22.
4. För varje uppsättning uppgifter som avses i punkt 1 ska CIR innehålla en hänvisning till den konkreta post i EU-informationssystemen som uppgifterna tillhör.
5. 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 ska de uppgifter som avses i artikel 18 vilka lagras i personakten i CIR automatiskt läggas till, ändras eller raderas.
2. Om en vit eller en röd länk skapas i MID i enlighet med artikel 32 eller 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. Sökningar i CIR får utföras av en polismyndighet i enlighet med punkterna 2 och 5 endast under följande omständigheter:
 - a) Om en polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet.
 - b) Om det föreligger tvivel om de identitetsuppgifter som lämnats av en person.
 - c) Om det föreligger tvivel om äktheten i den resehandling eller en annan trovärdig handling som lämnats av en person.
 - d) Om det föreligger tvivel om identiteten på innehavaren av en resehandling eller en annan trovärdig handling.
 - e) Om en person inte kan eller vägrar att samarbeta.

Sådana sökningar ska inte tillåtas när det gäller minderåriga under 12 år, såvida det inte sker för barnets bästa.

2. Om någon av de omständigheter som förtecknas i punkt 1 uppstår och en polismyndighet har bemyndigats genom de nationella lagstiftningsåtgärder som avses i punkt 5, får myndigheten, endast i syfte att identifiera en person, söka i CIR med den personens biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro.
3. Om sökningen visar att uppgifter om denna person finns lagrade i CIR, ska medlemsstatens polismyndighet ha åtkomst för 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.

4. Om en polismyndighet har bemyndigats genom de nationella lagstiftningsåtgärder som avses i punkt 6, får den, i händelse av en naturkatastrof, en olycka eller ett terrordåd och endast i syfte att identifiera okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor, söka i CIR med dessa personers biometriska uppgifter.
5. Medlemsstater som vill utnyttja den möjlighet som anges i punkt 2 ska anta nationella lagstiftningsåtgärder. När medlemsstaterna gör detta ska de ta hänsyn till att ingen diskriminering av tredjelandsmedborgare får förekomma. I sådana lagstiftningsåtgärder ska de exakta syftena med identifieringen anges inom ramen för de mål som avses i artikel 2.1 b och c. De behöriga polismyndigheterna ska utses, och förfaranden, villkor och kriterier för sådana kontroller ska fastställas i dessa lagstiftningsåtgärder.
6. Medlemsstater som vill utnyttja den möjlighet som anges i punkt 4 ska anta nationella lagstiftningsåtgärder som fastställer förfarandena, villkoren och kriterierna.

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 den manuella verifieringen av olika identiteter i enlighet med artikel 29 enbart i verifieringssyfte ha åtkomst till de uppgifter som avses i artikel 18.1 och 18.2, som lagrats i CIR och som är kopplade genom 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 uppgifter som avses i artikel 18.1 och 18.2, som lagrats i CIR och som är kopplade genom en röd länk.

Artikel 22

Sökningar i den gemensamma databasen för identitetsuppgifter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott

1. Om det i ett specifikt fall finns rimliga skäl att anta att en sökning i EU-informationssystem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, särskilt om det finns misstankar om att en person som misstänks för, har begått eller utsatts för ett terroristbrott eller ett annat grovt brott är en person vars uppgifter lagras i Eurodac, får de utsedda myndigheterna och Europol söka i CIR för att få information om huruvida det finns uppgifter om en viss person i Eurodac.
2. Om ett svar på en sökning i CIR visar att det finns uppgifter om den personen i Eurodac ska CIR tillhandahålla de utsedda myndigheterna och Europol ett svar i form av en hänvisning som avses i artikel 18.2 som anger att Eurodac innehåller motsvarande uppgifter. CIR ska svara på ett sådant sätt att uppgifternas säkerhet inte äventyras.

Det svar som anger att uppgifter om personen i fråga förekommer i Eurodac får användas endast i syfte att lämna in en begäran om full åtkomst som omfattas av de villkor och förfaranden som fastställs i det rättsliga instrument där sådan åtkomst regleras.

I händelse av en eller flera träffar ska den utsedda myndigheten eller Europol begära full åtkomst till minst ett av de informationssystem i vilka en träff genererats.

Om sådan full åtkomst i undantagsfall inte begärs ska de utsedda myndigheterna registrera motiveringen till varför en begäran inte gjorts, som ska kunna spåras till den nationella akten. Europol ska registrera motiveringen i motsvarande ärende.

3. Fullständig åtkomst till uppgifterna i Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott omfattas fortfarande av de villkor och förfaranden som fastställs i det rättsliga instrument där sådan åtkomst regleras.

*Artikel 23***Lagring av uppgifter i den gemensamma databasen för identitetsuppgifter**

1. De uppgifter som avses i artikel 18.1, 18.2 och 18.4 ska automatiskt raderas från CIR i enlighet med bestämmelserna om lagring av uppgifter i förordning (EU) 2019/816.
2. Personakten ska lagras i CIR endast så länge de motsvarande uppgifterna lagras i minst ett av de EU-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 29 i förordning (EU) 2019/816 ska eu-Lisa föra logg över all uppgiftsbehandling i CIR i enlighet med punkterna 2, 3 och 4 i den här artikeln.
2. eu-Lisa ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 20 i CIR. Dessa loggar ska omfatta följande:
 - a) Den medlemsstat eller den unionsbyrå som inlett sökningen.
 - b) Syftet med användarens åtkomst för att söka via CIR.
 - c) Datum och tidpunkt för sökningen.
 - d) Den typ av uppgifter som används för att inleda sökningen.
 - e) Sökningens resultat.
3. eu-Lisa ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 21 i CIR. Dessa loggar ska omfatta följande:
 - a) Den medlemsstat eller den unionsbyrå som inlett sökningen.
 - a) Syftet med användarens åtkomst för att söka via CIR.
 - b) Datum och tidpunkt för sökningen.
 - c) I fall där en länk skapas, de uppgifter som används för att inleda sökningen, och sökningens resultat med angivelse av det EU-informationssystem som uppgifterna erhållits från.
4. eu-Lisa ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 22 i CIR. Dessa loggar ska omfatta följande:
 - a) Datum och tidpunkt för sökningen.
 - b) De uppgifter som används för att inleda sökningen.
 - c) Sökningens resultat.
 - d) Den medlemsstat eller den unionsbyrå som söker i CIR.

Loggarna över sådan åtkomst ska kontrolleras regelbundet av den behöriga tillsynsmyndigheten i enlighet med artikel 41 i direktiv (EU) 2016/680 eller av Europeiska datatillsynsmannen i enlighet med artikel 43 i förordning (EU) 2016/794, med högst sex månaders mellanrum, för att kontrollera om förfarandena och villkoren i artikel 22.1 och 22.2 i den här förordningen är uppfyllda.

5. Varje medlemsstat ska föra logg över sökningar som dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda CIR utför i enlighet med artiklarna 20, 21 och 22. Varje unionsbyrå ska föra logg över sökningar som dess vederbörligen bemyndigade personal utför i enlighet med artiklarna 21 och 22.

För all åtkomst till CIR i enlighet med artikel 22 ska varje medlemsstat dessutom föra logg över följande:

- a) Referensnummer för den nationella akten.
 - b) Syftet med åtkomsten.
 - c) I enlighet med nationella regler, den unika användaridentitet som anger vilken tjänsteman som utförde sökningen och vilken tjänsteman som beordrade sökningen.
6. I enlighet med förordning (EU) 2016/794 ska Europol för all åtkomst till CIR i enlighet med artikel 22 i den här förordningen föra logg över den unika användaridentitet som anger vilken tjänsteman som utförde sökningen och vilken tjänsteman som beordrade sökningen.
7. De loggar som avses i punkterna 2–6 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 och dataintegritet. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats. För det fall de behövs för övervakningsförfaranden som redan har inletts, ska de emellertid raderas så snart loggarna i fråga inte längre behövs för övervakningsförfarandena.
8. eu-Lisa ska lagra loggarna över historiken avseende uppgifterna i personakterna. eu-Lisa ska automatiskt radera sådana loggar 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 (MID) som skapar och lagrar akter med identitetsbekräftelse som avses i artikel 34, som innehåller länkar mellan uppgifter i de EU-informationssystem som ingår i CIR och SIS och som gör det möjligt att spåra 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.
2. MID ska bestå av följande:
 - a) En central infrastruktur som lagrar länkar och hänvisningar till EU-informationssystem.
 - b) En säker kommunikationsinfrastruktur som kopplar MID till SIS och ESP:s och CIR:s centrala infrastrukturer.
3. eu-Lisa ska utveckla MID och säkerställa den tekniska förvaltningen.

Artikel 26

Åtkomst till detektorn för multipla identiteter

1. För den manuella verifiering av olika identiteter som avses i artikel 29 ska åtkomst till de uppgifter som avses i artikel 34 och som är lagrade i MID beviljas
 - a) Sirenekontoret i den medlemsstat som skapar eller uppdaterar en registrering i enlighet med förordning (EU) 2018/1862,
 - b) de centrala myndigheterna i den dömande medlemsstaten vid registrering eller ändring av uppgifter i Ecris-TCN i enlighet med artikel 5 eller 9 i förordning (EU) 2019/816.
2. De myndigheter i medlemsstaterna och de unionsbyråer som har åtkomst till minst ett av de EU-informationssystem som ingår i CIR 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.
3. Myndigheterna i medlemsstaterna och unionsbyråerna ska ha åtkomst till de vita länkar som avses i artikel 33 om de har åtkomst till de två EU-informationssystem som innehåller uppgifter mellan vilka den vita länken skapats.
4. Myndigheterna i medlemsstaterna och unionsbyråerna ska ha åtkomst till de gröna länkar som avses i artikel 31 om de har åtkomst till de två EU-informationssystem som innehåller uppgifter mellan vilka den gröna länken skapats och en sökning i dessa informationssystem gett en träff med de två uppsättningarna länkade uppgifter.

Artikel 27

Spårning av multipla identiteter

1. Spårning av multipla identiteter ska i följande fall inledas i CIR och i SIS:
 - a) En registrering om en person skapas eller uppdateras i SIS i enlighet med kapitlen VI–IX i förordning (EU) 2018/1862.
 - b) En datapost skapas eller ändras i Ecris-TCN i enlighet med artikel 5 eller 9 i förordning (EU) 2019/816.
2. Om de uppgifter i ett EU-informationssystem som avses i punkt 1 innehåller biometriska uppgifter ska CIR och 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 person redan finns lagrade i CIR eller i centrala SIS.
3. Utöver det förfarande som avses i punkt 2 ska CIR och centrala SIS använda ESP för att söka i uppgifter som lagrats i centrala SIS respektive CIR med hjälp av följande uppgifter:
 - a) Efternamn, förnamn, namn vid födelsen, tidigare använda namn och alias, födelseort, födelsedatum, kön och samtliga medborgarskap enligt artikel 20.3 i förordning (EU) 2018/1862.
 - b) Efternamn, förnamn, födelsedatum, födelseort (ort och land), medborgarskap (ett eller flera) och kön enligt artikel 5.1 a i förordning (EU) 2019/816.
4. Utöver det förfarande som avses i punkterna 2 och 3 ska CIR och centrala SIS använda ESP för att söka i uppgifter som lagrats i centrala SIS respektive CIR med hjälp av resehandlingsuppgifter.
5. En spårning av multipla identiteter ska endast inledas för att jämföra tillgängliga uppgifter i ett EU-informationssystem med tillgängliga uppgifter i andra EU-informationssystem.

