Regeringens proposition till riksdagen med förslag till lag om interoperabilitet mellan Europeiska unionens informationssystem

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att det stiftas en lag om interoperabilitet mellan Europeiska unionens informationssystem. I lagen föreslås sådana bestämmelser om behöriga myndigheter och deras åtkomst till den gemensamma databasen för identitetsuppgifter som kompletterar två förordningar av Europaparlamentet och rådet, det vill säga en förordning om interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete och en förordning om interoperabilitet mellan EU-informationssystem på området gränser och viseringar.

Propositionen hänför sig till budgetpropositionen för 2022 och avses bli behandlad i samband med den.

Den föreslagna lagen avses träda i kraft den 1 september 2022.

———

INNEHÅLL

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Beredningen av propositionen har inletts till följd av Europaparlamentets och rådets förordning (EU) 2019/818 om inrättande av en ram för interoperabilitet (eng. Interoperability) 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 (nedan *polisinteroperabilitetsförordningen*) och Europaparlamentets och rådets förordning (EU) 2019/817 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 (nedan *gränsinteroperabilitetsförordningen*), vilka trädde i kraft den 9 juni 2019.

Bakgrunden till lämnandet av förordningsförslagen var ökningen av olovliga gränsövergångar i samband med migrationskrisen samt terrordåd. Europeiska kommissionen (nedan *kommissionen*) ansåg att man för att stärka EU:s inre säkerhet bör förbättra resultaten och effektiviteten inom informationshanteringen med respekt för de grundläggande fri- och rättigheterna och särskilt skyddet för personuppgifter. På detta sätt kan man bättre skydda EU:s yttre gränser, förbättra hanteringen av migrationen och öka den inre säkerheten i enlighet med medborgarnas intresse.

På EU-nivå används och utvecklas redan flera informationssystem med hjälp av vilka gränsbevakare samt migrationsmyndigheter och brottsbekämpande myndigheter registrerar och får tillgång till uppgifter om personer. De informationssystem som används är EU:s informationssystem för viseringar (VIS), systemet för jämförelse av asylsökandes fingeravtryck (Eurodac) och Schengens informationssystem (SIS) samt som nya system skapas ett in- och utresesystem, ett EU-system för reseuppgifter och resetillstånd (Etias) och ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN). Systemen kompletterar varandra och med undantag för SIS gäller de endast tredjelandsmedborgare. Betraktat enligt mängden personuppgifter är de största systemen in- och utresesystemet, Etias och VIS, och dessa gäller endast tredjelandsmedborgare. För att det stöd som EU-informationssystemen erbjuder ska vara resultatrikt måste de uppgifter som fås från dem vara heltäckande, exakta och tillförlitliga. Enligt kommissionen finns det dock strukturella brister i EU:s informationsarkitektur. De nationella myndigheterna har tillgång till en komplex helhet av informationssystem som förvaltas på olika sätt. Dessutom är informationsarkitekturen för gränssäkerheten och den inre säkerheten splittrad, eftersom uppgifterna förs in separat i olika system som inte är kopplade till varandra. Detta leder till skuggområden som bland annat underlättar användningen av falska personuppgifter. Följden är att informationssystemen på EU-nivå för närvarande inte är interoperabla, det vill säga sådana att det med hjälp av dem är möjligt att utbyta och förmedla information så att myndigheterna och de behöriga tjänstemännen får de uppgifter de behöver, när och var uppgifterna än behövs.

Även Europaparlamentet har påskyndat åtgärder för att förbättra och utveckla befintliga informationssystem, ta itu med problem som bidrar till avbrott i informationsgången och sträva efter interoperabilitet mellan informationssystemen på EU-nivå och ett effektivare utbyte av information på EU-nivå.

1.2 Beredning

Beredningen av EU-rättsakter

Den 12 december 2017 lade kommissionen fram ett förslag till polisinteroperabilitetsförordning (COM(2017) 794 final) och ett förslag till gränsinteroperabilitetsförordning (COM(2017) 793 final). Förordningarnas allmänna syfte är att förbättra förvaltningen av Schengens yttre gränser och unionens inre säkerhet. Man blev tvungen att anta förordningarna separat, eftersom medlemsländernas deltagande varierar enligt politikområde och de rättsliga grunderna för förslagen avviker från varandra.

Efter förhandlingarna antog Europaparlamentet och rådet förordningarna och de trädde i kraft den 9 juni 2019. Förordningarna börjar tillämpas fullt ut vid en tidpunkt som fastställs av kommissionen.