Artikel 28

Resultat av en spårning av multipla identiteter

1. Om de sökningar som avses i artikel 27.2, 27.3 och 27.4 inte ger någon träff ska de förfaranden som avses i artikel 27.1 fortsätta i enlighet med respektive de rättsliga instrument genom vilka de regleras.
2. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 ger en eller flera träffar ska CIR 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 uppgifterna 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, 27.3 och 27.4 ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är desamma eller liknande, ska en vit länk skapas i enlighet med artikel 33.
4. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 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 anta delegerade akter i enlighet med artikel 69 för att fastställa förfarandena för att avgöra ärenden där identitetsuppgifter kan anses vara desamma eller liknande.
6. Länkarna ska lagras i den akt med identitetsbekräftelse som avses i artikel 34.
7. Kommissionen ska, i samarbete med eu-Lisa, fastställa de tekniska reglerna för att skapa länkar mellan uppgifter från olika EU-informationssystem genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 29

Manuell verifiering av olika identiteter och ansvariga myndigheter

1. Utan att det påverkar tillämpningen av punkt 2 ska den myndighet som ansvarar för manuell verifiering av olika identiteter vara följande:

- a) Sirenekontoret i medlemsstaten för träffar som uppstår när en registrering i SIS skapas eller uppdateras i enlighet med förordning (EU) 2018/1862.
- b) De centrala myndigheterna i den dömande medlemsstaten för träffar som uppstår vid registrering eller ändring av uppgifter i Ecris-TCN i enlighet med artikel 5 eller 9 i förordning (EU) 2019/816.

MID ska ange den myndighet som ansvarar för den manuella verifieringen av olika identiteter i akten med identitetsbekräftelse.

2. Den myndighet som ansvarar för den manuella 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 en registrering om

- a) personer som är efterlysta för att gripas och överlämnas eller för att utlämnas enligt artikel 26 i förordning (EU) 2018/1862,
- b) försvunna eller sårbara personer enligt artikel 32 i förordning (EU) 2018/1862,
- c) personer som söks för att delta i ett rättsligt förfarande enligt artikel 34 i förordning (EU) 2018/1862,
- d) personer för diskreta kontroller, undersökningskontroller eller särskilda kontroller enligt artikel 36 i förordning (EU) 2018/1862.

3. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter ska ha åtkomst till de länkade uppgifterna i den relevanta akten med identitetsbekräftelse och till de identitetsuppgifter som är länkade i CIR och, i förekommande fall, i SIS. Den ska bedöma de olika identiteterna utan dröjsmål. När den bedömningen slutförts ska den uppdatera länken i enlighet med artiklarna 31, 32 och 33 samt utan dröjsmål lägga till den i akten med identitetsbekräftelse.

4. Om fler än en länk skapas ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter bedöma varje länk separat.

5. Om uppgifter som ger en träff redan var länkade, ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter beakta de befintliga länkarna vid bedömningen av skapandet av nya länkar.

Artikel 30

Gul länk

1. När en manuell verifiering av olika identiteter ännu inte har ägt rum, ska en länk mellan uppgifter från två eller flera EU-informationssystem klassificeras som gul i samtliga följande fall:

- a) De länkade uppgifterna innehåller samma biometriska uppgifter men har liknande eller olika identitetsuppgifter.
- b) De länkade uppgifterna har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter, och minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen.
- c) De länkade uppgifterna innehåller samma identitetsuppgifter men har olika biometriska uppgifter.
- d) De länkade uppgifterna har liknande eller olika identitetsuppgifter, och innehåller samma resehandlingsuppgifter men har olika biometriska uppgifter.

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 EU-informationssystem ska klassificeras som grön om
 - a) de länkade uppgifterna har olika biometriska uppgifter men innehåller samma identitetsuppgifter och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer,
 - b) de länkade uppgifterna har olika biometriska uppgifter, har liknande eller olika identitetsuppgifter, innehåller samma resehandlingsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer,
 - c) de länkade uppgifterna har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter, minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer.
2. Om en sökning görs i CIR eller SIS och om det finns en grön länk mellan två eller fler av EU-informationssystemen, ska MID ange att identitetsuppgifterna i de länkade uppgifterna inte gäller samma person.
3. Om en myndighet i en medlemsstat har bevis som tyder på att en grön länk har registrerats felaktigt i MID, att en grön länk är inaktuell eller att uppgifter behandlats i MID eller EU-informationssystemen i strid med denna förordning, ska den kontrollera de berörda uppgifterna i CIR och SIS och vid behov utan dröjsmål korrigera eller radera länken från MID. Myndigheten i medlemsstaten ska utan dröjsmål informera den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter.

*Artikel 32***Röd länk**

1. En länk mellan uppgifter från två eller flera EU-informationssystem ska klassificeras som röd i samtliga följande fall:
 - a) De länkade uppgifterna innehåller samma biometriska uppgifter men har liknande eller olika identitetsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till en och samma person på ett oberättigat sätt.
 - b) De länkade uppgifterna har samma, liknande eller olika identitetsuppgifter och har samma resehandlingsuppgifter men olika biometriska uppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer, av vilka åtminstone en person använder en och samma resehandling på ett oberättigat sätt.
 - c) De länkade uppgifterna innehåller samma identitetsuppgifter men har olika biometriska uppgifter och olika eller inga resehandlingsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer på ett oberättigat sätt.
 - d) De länkade uppgifterna har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter, minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till en och samma person på ett oberättigat sätt.
2. Om CIR eller SIS är föremål för sökning och om det finns en röd länk mellan uppgifter i två eller fler av EU-informationssystemen, ska MID ange de uppgifter som avses i artikel 34. En uppföljning av en röd länk ska ske i enlighet med unionsrätten och nationell rätt, och eventuella rättsliga följder för den berörda personen ska bygga uteslutande på de relevanta uppgifterna om personen i fråga. Inga rättsliga följder för den berörda personen ska uppstå enbart till följd av att det finns en röd länk.
3. Om det skapas en röd länk mellan uppgifter i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN ska den personakt som lagras i CIR uppdateras i enlighet med artikel 19.2.

4. Utan att det påverkar tillämpningen av bestämmelserna om hantering av registreringar i SIS i förordningarna (EU) 2018/1860, (EU) 2018/1861 och (EU) 2018/1862, och utan att det påverkar begränsningar som är nödvändiga för att trygga säkerheten och den allmänna ordningen, förebygga och förhindra brott samt garantera att inga nationella utredningar kommer att äventyras, ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter, vid skapandet av en röd länk, underrätta den berörda personen om förekomsten av multipla olagliga identitetsuppgifter, och ska tillhandahålla personen i fråga det enda identifikationsnummer som avses i artikel 34 c i den här förordningen, en referens till den myndighet som ansvarar för den manuella verifieringen av olika identiteter enligt artikel 34 d i den här förordningen samt webbadressen till den webbportal som upprättats i enlighet med artikel 49 i den här förordningen.

5. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter ska skriftligen tillhandahålla den information som avses i punkt 4 i form av ett standardformulär. Kommissionen ska genom genomförandeakter fastställa innehållet i och utformningen av det formuläret. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

6. När en röd länk skapas ska MID automatiskt underrätta de myndigheter som ansvarar för de länkade uppgifterna.

7. Om en myndighet i en medlemsstat eller en unionsbyrå som har åtkomst till CIR eller SIS har bevis som tyder på att en röd länk har registrerats felaktigt i MID eller att uppgifter behandlats i MID, CIR eller SIS i strid med denna förordning, ska den myndigheten eller byrån kontrollera relevanta uppgifter som lagras i CIR och SIS och ska

a) om länken avser en av de SIS-registreringar som avses i artikel 29.2, omedelbart informera det berörda Sirenekontoret i den medlemsstat som skapade SIS-registreringen,

b) i alla övriga fall, omedelbart korrigera eller radera länken från MID.

Om ett Sirenekontor kontaktas i enlighet med led a i första stycket ska det verifiera de bevis som lämnats av myndigheten i medlemsstaten eller unionsbyrån och, i tillämpliga fall, omedelbart korrigera eller radera länken från MID.

Den myndighet i medlemsstaten som erhåller bevisen ska utan dröjsmål underrätta den medlemsstats myndighet som ansvarar för den manuella verifieringen av olika identiteter och ange eventuella relevanta rättelser eller raderingar av en röd länk.

Artikel 33

Vit länk

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

a) De länkade uppgifterna innehåller samma biometriska uppgifter och samma eller liknande identitetsuppgifter.

b) De länkade uppgifterna innehåller samma eller liknande identitetsuppgifter och samma resehandlingsuppgifter, och minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen.

c) De länkade uppgifterna innehåller samma biometriska uppgifter, samma resehandlingsuppgifter och liknande identitetsuppgifter.

d) De länkade uppgifterna innehåller samma biometriska uppgifter men har liknande eller olika identitetsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till en och samma person på ett berättigat sätt.

2. Om CIR eller SIS är föremål för sökning och om det finns en vit länk mellan uppgifter i två eller fler av EU-informationssystemen, ska MID ange att identitetsuppgifterna i de länkade uppgifterna gäller samma person. De EU-informationssystem som är föremål för sökning ska svara genom att i förekommande fall ange alla länkade uppgifter om personen, vilket därigenom ger upphov till en träff mot de uppgifter som är länkade genom den vita länken, om den myndighet som inlett sökningen har åtkomst till de länkade uppgifterna enligt unionsrätten eller nationell rätt.

3. Om det skapas en vit länk mellan uppgifter i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN ska den personakt som lagras i CIR uppdateras i enlighet med artikel 19.2.

4. Utan att det påverkar tillämpningen av bestämmelserna om hantering av registreringar i SIS i förordningarna (EU) 2018/1860, (EU) 2018/1861 och (EU) 2018/1862, och utan att det påverkar begränsningar som är nödvändiga för att trygga säkerheten och den allmänna ordningen, förebygga och förhindra brott samt garantera att nationella utredningar inte kommer att äventyras, ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter, vid skapandet av en vit länk efter en manuell verifiering av multipla identiteter, underrätta den berörda personen om förekomsten av liknande eller olika identitetsuppgifter, och ska tillhandahålla personen i fråga det enda identifikationsnummer som avses i artikel 34 c i den här förordningen, en referens till den myndighet som ansvarar för den manuella verifieringen av olika identiteter i enlighet med artikel 34 d i den här förordningen samt webbadressen till den webbportal som upprättats i enlighet med artikel 49 i den här förordningen.

5. Om en myndighet i en medlemsstat har bevis som tyder på att en vit länk har registrerats felaktigt i MID, att en vit länk är inaktuell eller att uppgifter behandlats i MID eller EU-informationssystemen i strid med denna förordning, ska den kontrollera de berörda uppgifterna i CIR och SIS och vid behov utan dröjsmål korrigera eller radera länken från MID. Myndigheten i medlemsstaten ska utan dröjsmål informera den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter.

6. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter ska skriftligen tillhandahålla den information som avses i punkt 4 i form av ett standardformulär. Kommissionen ska genom genomförandeakter fastställa innehållet i och utformningen av det formuläret. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 34

Akt med identitetsbekräftelse

Akten med identitetsbekräftelse ska innehålla följande uppgifter:

- a) De länkar som avses i artiklarna 30–33.
- b) En hänvisning till de EU-informationssystem i vilka de länkade uppgifterna finns.
- c) Ett enda identifikationsnummer som gör det möjligt att hämta de länkade uppgifterna från de motsvarande EU-informationssystemen.
- d) Den myndighet som ansvarar för den manuella av olika identiteter.
- e) Datum för skapande av länken eller uppdatering därav.

Artikel 35

Lagring av uppgifter i detektorn för multipla identiteter

Akterna med identitetsbekräftelse och uppgifterna i dem, inbegripet länkarna, ska lagras i MID endast under den tid som de länkade uppgifterna lagras i två eller fler EU-informationssystem. De ska raderas automatiskt från MID.

Artikel 36

Registerföring av loggar

1. eu-Lisa ska föra logg över all uppgiftsbehandling som sker i MID. Dessa loggar ska omfatta följande:

- a) Den medlemsstat som inlett sökningen.
- b) Syftet med användarens åtkomst.
- c) Datum och tidpunkt för sökningen.
- d) Den typ av uppgifter som används för att inleda sökningen.
- e) Hänvisning till de länkade uppgifterna.
- f) Historik tillhörande akten med identitetsbekräftelse.

2. Varje medlemsstat ska föra logg över sökningar som dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda MID utför. Varje unionsbyrå ska föra logg över sökningar som utförs av dess vederbörligen bemyndigade personal.

3. De loggar som avses i punkterna 1 och 2 får endast användas för övervakning av dataskyddet, inbegripet kontroll av om en sökning är tillåten och om uppgifter har behandlats på ett lagligt sätt, och för att säkerställa datasäkerhet och dataintegritet. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats. För det fall de behövs för övervakningsförfaranden som redan har inletts, ska de raderas så snart de inte längre behövs för övervakningsförfarandena.

KAPITEL VI

Åtgärder till stöd för interoperabilitet

Artikel 37

Uppgifternas kvalitet

1. Utan att det påverkar medlemsstaternas ansvar för kvaliteten på de uppgifter som förs in i systemen ska eu-Lisa inrätta automatiska mekanismer och förfaranden för kontroll av uppgifternas kvalitet avseende de uppgifter som lagras i SIS, Eurodac, Ecris-TCN, den gemensamma biometriska matchningstjänsten och CIR.

2. eu-Lisa ska införa mekanismer för utvärdering av den gemensamma biometriska matchningstjänstens exakthet, gemensamma indikatorer för uppgifternas kvalitet samt minimikvalitetsstandarder för lagring av uppgifter i SIS, Eurodac, Ecris-TCN, den gemensamma biometriska matchningstjänsten och CIR.

Endast uppgifter som uppfyller minimikvalitetsstandarderna får föras in i SIS, Eurodac, Ecris-TCN, den gemensamma biometriska matchningstjänsten, CIR och MID.

3. eu-Lisa ska regelbundet tillhandahålla medlemsstaterna rapporter om de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet och de gemensamma indikatorerna för uppgifternas kvalitet. eu-Lisa ska också regelbundet tillhandahålla kommissionen en rapport om de problem som uppstått och vilka medlemsstater som berörts. eu-Lisa ska även på begäran överlämna denna rapport till Europaparlamentet och rådet. Inga rapporter som tillhandahålls i enlighet med denna punkt ska innehålla några personuppgifter.

4. Detaljerna om de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma indikatorerna för uppgifternas kvalitet samt minimikvalitetsstandarderna för lagring av uppgifter i SIS, Eurodac, Ecris-TCN, den gemensamma biometriska matchningstjänsten och CIR, särskilt vad gäller biometriska uppgifter, ska fastställas i genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

5. Ett år efter inrättandet av de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma indikatorerna för uppgifternas kvalitet samt minimikvalitetsstandarderna för uppgifter, 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, i synnerhet, problem med uppgiftskvalitet vilka härrör från felaktiga uppgifter i EU-informationssystem. Medlemsstaterna ska regelbundet rapportera till kommissionen 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, Europeiska dataskyddsstyrelsen och Europeiska unionens byrå för grundläggande rättigheter, som inrättades genom rådets förordning (EG) nr 168/2007⁽³⁷⁾.

Artikel 38

Universellt meddelandeformat

1. Härmed inrättas en standard för ett universellt meddelandeformat (UMF). Genom UMF definieras standarder för vissa innehållselement i det gränsöverskridande informationsutbytet mellan informationssystem, myndigheter eller organisationer på området rättsliga och inrikes frågor.

⁽³⁷⁾ 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).

2. UMF-standarden ska användas vid utvecklingen av Eurodac, Ecris-TCN, ESP, CIR, MID och, när så är lämpligt, eu-Lisas eller andra unionsbyråers utveckling av nya modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor.
3. Kommissionen ska anta en genomförandeakt för att fastställa och utveckla den UMF-standard som avses i punkt 1 i denna artikel. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

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 SIS, Eurodac och Ecris-TCN, i enlighet med de respektive rättsliga instrument som reglerar de systemen, och för att tillhandahålla systemöverskridande statistiska uppgifter och analysrapporter för politiska och operativa syften samt för uppgiftskvaliteten.
2. eu-Lisa ska inrätta, implementera och hysa i sina tekniska anläggningar CRRS som innehåller de uppgifter och den statistik som avses i artikel 74 i förordning (EU) 2018/1862 och artikel 32 i förordning (EU) 2019/816, logiskt åtskilda per EU-informationssystem. Åtkomst till CRRS ska beviljas via kontrollerad, säkrad åtkomst och specifika användarprofiler enbart för rapportering och statistik, till de myndigheter som avses i artikel 74 i förordning (EU) 2018/1862 och artikel 32 i förordning (EU) 2019/816
3. eu-Lisa ska anonymisera uppgifterna och registrera de anonymiserade uppgifterna i CRRS. Förfarandet för att anonymisera uppgifterna ska vara automatiskt.

Uppgifterna i CRRS ska inte möjliggöra identifiering av enskilda personer.

4. CRRS ska bestå av följande:
 - a) De verktyg som är nödvändiga för anonymisering av uppgifter.
 - b) En central infrastruktur som består av en databas med anonymiserade uppgifter.
 - c) En säker kommunikationsinfrastruktur för att ansluta CRRS till SIS, Eurodac och Ecris-TCN samt de centrala infrastrukturerna för den gemensamma biometriska matchningstjänsten, CIR och MID.
5. Kommissionen ska anta en delegerad akt i enlighet med artikel 69 för att fastställa detaljerade bestämmelser om driften av CRRS, inbegripet särskilda skyddsåtgärder för behandlingen av personuppgifter enligt punkterna 2 och 3 i den här artikeln och de säkerhetsregler som är tillämpliga på databasen.

KAPITEL VII

Dataskydd

Artikel 40

Personuppgiftsansvarig

1. När det gäller behandling av uppgifter i den gemensamma biometriska matchningstjänsten ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för Eurodac, SIS respektive Ecris-TCN vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 avseende de biometriska mallar som erhållits från de uppgifter som avses i artikel 13 i den här förordningen och som de för in i de underliggande systemen och ska ansvara för behandlingen av de biometriska mallarna i den gemensamma biometriska matchningstjänsten.
2. När det gäller behandling av uppgifter i CIR ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för Eurodac respektive Ecris-TCN vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 avseende de uppgifter som avses i artikel 18 i den här förordningen och som de för in i de underliggande systemen och ska ansvara för behandlingen av de personuppgifterna i CIR.
3. När det gäller behandling av uppgifter i MID gäller följande:
 - a) Europeiska gräns- och kustbevakningsbyrån ska vara personuppgiftsansvarig i den mening som avses i artikel 3.8 i förordning (EU) 2018/1725 när det gäller den behandling av personuppgifter som utförs av Etias centralenhet.
 - b) De av medlemsstaternas myndigheter som lägger till eller ändrar uppgifter i akten med identitetsbekräftelse ska vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 och ska ansvara för behandlingen av personuppgifter i MID.

4. För övervakningen av dataskyddet, inbegripet kontroll av om en sökning är tillåten och om uppgifter har behandlats på ett lagligt sätt, ska de personuppgiftsansvariga ha åtkomst till de loggar som avses i artiklarna 10, 16, 24 och 36 för egenkontroll enligt vad som avses i artikel 44.

Artikel 41

Personuppgiftsbiträde

När det gäller behandling av personuppgifter i den gemensamma biometrisk matchningstjänsten, CIR och MID ska eu-Lisa vara personuppgiftsbiträde i den mening som avses i artikel 3.12 a i förordning (EU) 2018/1725.

Artikel 42

Säkerhet vid behandling

1. eu-Lisa, Etias centralenhet, Europol och medlemsstaternas myndigheter ska säkerställa säkerheten vid den behandling av personuppgifter som äger rum enligt denna förordning. eu-Lisa, Etias centralenhet, Europol och medlemsstaternas myndigheter ska samarbeta kring säkerhetsrelaterade uppgifter.

2. Utan att det påverkar tillämpningen av artikel 33 i förordning (EU) 2018/1725 ska eu-Lisa vidta nödvändiga åtgärder för att säkerställa interoperabilitetskomponenternas och den relaterade kommunikationsinfrastrukturens säkerhet.

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 åtkomst till utrustning eller anläggningar för uppgiftsbehandling,
- c) förhindra obehörig läsning, kopiering, ändring eller obehörigt avlägsnande av datamedier,
- d) hindra obehörigt inmatning av uppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter,
- e) förhindra obehörig behandling av uppgifter och obehörig kopiering, ändring eller radering av uppgifter,
- f) hindra obehöriga från att med hjälp av datakommunikationsutrustning använda automatiserade system för uppgiftsbehandling,
- g) säkerställa att personer som har åtkomstbehörighet till interoperabilitetskomponenterna har åtkomst endast till de uppgifter för vilka de är behöriga och endast genom individuella användaridentiteter och skyddade åtkomstmetoder,
- h) säkerställa att det finns möjlighet att kontrollera och fastställa till vilka organ personuppgifter får överföras med hjälp av datakommunikationsutrustning,
- i) säkerställa att det finns möjlighet att kontrollera och fastställa vilka uppgifter som har behandlats i interoperabilitetskomponenterna, när detta har gjorts, av vem och i vilket syfte,
- j) 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,
- k) säkerställa att installerade system i händelse av driftavbrott kan återställas till normal drift,
- l) säkerställa driftsäkerhet genom att se till att eventuella driftfel hos interoperabilitetskomponenterna rapporteras på korrekt sätt,
- m) övervaka att de säkerhetsåtgärder som avses i denna punkt är verksamma och vidta nödvändiga organisatoriska åtgärder i fråga om intern övervakning för att säkerställa att denna förordning efterlevs och för att bedöma dessa säkerhetsåtgärder mot bakgrund av utvecklingen av ny teknik.

4. Medlemsstaterna, Europol och Etias centralenhet 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 rätt till åtkomst till någon av interoperabilitetskomponenterna.

*Artikel 43***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 om uppgifters tillgänglighet, integritet och konfidentialitet har äventyrats eller kan ha äventyrats.
2. Säkerhetstillbud ska hanteras på ett sätt som säkerställer snabba, effektiva och välavvägda motåtgärder.
3. Utan att det påverkar anmälan av och information om personuppgiftsincidenter i enlighet med artikel 33 i förordning (EU) 2016/679, artikel 30 i direktiv (EU) 2016/680, eller båda, ska medlemsstaterna utan dröjsmål underrätta kommissionen, eu-Lisa, de behöriga tillsynsmyndigheterna och Europeiska datatillsynsmannen om alla säkerhetstillbud.

Utan att det påverkar tillämpningen av artiklarna 34 och 35 i förordning (EU) 2018/1725 och artikel 34 i förordning (EU) 2016/794 ska Etias centralenhet och Europol utan dröjsmål underrätta kommissionen, eu-Lisa och Europeiska datatillsynsmannen om alla säkerhetstillbud.

Om ett säkerhetstillbud inträffar avseende interoperabilitetskomponenternas centrala infrastruktur ska eu-Lisa utan dröjsmål underrättakommissionen och Europeiska datatillsynsmannen.

4. Information om säkerhetstillbud som har eller kan ha inverkan på interoperabilitetskomponenternas drift eller på uppgifternas tillgänglighet, integritet och konfidentialitet ska utan dröjsmål tillhandahållas medlemsstaterna, Etias centralenhet samt Europol och rapporteras i enlighet med den incidenthanteringsplan som eu-Lisa ska tillhandahålla.
5. De berörda medlemsstaterna, Etias centralenhet, Europol 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 70.2.

*Artikel 44***Egenkontroll**

Medlemsstaterna och de relevanta unionsbyråerna ska se till 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, inklusive genom frekventa kontroller av de loggar som avses i artiklarna 10, 16, 24 och 36, och vid behov samarbeta med tillsynsmyndigheterna och med Europeiska datatillsynsmannen.