Statsrådet har informerat riksdagen om EU:s förslag till förordningar om interoperabilitet genom U-skrivelse U 7/2018 rd, som förvaltningsutskottet (FvUU 6/2018 rd) och grundlagsutskottet (GrUU 11/2018 rd) har avgett utlåtanden om. Till helheten hänför sig även förordningsförslag om varje EU-omfattande informationssystem (in- och utresesystemet, Etias, SIS, VIS, Eurodac, Ecris-TCN) eller om ändring av dem.

De informationssystemsfunktioner som är förknippade med interoperabilitet skapas stegvis av Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA) före år 2024. Interoperabiliteten och uppgifternas integritet förutsätter samarbete på europeisk nivå samt sådant genomförande och ibruktagande som sker samtidigt.

Beredningen av propositionen

Den 2 april 2020 tillsattes det en arbetsgrupp för att bereda regeringspropositionen. I arbetsgruppen ingick representanter för inrikesministeriets polisavdelning, gränsbevakningsavdelning, förvaltnings- och utvecklingsavdelning och migrationsavdelning, finansministeriet, justitieministeriet, utrikesministeriet, Polisstyrelsen, skyddspolisen, centralkriminalpolisen, Tullen och Migrationsverket.

Begäran om utlåtande sändes till utrikesministeriet, justitieministeriet, finansministeriet, inrikesministeriets förvaltnings- och utvecklingsavdelning, migrationsavdelning, gränsbevakningsavdelning och enhet för nationell säkerhet, dataombudsmannen, Polisstyrelsen, centralkriminalpolisen, skyddspolisen, Migrationsverket, Tullen och Rättsregistercentralen.

Den fortsatta beredningen av propositionen har gjorts som tjänsteuppdrag vid inrikesministeriet. Bakgrundsmaterialet till regeringens proposition finns tillgängligt på adressen Lagstiftningsprojekt för inrättande av en ram för interoperabilitet mellan EU-informationssystem med projektnummer SM008:00/2020 (huvudsakligen på finska).

2 EU-rättsakternas målsättning och huvudsakliga innehåll

Målsättningen med polis- och gränsinteroperabilitetsförordningarna är i synnerhet följande:

1. Säkerställa att slutanvändarna har snabb, smidig, systematisk och kontrollerad åtkomst till den information som de behöver för att kunna utföra sina uppgifter.

2. Bidra med en lösning för att avslöja olika identiteter som är kopplade till samma biometriska uppgifter. Detta gör det möjligt att bekämpa användningen av falsk identitet.

3. Underlätta kontrollen av tredjelandsmedborgares identitet.

4. Påskynda och förenkla de brottsbekämpande myndigheternas åtkomst till andra system än sådana som inrättats för brottsbekämpande ändamål, om detta är nödvändigt för att förebygga eller avslöja allvarlig brottslighet och terrorism eller för att väcka åtal på grund av gärningarna.

Förordningarna är direkt tillämpliga. Till följd av förordningarna ska den nationella regleringen ändras till den del förordningarna förutsätter att det utfärdas nationell lagstiftning eller den gällande nationella lagstiftningen står i strid med förordningarna.

2.1 Polisinteroperabilitetsförordningen

2.1.1 Allmänna bestämmelser

I kapitel I i förordningen behandlas allmänna bestämmelser. Genom polisinteroperabilitetsförordningen tillsammans med Europaparlamentets och rådets förordning (EU) 2019/817 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).

Denna ram omfattar följande interoperabilitetskomponenter:

a. En europeisk sökportal (ESP) där man kan söka i flera informationssystem samtidigt.

b. En gemensam biometrisk matchningstjänst.

c. En gemensam databas för identitetsuppgifter (CIR).

d. En detektor för multipla identiteter (MID).

Förordningen 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.

I kapitlet finns det också bestämmelser om de definitioner som används i förordningen. I artikel 4.19 definieras polismyndighet. I definitionen hänvisas det i fråga om polismyndigheten till Europaparlamentets och rådets förordning (EU) 2016/680 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 och till direktivets definition av behörig myndighet i artikel 3.7. Enligt definitionen avses med behörig myndighet a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller b) annat organ eller annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller

lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten.

Förordningen tillämpas på systemen Eurodac, SIS och Ecris-TCN. Förordningen tillämpas också på Europoluppgifter i den mån det är möjligt att utföra sökningar i dem samtidigt som sökningar görs i de ovannämnda EU-informationssystemen. Förordningens tillämpningsområde har i artikel 3 begränsats till personer vars personuppgifter får behandlas i de EU-informationssystem och Europoluppgifter som avses i artikeln.