*Artikel 45***Sanktioner**

Medlemsstaterna ska se till att missbruk av uppgifter eller behandling eller utbyte av uppgifter i strid med denna förordning är belagt med sanktioner i enlighet med nationell rätt. Sanktionerna ska vara effektiva, proportionella och avskräckande.

*Artikel 46***Skadeståndsansvar**

1. Utan att det påverkar rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet, eller dessas skadeståndsansvar i enlighet med förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725, ska följande gälla:
 - a) Varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en otillåten behandling av personuppgifter eller av någon annan åtgärd från en medlemsstats sida som är oförenlig med denna förordning ska ha rätt till ersättning från den berörda medlemsstaten.

- b) Varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en åtgärd från Europol, Europeiska gräns- och kustbevakningsbyråns eller eu-Lisas sida som är oförenlig med denna förordning ska ha rätt till ersättning från byrån i fråga.

Den berörda medlemsstaten, Europol, Europeiska gräns- och kustbevakningsbyrån eller eu-Lisa ska helt eller delvis undantas från sitt skadeståndsansvar enligt första stycket om de bevisar att de inte är ansvariga för den händelse som orsakade skadan.

2. Om en medlemsstats underlåtenhet att fullgöra sina skyldigheter i enlighet med denna förordning skadar interoperabilitetskomponenterna, ska den medlemsstaten vara ansvarig för denna skada, såvida inte och i den mån eu-Lisa eller en annan medlemsstat som är bunden av denna förordning har underlåtit att vidta rimliga åtgärder för att hindra skadan från att uppstå eller för att begränsa dess verkningar.

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

Artikel 47

Rätt till information

1. Den myndighet som samlar in de personuppgifter som ska lagras i den gemensamma biometrisk matchnings-tjänsten, CIR eller MID ska tillhandahålla de personer vars uppgifter insamlas den information som krävs enligt artiklarna 13 och 14 i förordning (EU) 2016/679, artiklarna 12 och 13 i förordning (EU) 2016/680 samt artiklarna 15 och 16 i förordning (EU) 2018/1725. Myndigheten ska tillhandahålla informationen vid den tidpunkt då uppgifterna samlas in.

2. All information ska göras tillgänglig med hjälp av ett klart och tydligt språkbruk i en språkversion som den berörda personen förstår eller rimligen kan förväntas förstå. Detta ska innefatta att information tillhandahålls på ett sätt som är lämpligt med hänsyn till åldern för registrerade personer som är minderåriga.

3. Bestämmelserna om rätten till information i unionens tillämpliga dataskyddsregler ska tillämpas på personuppgifter som har registrerats i Ecris-TCN och behandlas i enlighet med denna förordning.

Artikel 48

Rätt till åtkomst till, rättelse och radering av samt begränsning av behandlingen av personuppgifter som lagras i MID

1. För att utöva sina rättigheter enligt artiklarna 15–18 i förordning (EU) 2016/679, artiklarna 17–20 i förordning (EU) 2018/1725 samt artiklarna 14, 15 och 16 i direktiv (EU) 2016/680 ska varje person ha rätt att vända sig till den behöriga myndigheten i vilken medlemsstat som helst, som ska pröva och besvara begäran.

2. Den medlemsstat som prövar en sådan begäran ska svara utan otillbörligt dröjsmål, dock senast inom 45 dagar efter mottagandet. Denna period får vid behov förlängas med ytterligare 15 dagar, med beaktande av hur komplicerade och hur många begärandena är. Den medlemsstat som prövar begäran ska underrätta den registrerade om en sådan förlängning inom 45 dagar efter mottagandet av begäran och ange orsakerna till förseningen. Medlemsstaterna får besluta att dessa svar ska lämnas av centralenheter.

3. Om en begäran om rättelse eller radering av personuppgifter ställs till en annan medlemsstat än den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter ska den medlemsstat till vilken begäran ställts inom sju dagar kontakta myndigheterna i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter. Den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter ska utan otillbörligt dröjsmål, dock senast inom 30 dagar från en sådan kontakt, kontrollera om uppgifterna är korrekta och om de har behandlats på ett lagligt sätt. Denna period får vid behov förlängas med ytterligare 15 dagar, med beaktande av hur komplicerade och hur många begärandena är. Den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter ska underrätta den medlemsstat som kontaktade denna om en sådan förlängning samt orsakerna till förseningen. Den berörda personen ska informeras av den medlemsstat som kontaktade myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter om det fortsatta förfarandet.

4. Om en begäran om rättelse eller radering av personuppgifter ställs till en medlemsstat där Etias centralenhet ansvarade för den manuella verifieringen av olika identiteter, ska den medlemsstat till vilken begäran ställdes kontakta Etias centralenhet inom sju dagar och begära att den avger ett yttrande. Etias centralenhet ska avge sitt yttrande utan otillbörligt dröjsmål, dock senast inom 30 dagar efter det att den kontaktades. Denna period får vid behov förlängas med ytterligare 15 dagar, med beaktande av hur komplicerade och hur många begärandena är. Den berörda personen ska informeras om det fortsatta förfarandet av den medlemsstat som kontaktade Etias centralenhet.
5. Om det, efter en prövning, visar sig att de uppgifter som lagrades i MID är oriktiga eller har registrerats på ett olagligt sätt, ska den medlemsstat som ansvarade för den manuella verifieringen av olika identiteter eller – om det inte fanns någon medlemsstat som ansvarade för den manuella verifieringen av olika identiteter eller om Etias centralenhet ansvarade för den manuella verifieringen av olika identiteter – den medlemsstat till vilken begäran har ställts utan otillbörligt dröjsmål rätta eller radera dessa uppgifter. Den berörda personen ska informeras skriftligen om att hans eller hennes uppgifter har rättats eller raderats.
6. Om uppgifter som lagras i MID ändras av en medlemsstat under lagringsperioden, ska den 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 medlemsstaten radera uppgifterna från akten med identitetsbekräftelse. Om den automatiska behandlingen ger en eller flera träffar ska den medlemsstaten skapa eller uppdatera den relevanta länken i enlighet med de relevanta bestämmelserna i denna förordning.
7. Om den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts inte instämmer i att uppgifter som lagras i MID är oriktiga eller har registrerats på ett olagligt sätt, ska den medlemsstaten utan dröjsmål anta ett administrativt beslut med en skriftlig förklaring till den berörda personen om varför den inte är beredd att rätta eller radera uppgifter som rör honom eller henne.
8. Det beslut som avses i punkt 7 ska även ge den berörda personen information om möjligheten att invända mot det beslut som fattats med avseende på begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter 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 tillsynsmyndigheterna.
9. En begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter ska innehålla den information som behövs för att den berörda personen ska kunna identifieras. Denna information ska användas uteslutande för att de rättigheter som avses i denna artikel ska kunna utövas och ska sedan omedelbart raderas.
10. Den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts ska spara skriftlig dokumentation av att en begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter har gjorts och hur den behandlats, och ska utan dröjsmål tillhandahålla tillsynsmyndigheterna denna dokumentation.
11. Denna artikel påverkar inte begränsningar och inskränkningar av de rättigheter som anges i denna artikel i enlighet med förordning (EU) 2016/679 och direktiv (EU) 2016/680.

Artikel 49

Webbportal

1. En webbportal inrättas för att underlätta utövandet av rätten till åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter.
2. Webbportalen ska innehålla information om de rättigheter och förfaranden som avses i artiklarna 47 och 48 och ett användargränssnitt som gör det möjligt för personer vars uppgifter behandlas i MID och som underrättats om förekomsten av en röd länk i enlighet med artikel 32.4 att få kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter.
3. För att få kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter bör den person vars uppgifter behandlas i MID uppges referensen för den myndighet som ansvarar för den manuella verifieringen av olika identiteter enligt vad som avses i artikel 34 d. Webbportalen ska använda denna referens för att hämta kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter. Webbportalen ska också inkludera en mall för ett e-postmeddelande för att underlätta kommunikationen mellan portalanvändaren och den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter. Detta e-postmeddelande ska innehålla ett fält för det enda identifikationsnummer som avses i artikel 34 c, så att den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter kan identifiera de berörda uppgifterna.

4. Medlemsstaterna ska ge eu-Lisa kontaktuppgifter till alla myndigheter som är behöriga att pröva och besvara varje sådan begäran som avses i artiklarna 47 och 48 och ska regelbundet se över huruvida dessa kontaktuppgifter är aktuella.
5. eu-Lisa ska utveckla webbportalen och säkerställa dess tekniska förvaltning.
6. Kommissionen ska anta en delegerad akt i enlighet med artikel 69 för att fastställa närmare bestämmelser om driften av webbportalen, inklusive användargränssnittet, de språk på vilka webbportalen ska finnas tillgänglig och e-postmallen.

Artikel 50

Överföring av personuppgifter till tredjeländer, internationella organisationer och privata parter

Utan att det påverkar tillämpningen av artikel 31 i förordning (EG) nr 767/2008, artiklarna 25 och 26 i förordning (EU) 2016/794, artikel 41 i förordning (EU) 2017/2226, artikel 65 i förordning (EU) 2018/1240 eller sökning via ESP i enlighet med artikel 9.5 i den här förordningen i de av Interpols databaser vilka uppfyller bestämmelserna i kapitel V i förordning (EU) 2018/1725 och kapitel V i förordning (EU) 2016/679 får personuppgifter som lagras eller behandlas i interoperabilitetskomponenterna eller till vilka interoperabilitetskomponenterna fått åtkomst inte överföras till eller göras tillgängliga för tredjeländer, internationella organisationer eller privata parter.

Artikel 51

Tillsynsmyndigheternas övervakning

1. Varje medlemsstat ska se till att tillsynsmyndigheterna på ett oberoende sätt övervakar lagligheten i den berörda medlemsstatens behandling av personuppgifter enligt den här förordningen, inklusive överföringen av dem till och från interoperabilitetskomponenterna.
2. Varje medlemsstat ska se till att de nationella lagar, föreskrifter och administrativa bestämmelser som antas i enlighet med direktiv (EU) 2016/680 vid behov är tillämpliga också på polismyndigheters och utsedda myndigheters åtkomst till interoperabilitetskomponenterna, även med avseende på rättigheterna för de personer vars uppgifter åtkomsten gäller.
3. Tillsynsmyndigheterna ska säkerställa att en revision av den behandling av personuppgifter som utförs av de ansvariga nationella myndigheterna vid tillämpningen av denna förordning genomförs i enlighet med relevanta internationella revisionsstandarder minst vart fjärde år.

Tillsynsmyndigheterna ska varje år offentliggöra antalet begäranden om rättelse, radering eller begränsning av behandling av personuppgifter, åtgärder som vidtagits till följd av detta och antalet rättelser, raderingar eller begränsningar av behandling som gjorts till följd av begärandena från de berörda personerna.

4. Medlemsstaterna ska se till att deras tillsynsmyndigheter har de resurser och den expertis som krävs för att fullgöra de uppgifter som de åläggs enligt denna förordning.
5. Medlemsstaterna ska tillhandahålla all information som begärs av en sådan tillsynsmyndighet som avses i artikel 51.1 i förordning (EU) 2016/679 och ska i synnerhet förse den med information om verksamhet som bedrivs i enlighet med deras ansvarsområden enligt den här förordningen. Medlemsstaterna ska bevilja de tillsynsmyndigheter som avses i artikel 51.1 i förordning (EU) 2016/679 åtkomst till de loggar som avses i artiklarna 10, 16, 24 och 36 i den här förordningen och till de motiveringar som avses i artikel 22.2 i den här förordningen och när som helst bereda dem tillträde till alla sina lokaler som används för interoperabilitetsändamål.

Artikel 52

Europeiska datatillsynsmannens revisioner

Europeiska datatillsynsmannen ska säkerställa att en revision av eu-Lisas, Etias centralenhets och Europolns behandling av personuppgifter vid tillämpningen av denna förordning genomförs i enlighet med relevanta internationella revisionsstandarder minst vart fjärde år. En rapport om revisionen ska sändas till Europaparlamentet, rådet, eu-Lisa, kommissionen, medlemsstaterna och den berörda unionsbyrån. eu-Lisa, Etias centralenhet och Europol ska ges tillfälle att yttra sig innan rapporterna antas.

eu-Lisa, Etias centralenhet och Europol ska tillhandahålla Europeiska datatillsynsmannen den information som denna begär, ge Europeiska datatillsynsmannen tillgång till alla handlingar som den begär och åtkomst till sina loggar enligt vad som avses i artiklarna 10, 16, 24 och 36 samt när som helst bereda Europeiska datatillsynsmannen tillträde till alla sina lokaler.

Artikel 53

Samarbete mellan tillsynsmyndigheterna och Europeiska datatillsynsmannen

1. Tillsynsmyndigheterna och Europeiska datatillsynsmannen ska, var och en inom ramen för sina respektive befogenheter, aktivt samarbeta inom ramen för sina respektive ansvarsområden och säkerställa en samordnad tillsyn av användningen av interoperabilitetskomponenterna och tillämpningen av övriga bestämmelser i denna förordning, i synnerhet om Europeiska datatillsynsmannen eller en tillsynsmyndighet upptäcker stora skillnader mellan praxis i medlemsstaterna eller upptäcker eventuellt olagliga överföringar genom interoperabilitetskomponenternas kommunikationskanaler.
2. I de fall som avses i punkt 1 i den här artikeln ska en samordnad tillsyn säkerställas i enlighet med artikel 62 i förordning (EU) 2018/1725.
3. Europeiska dataskyddsstyrelsen ska senast den 12 juni 2021, och därefter vartannat år, skicka en gemensam rapport om sina aktiviteter enligt denna artikel till Europaparlamentet, rådet, kommissionen, Europol, Europeiska gräns- och kustbevakningsbyrån och eu-Lisa. Denna rapport ska innehålla ett kapitel om varje medlemsstat som utarbetats av den berörda medlemsstatens tillsynsmyndighet.

KAPITEL VIII

Ansvarsområden

Artikel 54

eu-Lisas ansvarsområden 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 prestanda som anges i artikel 55.1.
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, ESP, den gemensamma biometriska matchningstjänsten, CIR, MID och CRRS.

Utan att det påverkar tillämpningen av artikel 62 ska eu-Lisa inte ha tillgång till några av de personuppgifter som behandlas i ESP, den gemensamma biometriska matchningstjänsten, CIR eller MID.

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 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 28.7, 37.4, 38.3, 39.5, 43.5 och 74.10.

Utvecklingen ska bestå i att utarbeta och genomföra de tekniska specifikationerna, testerna och den övergripande projektledningen och projektsamordningen.

4. En förvaltningsgrupp för programmet bestående av högst tio medlemmar ska inrättas under utformnings- och utvecklingsfasen. Den ska bestå av sju medlemmar som utses av eu-Lisas styrelse bland dess ledamöter eller ställföreträdare, ordföranden för den rådgivande grupp för interoperabilitet som avses i artikel 71, en medlem som företräder eu-Lisa och som utses av dess verkställande direktör samt en medlem som utses av kommissionen. De medlemmar som utses av eu-Lisas styrelse ska väljas enbart från de medlemsstater som enligt unionsrätten fullt ut omfattas av de rättsliga instrument som reglerar utveckling, inrättande, drift och användning av samtliga EU-informationssystem 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 hantering av interoperabilitetskomponenternas utformnings- och utvecklingsfas.

Förvaltningsgruppen för programmet ska varje månad lämna skriftliga rapporter till eu-Lisas styrelse om projektets framsteg. Förvaltningsgruppen för programmet ska varken ha befogenhet att fatta beslut eller mandat att företräda ledamöterna i eu-Lisas styrelse.

6. eu-Lisas styrelse ska fastställa arbetsordningen för förvaltningsgruppen för programmet, vilken i synnerhet 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 rättsliga instrument som reglerar utveckling, inrättande, drift och användning av samtliga EU-informationssystem och som kommer att delta i interoperabilitetskomponenterna.

Medlemmarna i förvaltningsgruppen för programmet ska få alla sina utgifter för resa och uppehälle ersatta av eu-Lisa, och artikel 10 i eu-Lisas arbetsordning ska gälla i tillämpliga delar. eu-Lisa ska tillhandahålla förvaltningsgruppen ett sekretariat.

Den rådgivande grupp för interoperabilitet som avses i artikel 71 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 55

eu-Lisas ansvarsområden 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 för interoperabilitetskomponenterna, inbegripet underhållet av dem och den tekniska utvecklingen. I samarbete med medlemsstaterna ska byrån se till att bästa tillgängliga teknik används, 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 och tekniska lösningar som krävs för att interoperabilitetskomponenterna ska kunna fungera och tillhandahålla medlemsstaterna och unionsbyråerna oavbruten service dygnet runt alla dagar i veckan i enlighet med denna förordning. Den ska inbegripa det underhåll och den tekniska utveckling som krävs för att komponenterna ska fungera med tillfredsställande teknisk kvalitet, särskilt vad gäller svarstiden vid sökningar i de centrala infrastrukturerna i enlighet med de tekniska specifikationerna.

Alla interoperabilitetskomponenter ska utvecklas och förvaltas på ett sätt som säkerställer snabb, smidig, effektiv och kontrollerad åtkomst samt fullständig och oavbruten tillgänglighet till de komponenter och uppgifter som lagras i MID, den gemensamma biometriska matchningstjänsten och CIR, liksom en svarstid i linje med medlemsstaternas myndigheters och unionsbyråernas operativa behov.

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 konfidentialitetskrav på all personal som arbetar med uppgifter som lagras i interoperabilitetskomponenterna. Denna skyldighet ska gälla även efter det att den anställda i fråga lämnat sin tjänst eller anställning eller upphört med sin verksamhet.

Utan att det påverkar tillämpningen av artikel 62 ska eu-Lisa inte ha tillgång till några av de personuppgifter som behandlas i ESP, den gemensamma biometriska matchningstjänsten, CIR och MID.

3. eu-Lisa ska utveckla och underhålla en mekanism och förfaranden för att genomföra kvalitetskontroller av de uppgifter som lagras i den gemensamma biometriska matchningstjänsten och CIR i enlighet med artikel 37.

4. eu-Lisa ska också utföra uppgifter avseende tillhandahållandet av utbildning om interoperabilitetskomponenternas tekniska användning.

*Artikel 56***Medlemsstaternas ansvarsområden**

1. Varje medlemsstat ska ansvara för följande:
 - a) Anslutning av till ESP:s och CIR:s kommunikationsinfrastruktur.
 - b) Integration av de befintliga nationella systemen och infrastrukturerna med ESP, CIR och MID.
 - 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 personal vid de behöriga nationella myndigheterna till ESP, CIR och MID i enlighet med denna förordning och upprättande och regelbunden uppdatering av en förteckning över denna personal och deras profiler.
 - e) Antagande av de lagstiftningsåtgärder som avses i artikel 20.5 och 20.6 för att få åtkomst till CIR i identifieringssyfte.
 - f) Den manuella verifiering av olika identiteter som avses i artikel 29.
 - g) Efterlevnad av de krav på uppgiftskvalitet som fastställs i unionsrätten.
 - h) Efterlevnad av reglerna i varje EU-informationssystem beträffande personuppgifternas säkerhet och integritet.
 - i) Avhjälpan av eventuella brister som konstaterats i kommissionens utvärderingsrapport om uppgifternas kvalitet som avses i artikel 37.5.
2. Varje medlemsstat ska ansluta sina utsedda myndigheter till CIR.

*Artikel 57***Europolns ansvarsområden**

1. Europol ska säkerställa att ESP behandlar sökningarna i Europoluppgifter. Europol 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 arrangemangen för, dess vederbörligen bemyndigade personals användning av och åtkomst till ESP och CIR enligt denna förordning samt upprättandet och regelbunden uppdatering av en förteckning över denna personal och deras profiler.

*Artikel 58***Etias centralenhets ansvarsområden**

Etias centralenhet ska ansvara för följande:

- a) Den manuella verifieringen av olika identiteter i enlighet med artikel 29.
- b) Genomförande av en spårning av multipla identiteter bland de uppgifter som lagras i in- och utresesystemet, VIS, Eurodac och SIS enligt vad som avses i artikel 65.

KAPITEL IX**Ändringar av andra unionsinstrument***Artikel 59***Ändringar av förordning (EU) 2018/1726**

Förordning (EU) 2018/1726 ska ändras på följande sätt:

1. Artikel 12 ska ersättas med följande:

”Artikel 12

Uppgifternas kvalitet

1. Utan att det påverkar medlemsstaternas ansvar för de uppgifter som förs in i systemen under byråns operativa ansvar ska byrån, i nära samarbete med sina rådgivande grupper, för alla system under byråns operativa ansvar inrätta automatiska mekanismer och förfaranden för kontroll av uppgifternas kvalitet, gemensamma uppgiftskvalitetsindikatorer och minimikvalitetsstandarder för att lagra uppgifter, i enlighet med de relevanta bestämmelserna i de rättsliga instrument som reglerar de informationssystemen och i artikel 37 i Europaparlamentets och rådets förordningar (EU) 2019/817 (*) och (EU) 2019/818 (**).

2. Byrån ska inrätta en central databas som innehåller enbart anonymiserade uppgifter för rapporter och statistik i enlighet med artikel 39 i förordningarna (EU) 2019/817 och (EU) 2019/818, som omfattas av särskilda bestämmelser i de rättsliga instrument som reglerar utveckling, inrättande, drift och användning av stora it-system som byrån förvaltar.

(*) Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726, och (EU) 2018/1861, samt rådets beslut 2004/512/EG och 2008/633/RIF (EUT L 135, 22.5.2019, s. 27).

(**) Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och rättsligt samarbete, asyl och migration och om ändring av Europaparlamentets och rådets förordningar (EU) nr 603/2013, (EU) 2018/1862, (EU) 2019/816 och (EU) 2018/1726 (EUT L 135, 22.5.2019, s. 85)."

2. Artikel 19.1 ska ändras på följande sätt:

a) Följande led ska införas:

"eea) Anta rapporter om hur interoperabilitetskomponenternas utveckling fortskrider i enlighet med artikel 78.2 i förordning (EU) 2019/817 och artikel 74.2 i förordning (EU) 2019/818."

b) Led ff ska ersättas med följande:

"ff) Anta rapporter om den tekniska funktionen hos SIS i enlighet med artikel 60.7 i Europaparlamentets och rådets förordning (EU) 2018/1861 (*) och artikel 74.8 i Europaparlamentets och rådets förordning (EU) 2018/1862 (**), hos VIS i enlighet med artikel 50.3 i förordning (EG) nr 767/2008 och artikel 17.3 i beslut 2008/633/RIF, hos in- och utresesystemet i enlighet med artikel 72.4 i förordning (EU) 2017/2226, hos Etias i enlighet med artikel 92.4 i förordning (EU) 2018/1240, hos Ecris-TCN och hos Ecris genomförande-hänvisning enligt artikel 36.8 i Europaparlamentets och rådets förordning (EU) 2019/816 (***) samt hos interoperabilitetskomponenterna i enlighet med artikel 78.3 i förordning (EU) 2019/817, och i artikel 74.3 i förordning (EU) 2019/818.

(*) Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006 (EUT L 312, 7.12.2018, s. 14).

(**) Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU (EUT L 312, 7.12.2018, s. 56).

(***) Europaparlamentets och rådets förordning (EU) 2019/816 av den 17 april 2019 om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN) för att komplettera och stödja det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726 (EUT L 135, 22.5.2019, s. 1)."

c) Led hh ska ersättas med följande:

"hh) Anta formella kommentarer om Europeiska datatillsynsmannens granskningsrapporter enligt artikel 56.2 i förordning (EU) 2018/1861, artikel 42.2 i förordning (EG) nr 767/2008, artikel 31.2 i förordning (EU) nr 603/2013, artikel 56.2 i förordning (EU) 2017/2226, artikel 67 i förordning (EU) 2018/1240, artikel 29.2 i förordning (EU) 2019/816 och artikel 52 i förordningarna (EU) 2019/817 och (EU) 2019/818 samt säkerställa lämplig uppföljning av granskningarna."

d) Led mm ska ersättas med följande:

"mm) Årligen offentliggöra förteckningen över behöriga myndigheter som har tillstånd att direkt söka uppgifter i SIS enligt artikel 41.8 i förordning (EU) nr 2018/1861 och artikel 56.7 i förordning (EU) 2018/1862, tillsammans med förteckningen över kontoren i de nationella SIS-systemen (N.SIS) och Sirenekontoren enligt artikel 7.3 i förordning (EU) 2018/1861 respektive artikel 7.3 i förordning (EU) 2018/1862, liksom förteckningen över behöriga myndigheter enligt artikel 65.2 i förordning (EU) 2017/2226, förteckningen över behöriga myndigheter enligt artikel 87.2 i förordning (EU) 2018/1240, förteckningen över centrala myndigheter enligt artikel 34.2 i förordning (EU) 2019/816 samt förteckningen över myndigheter enligt artikel 71.1 i förordning (EU) 2019/817 och artikel 67.1 i förordning (EU) 2019/818."

3. Artikel 22.4 ska ersättas med följande:

"4. Europol och Eurojust får delta i styrelsens möten som observatörer när en fråga rörande SIS II angående tillämpningen av beslut 2007/533/RIF står på dagordningen.

Europeiska gräns- och kustbevakningsbyrån får delta i styrelsens möten som observatör när en fråga rörande SIS angående tillämpningen av förordning (EU) 2016/1624 står på dagordningen.

Europol får delta i styrelsens möten som observatör när en fråga rörande VIS angående tillämpningen av beslut 2008/633/RIF, eller en fråga rörande Eurodac angående tillämpningen av förordning (EU) nr 603/2013, står på dagordningen.

Europol får delta i styrelsens möten som observatör när en fråga rörande in- och utresesystemet angående tillämpningen av förordning (EU) 2017/2226 står på dagordningen eller när en fråga rörande Etias angående tillämpningen av förordning (EU) 2018/1240 står på dagordningen.

Europeiska gräns- och kustbevakningsbyrån får delta i styrelsens möten som observatör när en fråga rörande Etias angående tillämpningen av förordning (EU) 2018/1240 står på dagordningen.

Eurojust, Europol och Europeiska åklagarmyndigheten får delta i styrelsens möten som observatörer när en fråga rörande förordning (EU) 2019/816 står på dagordningen.

Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån får delta i styrelsens möten som observatörer när en fråga rörande förordningarna (EU) 2019/817 och (EU) 2019/818 står på dagordningen.

Styrelsen får bjuda in alla personer vars åsikter kan vara av intresse att delta som observatörer vid mötena."

4. I artikel 24.3 ska led p ersättas med följande:

"p) Utan att det påverkar tillämpningen av artikel 17 i tjänsteföreskrifterna för tjänstemän fastställa krav avseende konfidentiell behandling som överensstämmer med artikel 17 i förordning (EG) nr 1987/2006, artikel 17 i beslut 2007/533/RIF, artikel 26.9 i förordning (EG) nr 767/2008, artikel 4.4 i förordning (EU) nr 603/2013, artikel 37.4 i förordning (EU) 2017/2226, artikel 74.2 i förordning (EU) 2018/1240, artikel 11.16 i förordning (EU) 2019/816 och artikel 55.2 i förordningarna (EU) 2019/817 och (EU) 2019/818."

5. Artikel 27 ska ändras på följande sätt:

a) I punkt 1 ska följande led införas:

"da) Den rådgivande gruppen för interoperabilitet."

b) Punkt 3 ska ersättas med följande:

"3. Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån får utnämna var sin företrädare i den rådgivande gruppen för SIS II.

Europol får också utnämna en företrädare i de rådgivande grupperna för VIS, Eurodac respektive in- och utresesystemet och Etias.

Europeiska gräns- och kustbevakningsbyrån får också utnämna en företrädare i den rådgivande gruppen för in- och utresesystemet och Etias.

Eurojust, Europol och Europeiska åklagarmyndigheten får utnämna var sin företrädare i den rådgivande gruppen för Ecris-TCN.

Europol, Eurojust och Europeiska gräns- och kustbevakningsbyrån får utnämna var sin företrädare i den rådgivande gruppen för interoperabilitet."

Artikel 60

Ändringar av förordning (EU) 2018/1862

Förordning (EU) 2018/1862 ska ändras på följande sätt:

1. I artikel 3 ska följande led läggas till:

- ”18. ESP: den europeiska sökportal som inrättas genom artikel 6.1 i Europaparlamentets och rådets förordning (EU) 2019/818 (*),
- 19. *den gemensamma biometriska matchningstjänsten*: den gemensamma biometriska matchningstjänst som inrättas genom artikel 12.1 i förordning (EU) 2019/818,
- 20. CIR: den gemensamma databas för identitetsuppgifter som inrättas genom artikel 17.1 i förordning (EU) 2019/818,
- 21. MID: den detektor för multipla identiteter som inrättas genom artikel 25.1 i förordning (EU) 2019/818,

(*) Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och rättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816 (EUT L 135, 22.5.2019, s. 85).”

2. Artikel 4 ska ändras på följande sätt:

a) I punkt 1 ska leden b och c ersättas med följande:

- ”b) Ett nationellt system (nedan kallat N.SIS) i var och en av medlemsstaterna, bestående av de nationella datasystem som står i förbindelse med det centrala SIS, inklusive minst en nationell eller gemensam backup av N.SIS.
- c) En kommunikationsinfrastruktur som förenar CS-SIS och dess backup samt NI-SIS (nedan kallad *kommunikationsinfrastrukturen*) och som tillhandahåller ett krypterat virtuellt nätverk särskilt avsett för SIS-uppgifter och utbytet av uppgifter mellan Sirenekontoren i enlighet med vad som avses i artikel 7.2.
- d) En säker kommunikationsinfrastruktur mellan CS-SIS och de centrala infrastrukturerna för ESP, den gemensamma biometriska matchningstjänsten och MID.”

b) Följande punkter ska läggas till:

- ”8. Utan att det påverkar tillämpningen av punkterna 1–5 får sökningar i SIS-uppgifter om personer och identitetshandlingar göras också via ESP.
- 9. Utan att det påverkar tillämpningen av punkterna 15 i denna artikel får SIS-uppgifter om personer och identitetshandlingar också överföras via den säkra kommunikationsinfrastruktur som avses i punkt 1 d. Dessa överföringar ska begränsas till den utsträckning i vilken uppgifterna krävs för tillämpningen av förordning (EU) 2019/818.”

3. I artikel 7 ska följande punkt införas:

”2a. Sirenekontoren ska också säkerställa den manuella verifieringen av olika identiteter i enlighet med artikel 29 i förordning (EU) 2019/818. I den utsträckning som krävs för att utföra denna uppgift ska Sirenekontoren ha åtkomst till uppgifterna i CIR och MID för de ändamål som anges i artiklarna 21 och 26 i förordning (EU) 2019/818.”

4. I artikel 12.1 ska följande stycke läggas till:

”Medlemsstaterna ska säkerställa att all åtkomst till personuppgifter via ESP också loggas för att möjliggöra kontroll av huruvida sökningen var laglig, övervakning av att uppgiftsbehandlingen sker på ett lagligt sätt, egenkontroll samt dataintegritet och datasäkerhet.”

5. I artikel 44.1 ska följande led läggas till:

”f) Verifiering av olika identiteter och bekämpande av identitetsbedrägeri i enlighet med kapitel V i förordning (EU) 2019/818.”

6. Artikel 74.7 ska ersättas med följande:

"7. Vid tillämpningen av artikel 15.4 och punkterna 3, 4 och 6 i den här artikeln ska eu-Lisa lagra de uppgifter som avses i artikel 15.4 och i punkt 3 i den här artikeln vilka inte ska möjliggöra identifiering av enskilda personer, i den centrala databas för rapporter och statistik som avses i artikel 39 i förordning (EU) 2019/818.

eu-Lisa ska låta kommissionen och de organ som avses i punkt 6 i denna artikel få skräddarsydd rapportering och statistik. På begäran ska eu-Lisa bevilja medlemsstaterna, kommissionen, Europol och Europeiska gräns- och kustbevakningsbyrån åtkomst till den centrala databasen för rapporter och statistik i enlighet med artikel 39 i förordning (EU) 2019/818."

Artikel 61

Ändringar av förordning (EU) 2019/816

Förordning (EU) 2019/816 ska ändras på följande sätt:

1. I artikel 1 ska följande led läggas till:

"c) fastställer de villkor enligt vilka Ecris-TCN bidrar till att underlätta och bistå korrekt identifiering av personer som är registrerade i Ecris-TCN på de villkor och med avseende på artikel 20 i Europaparlamentets och rådets förordning (EU) 2019/818 (*), genom att lagra identitetsuppgifter, resehandlingsuppgifter samt biometriska uppgifter i CIR.

(*) Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816 (EUT L 135, 22.5.2019, s. 85)."

2. Artikel 2 ska ersättas med följande:

"Artikel 2

Tillämpningsområde

Denna förordning ska tillämpas på behandlingen av identitetsuppgifter om tredjelandsmedborgare som har varit föremål för fällande domar i medlemsstaterna, för ändamålet att identifiera den eller de medlemsstater där dessa domar har meddelats. Med undantag för artikel 5.1 b ii är de bestämmelser i denna förordning som är tillämpliga på tredjelandsmedborgare även tillämpliga på unionsmedborgare som även är medborgare i ett tredjeland och som har varit föremål för fällande domar i medlemsstaterna. Denna förordning underlättar och stödjer även korrekt identifiering av personer i enlighet med denna förordning och förordning (EU) 2019/818."

3. Artikel 3 ska ändras på följande sätt:

a) Led 8 utgår.

b) Följande led ska läggas till:

"19. CIR: den gemensamma databas för identitetsuppgifter som inrättas genom artikel 17.1 i förordning (EU) 2019/818,

20. Ecris-TCN-uppgifter: alla uppgifter som lagras i det centrala systemet och i CIR i enlighet med artikel 5,

21. ESP: den europeiska sökportal som inrättas genom artikel 6.1 i Europaparlamentets och rådets förordning (EU) 2019/818."

4. Artikel 4.1 ska ändras på följande sätt:

a) Led a ska ersättas med följande:

"a) ett centralt system,".

b) Följande led ska införas:

"aa) CIR,".

c) Följande led ska läggas till:

"e) en kommunikationsinfrastruktur mellan det centrala systemet och de centrala infrastrukturerna för ESP och CIR."

5. Artikel 5 ska ändras på följande sätt:

a) I punkt 1 ska inledningen ersättas med följande:

"1. För varje dömd tredjelandsmedborgare ska den dömande medlemsstatens centralmyndighet skapa en uppgiftspost i ECRIS-TCN. Uppgiftsposten ska innehålla".

b) Följande punkt ska införas:

"1a. CIR ska innehålla de uppgifter som avses i punkt 1 b och följande uppgifter i punkt 1 a: Efternamn, förnamn, födelsedatum, födelseort (ort och land), medborgarskap, kön, i tillämpliga fall tidigare namn, om tillgängligt pseudonymer eller alias, om tillgängligt resehandlingens typ och nummer samt utfärdande myndighet. CIR får även innehålla de uppgifter som avses i artikel 3. Återstående Ecris-TCN-uppgifter ska lagras i det centrala systemet."

6. Artikel 8 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

"1. Varje uppgiftspost ska lagras i det centrala systemet och CIR så länge som de uppgifter som gäller de fällande domarna mot den berörda personen lagras i kriminalregistret."

b) Punkt 2 ska ersättas med följande:

"2. Efter utgången av den lagringsperiod som avses i punkt 1 ska den dömande medlemsstatens centralmyndighet radera uppgiftsposten, inbegripet uppgifter som fingeravtryck eller ansiktsbilder, ur det centrala systemet och CIR. Raderingen ska om möjligt ske automatiskt, och under inga omständigheter senare än en månad efter lagringsperiodens utgång."

7. Artikel 9 ska ändras på följande sätt:

a) I punkt 1 ska ordet "Ecris-TCN" ersättas med orden "det centrala systemet och CIR".

b) I punkterna 2, 3 och 4 ska orden "det centrala systemet" ersättas med orden "det centrala systemet och CIR".

8. I artikel 10.1 ska led j utgå.

9. I artikel 12.2 ska orden "det centrala systemet" ersättas med orden "det centrala systemet och CIR".

10. I artikel 13.2 ska orden "det centrala systemet" ersättas med orden "det centrala systemet CIR".

11. I artikel 23.2 ska orden "det centrala systemet" ersättas med orden "det centrala systemet och CIR".

12. Artikel 24 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

"1. De uppgifter som förs in i det centrala systemet och CIR ska endast behandlas med ändamålet att identifiera de medlemsstater som innehar uppgifterna i kriminalregister om tredjelandssmedborgare. De uppgifter som förs in i CIR ska också behandlas i enlighet med förordning (EU) 2019/818 för att underlätta och bistå med en korrekt identifiering av personer som är registrerade i Ecris-TCN-systemet i enlighet med den här förordningen."

b) Följande punkt ska läggas till:

"3. Utan att det påverkar punkt 2 ska åtkomst för ändamålet att konsultera de uppgifter som lagras i CIR också förbehållas vederbörligen bemyndigad personal vid de nationella myndigheterna i varje medlemsstat och vederbörligen bemyndigad personal vid de unionsbyråer som är behöriga för de syften som anges i artiklarna 20 och 21 i förordning (EU) 2019/818. Sådan åtkomst ska begränsas enligt den utsträckning uppgifterna krävs för att de ska kunna utföra sina arbetsuppgifter för dessa syften och stå i proportion till de mål som eftersträvas."

13. Artikel 32 ska ersättas med följande:

"2. Vid tillämpningen av punkt 1 i denna artikel ska eu-Lisa lagra de uppgifter som avses i den punkten i den centrala databas för rapporter och statistik som avses i artikel 39 i förordning (EU) 2019/818."

14. I artikel 33.1 ska orden "det centrala systemet" ersättas med orden "det centrala systemet, CIR och".

15. Artikel 41.2 ska ersättas med följande:

"2. För fällande domar som meddelats före den dag då uppgifter ska börja föras in i enlighet med artikel 35.1 ska centralmyndigheterna inrätta de enskilda uppgiftsposterna i det centrala systemet och CIR enligt följande:

- a) Alfnumeriska uppgifter ska föras in i det centrala systemet och CIR senast vid utgången av den period som avses i artikel 35.2.
- b) Uppgifter om fingeravtryck ska föras in i det centrala systemet och CIR inom två år från driftstarten i enlighet med artikel 35.4."

KAPITEL IX

Slutbestämmelser

Artikel 62

Rapportering och statistik

1. Den vederbörligen bemyndigade personalen vid medlemsstaternas behöriga myndigheter, kommissionen och eu-Lisa ska ha åtkomst för att ta del av endast för rapporterings- och statistikändamål, antalet sökningar per ESP-användarprofil.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

2. Den vederbörligen bemyndigade personalen vid medlemsstaternas behöriga myndigheter, kommissionen och eu-Lisa ska ha åtkomst för att söka på följande uppgifter avseende CIR, dock endast för rapporterings- och statistikändamål:

- 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 trebokstavskoden för det utfärdande landet.
- d) Antalet sökningar som utförts med och utan biometriska uppgifter.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

3. Den vederbörligen bemyndigade personalen vid medlemsstaternas behöriga myndigheter, kommissionen och eu-Lisa ska ha åtkomst för att söka på följande uppgifter avseende MID, dock endast för rapporterings- och statistikändamål:

- a) Antalet sökningar som utförts med och utan biometriska uppgifter.
- b) Antalet länkar per typ och de EU-informationssystem som innehåller de länkade uppgifterna.
- c) Den tidsperiod under vilken en gul och en röd länk har blivit kvar i systemet.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

4. Den vederbörligen bemyndigade personalen vid Europeiska gräns- och kustbevakningsbyrån ska ha åtkomst för att söka i de uppgifter som avses i punkterna 1, 2 och 3 i denna artikel i syfte att utföra de riskanalyser och sårbarhetsanalyser som avses i artiklarna 11 och 13 i Europaparlamentets och rådets förordning (EU) 2016/1624 ⁽³⁸⁾.

5. Europols vederbörligen bemyndigade personal ska ha åtkomst till de uppgifter som avses i punkterna 2 och 3 i denna artikel i syfte att utföra strategiska, tematiska och operativa analyser enligt vad som avses i artikel 18.2 b och c i förordning (EU) 2016/794.

6. Vid tillämpningen av punkterna 1, 2 och 3 ska eu-Lisa lagra de uppgifter som avses i de punkterna i CRRS. De uppgifter som ingår i CRRS får inte möjliggöra identifiering av enskilda personer, men uppgifterna ska göra det möjligt för de myndigheter som förtecknas i punkterna 1, 2 och 3 att erhålla anpassade rapporter och anpassad statistik för att effektivisera in- och utresekontroller, hjälpa myndigheternas handläggning av viseringsansökningar och stödja evidensbaserat beslutsfattande om migration och säkerhet i unionen.

7. På begäran ska kommissionen göra relevant information tillgänglig för Europeiska unionens byrå för grundläggande rättigheter i syfte att utvärdera denna förordnings inverkan på de grundläggande rättigheterna.

⁽³⁸⁾ 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).

*Artikel 63***Övergångsperiod för användning av den europeiska sökportalen**

1. Under en tvåårsperiod från och med den dag då ESP tas i drift ska de skyldigheter som avses i artikel 7.2 och 7.4 inte tillämpas och det ska vara frivilligt att använda ESP.
2. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 69 för att ändra denna förordning genom att förlänga den period som avses i punkt 1 i den här artikeln en gång med högst ett år, om en bedömning av genomförandet av ESP visar att en sådan förlängning är nödvändig, särskilt mot bakgrund av de konsekvenser som idrifttagandet av ESP skulle ha för organisationen och varaktigheten av in- och utresekontroller.

*Artikel 64***Övergångsperiod som är tillämplig på bestämmelserna om åtkomst till den gemensamma databasen för identitetsuppgifter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott**

Artikel 22 ska tillämpas från och med den dag för idrifttagande av CIR som avses i artikel 68.3.

*Artikel 65***Övergångsperiod för spårning av multipla identiteter**

1. Under en ettårsperiod efter det att eu-Lisa har anmält slutförandet av det test av MID som avses i artikel 68.4 b och innan MID tas i drift ska Etias centralenhet ansvara för att utföra spårning av multipla identiteter med användning av de uppgifter som lagras i in- och utresesystemet, VIS, Eurodac och SIS. Spårningarna av multipla identiteter ska utföras med hjälp av enbart biometriska.
2. Om sökningen ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är desamma 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 mellan alla uppgifter som gett upphov till träffen.

3. Om en gul länk skapas ska MID bevilja Etias centralenhet åtkomst till de identitetsuppgifter som finns i de olika EU-informationssystemen.
4. Om det skapas en länk till en registrering i SIS, utom en registrering som skapats enligt artikel 3 i förordning (EU) 2018/1860, artiklarna 24 och 25 i förordning (EU) 2018/1861 eller artikel 38 i förordning (EU) 2018/1862, ska MID bevilja Sirenekontoret i den medlemsstat som skapade registreringen åtkomst till de identitetsuppgifter som finns i de olika informationssystemen.
5. Etias centralenhet eller, i de fall som avses i punkt 4 i denna artikel, 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. Etias centralenhet ska underrätta kommissionen i enlighet med artikel 67.3 först efter det alla gula länkar har verifierats manuellt och deras status uppdaterats till antingen gröna, vita eller röda länkar.
7. Medlemsstaterna ska vid behov bistå Etias centralenhet med att utföra spårning av multipla identiteter enligt denna artikel.
8. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 69 för att ändra denna förordning genom att förlänga den period som avses i punkt 1 i den här artikeln med sex månader, vilken kan förlängas två gånger med sex månader i taget. En sådan förlängning ska beviljas endast efter en bedömning av den uppskattade tiden för slutförande av spårning av multipla identiteter enligt denna artikel som visar att spårningen av multipla identiteter inte kan slutföras före utgången av den period som återstår antingen enligt punkt 1 i den här artikeln eller av en pågående förlängning, av skäl som ligger utanför Etias centralenhets kontroll, och att inga avhjälpande åtgärder kan tillämpas. Bedömningen ska genomföras senast tre månader före utgången av en sådan period eller av en pågående förlängning.,

*Artikel 66***Kostnader**

1. Kostnaderna i samband med inrättandet och driften av ESP, den gemensamma biometriska matchningstjänsten, CIR och MID 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. Utan att det påverkar ytterligare finansiering för detta ändamål från andra källor i Europeiska unionens allmänna budget ska ett belopp på 32 077 000 EUR tas i anspråk från det anslag på 791 000 000 EUR som tilldelas i artikel 5.5 b i förordning (EU) nr 515/2014 för att täcka kostnaderna för genomförandet av denna förordning i enlighet med punkterna 1 och 2 i den här artikeln.

4. Av det anslag som avses i punkt 3 ska 22 861 000 EUR tilldelas eu-Lisa, 9 072 000 EUR Europol och 144 000 EUR Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Cepol) för att hjälpa dessa byråer att utföra sina respektive uppgifter enligt denna förordning. Denna finansiering ska genomföras under indirekt förvaltning.

5. Kostnaderna för de utsedda myndigheterna ska belasta de respektive utseende medlemsstaterna. Kostnaderna för anslutningen av varje utsedd myndighet till CIR ska belasta varje medlemsstat.

Kostnaderna för Europol, inklusive kostnaderna för anslutning till CIR, ska belasta Europol.

*Artikel 67***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 ESP, CIR respektive MID.

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 68. 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 68.1 b, 68.2 b, 68.3 b, 68.4 b, 68.5 b och 68.6 b har slutförts på ett framgångsrikt sätt.

3. Etias centralenhet ska underrätta kommissionen om att den övergångsperiod som avses i artikel 65 har slutförts på ett framgångsrikt sätt.

4. Kommissionen ska tillhandahålla medlemsstaterna och allmänheten den information som anmäls i enlighet med punkt 1 via en kontinuerligt uppdaterad offentlig webbplats.

*Artikel 68***Driftsstart**

1. Kommissionen ska fastställa den dag då ESP ska tas i drift genom en genomförandeakt så snart följande villkor är uppfyllda:

- a) De åtgärder som avses i artiklarna 8.2, 9.7 och 43.5 har antagits.

- b) eu-Lisa har förklarat att ett övergripande test av ESP, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter och de unionsbyråer som får använda ESP, har slutförts på ett framgångsrikt sätt.
- c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 8.1 och har anmält dessa till kommissionen.

ESP får söka i Interpols databaser först när de tekniska arrangemangen gör det möjligt att uppfylla de krav som avses i artikel 9.5. Om det inte går att uppfylla kraven i artikel 9.5 ska det leda till att ESP inte söker i Interpols databaser, men det ska inte försena idrifttagandet av ESP.

Kommissionen ska fastställa det datum som avses i första stycket till senast 30 dagar efter antagandet av genomförandeakten.

2. Kommissionen ska fastställa den dag då den gemensamma biometriska matchningstjänsten ska tas i drift genom en genomförandeakt så snart följande villkor är uppfyllda:

- a) De åtgärder som avses i artiklarna 13.5 och 43.5 har antagits.
- b) eu-Lisa har förklarat att ett övergripande test av den gemensamma biometriska matchningstjänsten, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.
- c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 13 och har anmält dessa till kommissionen.
- d) eu-Lisa har förklarat att det test som avses i punkt 5 b har slutförts på ett framgångsrikt sätt.

Kommissionen ska fastställa det datum som avses i första stycket till senast 30 dagar efter antagandet av genomförandeakten.

3. Kommissionen ska fastställa den dag då CIR ska tas i drift genom en genomförandeakt så snart följande villkor är uppfyllda:

- a) De åtgärder som avses i artiklarna 43.5 och 74.10 har antagits.
- b) eu-Lisa har förklarat att ett övergripande test av CIR, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.
- c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 18 och har anmält dessa till kommissionen.
- d) eu-Lisa har förklarat att det test som avses i punkt 5 b har slutförts på ett framgångsrikt sätt.

Kommissionen ska fastställa det datum som avses i första stycket till senast 30 dagar efter antagandet av genomförandeakten.

4. Kommissionen ska fastställa den dag då MID ska tas i drift genom en genomförandeakt så snart följande villkor är uppfyllda:

- a) De åtgärder som avses i artiklarna 28.5 och 28.7, 32.5, 33.6, 43.5 och 49.6 har antagits.
- b) eu-Lisa har förklarat att ett övergripande test av MID, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter och Etias centralenhet, har slutförts på ett framgångsrikt sätt.
- c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 34 och har anmält dessa till kommissionen.
- d) Etias centralenhet har underrättat kommissionen i enlighet med artikel 67.3.
- e) eu-Lisa har förklarat att de tester som avses i punkterna 1 b, 2 b, 3 b och 5 b har slutförts på ett framgångsrikt sätt.

Kommissionen ska fastställa det datum som avses i första stycket till senast 30 dagar efter antagandet av genomförandeakten.

5. Kommissionen ska genom genomförandeakter fastställa den dag då de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma uppgiftskvalitetsindikatorerna samt minimikvalitetsstandarderna för uppgifter ska börja användas så snart följande villkor är uppfyllda:

- a) De åtgärder som avses i artikel 37.4 har antagits.

- b) v har förklarat att ett övergripande test av de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma uppgiftskvalitetsindikatorerna samt minimikvalitetsstandarderna för uppgifter, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.

Kommissionen ska fastställa det datum som avses i första stycket till senast 30 dagar efter antagandet av genomförandeakten.

6. Kommissionen ska fastställa den dag då CRRS ska tas i drift genom en genomförandeakt så snart följande villkor är uppfyllda:

- a) De åtgärder som avses i artiklarna 39.5 och 43.5 har antagits.
- b) eu-Lisa har förklarat att ett övergripande test av CRRS, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.
- c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 39 och har anmält dessa till kommissionen.

Kommissionen ska fastställa det datum som avses i första stycket till senast 30 dagar efter antagandet av genomförandeakten.

7. Kommissionen ska underrätta Europaparlamentet och rådet om resultaten av de tester som genomförts i enlighet med punkterna 1 b, 2 b, 3 b, 4 b, 5 b och 6 b.

8. Medlemsstaterna, Etias centralenhet och Europol ska börja använda var och en av interoperabilitetskomponenterna från den dag som fastställts av kommissionen i enlighet med punkterna 1, 2, 3 respektive 4.

Artikel 69

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 28.5, 39.5, 49.6, 63.2 och 65.8 ska ges till kommissionen för en period på fem år från och med den 11 juni 2019. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av femårsperioden. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.
3. Den delegering av befogenhet som avses i artiklarna 28.5, 39.5, 49.6, 63.2 och 65.8 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 datum som anges i beslutet. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artiklarna 28.5, 39.5, 49.6, 63.2 och 65.8 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 70

Kommittéförfarande

1. Kommissionen ska biträddas 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.

Om kommittén inte avger något yttrande ska kommissionen inte anta utkastet till genomförandeakt och artikel 5.4 tredje stycket i förordning (EU) nr 182/2011 ska tillämpas.

*Artikel 71***Rådgivande grupp**

eu-Lisa ska inrätta en rådgivande grupp för interoperabilitet. Under utformnings- och utvecklingsfasen av interoperabilitetskomponenterna ska artikel 54.4, 54.5 och 54.6 vara tillämplig.

*Artikel 72***Utbildning**

eu-Lisa ska utföra uppgifter vad gäller tillhandahållandet av utbildning i den tekniska användningen av interoperabilitetskomponenterna i enlighet med förordning (EU) 2018/1726.

Medlemsstaternas myndigheter och unionsbyråerna ska för sin personal som är behörig att behandla uppgifter med hjälp av interoperabilitetskomponenterna tillhandahålla ett lämpligt utbildningsprogram om datasäkerhet, uppgifters kvalitet, dataskydd, de förfaranden som är tillämpliga på uppgiftsbehandlingen samt skyldigheter att informera enligt artiklarna 32.4, 33.4 och 47.

Vid behov ska gemensamma kurser i dessa ämnen organiseras på unionsnivå för att förbättra samarbetet och utbytet av bästa praxis mellan personal vid medlemsstaternas myndigheter och unionsbyråer som har behörighet att behandla uppgifter med hjälp av interoperabilitetskomponenterna. Särskild uppmärksamhet ska ägnas åt processen för spårning av multipla identiteter, inbegripet den manuella verifieringen av olika identiteter och det åtföljande behovet att upprätthålla lämpliga skyddsåtgärder i fråga om grundläggande rättigheter.

*Artikel 73***Handbok**

Kommissionen ska i nära samarbete med medlemsstaterna, eu-Lisa och andra relevanta unionsbyråer 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 74***Övervakning och utvärdering**

1. eu-Lisa ska säkerställa att det finns förfaranden för att övervaka utvecklingen av interoperabilitetskomponenterna och deras anslutning till det enhetliga nationella gränssnittet 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. Senast den 12 december 2019 och därefter var sjätte månad under interoperabilitetskomponenternas utvecklingsfas ska eu-Lisa lämna en rapport till Europaparlamentet och rådet om hur utvecklingen av interoperabilitetskomponenterna och deras anslutning till det enhetliga nationella gränssnittet fortskrider. 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. Fyra år efter det att respektive interoperabilitetskomponent i enlighet med artikel 68 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.

4. Dessutom ska kommissionen ett år efter varje rapport från eu-Lisa utarbeta en övergripande utvärdering av interoperabilitetskomponenterna, inbegripet följande:

- a) En bedömning av tillämpningen av denna förordning.
- b) En granskning av uppnådda resultat i relation till denna förordnings mål och dess inverkan på de grundläggande rättigheterna, inbegripet i synnerhet en bedömning av påverkan av interoperabilitetskomponenterna på rätten till icke-diskriminering.
- c) En bedömning av hur webbportalen fungerar, inklusive sifferuppgifter om användningen av webbportalen och antalet tillgodosedda begäranden.
- d) En bedömning av huruvida de förutsättningar som ligger till grund för interoperabilitetskomponenterna fortfarande är giltiga.

- e) En bedömning av säkerheten i interoperabilitetskomponenterna.
- f) En bedömning av användningen av CIR för identifiering.
- g) En bedömning av användningen av CIR för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.
- h) En bedömning av eventuella konsekvenser, inbegripet eventuell oproportionellt stor inverkan på trafikflödet vid gränsövergångsställena, samt budgetkonsekvenser för unionens allmänna budget.
- i) En bedömning av sökningar i Interpols databaser via ESP, inbegripet information om antalet träffar i Interpols databaser samt information om eventuella problem som uppstått.

Den övergripande utvärderingen enligt första stycket i denna punkt ska inkludera eventuella nödvändiga rekommendationer. Kommissionen ska överlämna utvärderingsrapporten till Europaparlamentet, rådet, Europeiska datatillsynsmannen och Europeiska unionens byrå för grundläggande rättigheter.

5. Senast den 12 juni 2020 och därefter varje år fram till dess att kommissionen har antagit de genomförandeakter som avses i artikel 68 ska kommissionen lägga fram en rapport för Europaparlamentet och rådet om läget i fråga om förberedelserna för ett fullständigt genomförande av denna förordning. Denna rapport ska även innehålla detaljerad information om de kostnader som uppkommit och information om eventuella risker som kan påverka de totala kostnaderna.

6. Två år efter idrifttagande av MID i enlighet med artikel 68.4 ska kommissionen göra en granskning av hur MID påverkar rätten till icke-diskriminering. Efter denna första rapport ska granskningen av hur MID påverkar rätten till icke-diskriminering vara en del av den granskning som avses i punkt 4 b i den här artikeln.

7. Medlemsstaterna och Europol ska ge eu-Lisa och kommissionen den information som de behöver för att utarbeta de rapporter som avses i punkterna 3–6. Denna information får inte äventyra arbetsmetoder eller innehålla uppgifter som röjer de utsedda myndigheternas källor, personal eller utredningar.

8. eu-Lisa ska ge kommissionen den information som den behöver för att utarbeta de övergripande utvärderingar som avses i punkt 4.

9. Varje medlemsstat och Europol ska, med respekt för bestämmelserna i nationell rätt om offentliggörande av känsliga uppgifter, och utan att det påverkar begränsningar som är nödvändiga för att trygga säkerheten och den allmänna ordningen, förebygga och förhindra brott samt garantera att nationella utredningar inte kommer att äventyras, utarbeta årliga rapporter om effektiviteten av åtkomst till uppgifter som lagras i CIR i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, som innehåller information och statistik om

- a) de exakta syftena med sökningarna, däribland vilken typ av terroristbrott eller andra grova brott det gäller,
- b) de välgrundade skälen att tro att en person som misstänks för, har begått eller utsatts för ett brott omfattas av förordning (EU) nr 603/2013,
- c) antalet begäranden om åtkomst till CIR i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott,
- 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 kontroll i efterhand som genomfördes av den centrala åtkomstpunkten.

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

10. En teknisk lösning ska göras tillgänglig för medlemsstaterna i syfte att hantera åtkomstbegäranden från användare enligt vad som avses i artikel 22 och underlätta insamlingen av informationen enligt punkterna 7 och 9 i den här artikeln i syfte att generera de rapporter och den statistik som avses i de punkterna. Kommissionen ska anta genomförandeakter för att fastställa specifikationerna för den tekniska lösningen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 75

Ikraftträdande och tillämplighet

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

De bestämmelser i denna förordning som rör ESP ska tillämpas från och med den dag som fastställs av kommissionen i enlighet med artikel 68.1.

De bestämmelser i denna förordning som rör den gemensamma biometriska matchningstjänsten ska tillämpas från och med den dag som fastställs av kommissionen i enlighet med artikel 68.2.

De bestämmelser i denna förordning som rör CIR ska tillämpas från och med den dag som fastställs av kommissionen i enlighet med artikel 68.3.

De bestämmelser i denna förordning som rör MID, ska tillämpas från och med den dag som fastställs av kommissionen i enlighet med artikel 68.4.

De bestämmelser i denna förordning som rör de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma uppgiftskvalitetsindikatorerna samt minimikvalitetsstandarderna för uppgifter ska tillämpas från och med den dag som fastställs av kommissionen i enlighet med artikel 68.5.

De bestämmelser i denna förordning som rör CRRS ska tillämpas från och med den dag som fastställs av kommissionen i enlighet med artikel 68.6.

Artiklarna 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71, 73 och 74.1 ska tillämpas från och med den 11 juni 2019.

Denna förordning ska i förhållande till Eurodac tillämpas från och med den dag då omarbetningen av förordning (EU) nr 603/2013 blir tillämplig.

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

Utfärdad i Bryssel den 20 maj 2019.

På Europaparlamentets vägnar

A. TAJANI

Ordförande

På rådets vägnar

G. CIAMBA

Ordförande