2.1.2 Interoperabilitetskomponenter

I kapitel II i förordningen finns det bestämmelser om den europeiska sökportalen (ESP), i kapitel III om den gemensamma biometriska matchningstjänsten, i kapitel IV om den gemensamma databasen för identitetsuppgifter (CIR) och i kapitel V om detektorn för multipla identiteter (MID).

Genom förordningen inrättas ESP som underlättar 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 som stöder målen för och syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. Med ESP avses inte en webbplats som är synlig för slutanvändaren, utan det är en funktion genom vilken sökningar som förs in med hjälp av nationella användargränssnitt genomförs inom ramen för interoperabiliteten.

Genom förordningen inrättas en gemensam biometrisk matchningstjänst där biometriska mallar som fåtts av uppgifter som lagrats i CIR och SIS lagras. På detta sätt möjliggörs sökningar med biometriska uppgifter i flera EU-informationssystem samt verksamheten för CIR och MID och stödjande av målen för in- och utresesystemet, VIS, Eurodac, SIS och Ecris-TCN.

Genom förordningen inrättas även 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 för att underlätta och bistå vid en korrekt identifiering av personer som är registrerade i in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN, stödja funktionen av MID 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.

I artikel 18 finns bestämmelser om de uppgifter som ska lagras i CIR. I artikeln hänvisas det till förordning (EU) 2019/816 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 det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726. Uppgifter som ska lagras i enlighet med artikel 18 är uppgifter som är logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör, det vill säga de uppgifter som avses i artikel 5.1 b och 5.2 i förordning (EU) 2019/816, vilka i fråga om uppgifter om fingeravtryck är i) uppgifter om fingeravtryck som har samlats in i enlighet med nationell rätt under ett brottmålsförfarande, ii) åtminstone uppgifter om fingeravtryck på grundval av något av följande kriterier: tredjelandsmedborgaren har dömts till ett fängelsestraff på minst sex månader, eller tredjelandsmedborgaren har dömts för ett brott som enligt medlemsstatens rätt är belagt med ett maximalt fängelsestraff på minst tolv månader.

I artikel 20 i förordningen föreskrivs det om åtkomst till CIR för identifiering av en person. Enligt artikel 20.1 får sökningar i CIR 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, eller e) om en person inte kan eller vägrar att samarbeta. Enligt artikeln ska sådana sökningar inte tillåtas när det gäller minderåriga under 12 år, såvida det inte sker för barnets bästa.

I artikel 20.2 föreskrivs det att om någon av dessa omständigheter uppstår får en polismyndighet som genom nationella lagstiftningsåtgärder bemyndigats att söka i CIR med en persons biometriska uppgifter som tagits direkt under en identitetskontroll, utföra sökningar endast i syfte att identifiera personen, förutsatt att förfarandet inletts i den berörda personens närvaro. 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. Dessutom får en polismyndighet som genom nationella lagstiftningsåtgärder har bemyndigats till detta, 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.

Artikel 20.5 och 20.6 förpliktar de medlemsstater som vill utnyttja de möjligheter som föreskrivs för behöriga myndigheter i artikeln att få åtkomst till den gemensamma databasen för identitetsuppgifter att anta nationella lagstiftningsåtgärder om detta. Enligt artikel 20.5 ska medlemsstater som vill utnyttja den föreskrivna möjligheten anta nationella lagstiftningsåtgärder om detta. När medlemsstaterna gör detta ska de ta hänsyn till att ingen diskriminering av tredjelandsmedborgare får förekomma. Dessutom konstateras det att de exakta syftena med identifieringen ska anges inom ramen för de mål som avses i artikeln i sådana lagstiftningsåtgärder. Medlemsstaterna ska utse de behöriga polismyndigheterna, och fastställa förfaranden, villkor och kriterier för sådana kontroller i dessa lagstiftningsåtgärder.

I artikel 21 i förordningen föreskrivs det om åtkomst till CIR för spårning av identiteter.

I artikel 22 finns det bestämmelser om de sökningar som utförs i CIR i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. Enligt artikel 22.1 får de utsedda myndigheterna och Europol söka i CIR för att få information om huruvida det finns uppgifter om en viss person i Eurodac. En sådan sökning är tillåten i specifika fall, om det finns rimliga skäl att anta sökningen bidrar till att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. Detta kan särskilt göras om det finns misstankar om att det i Eurodac lagras uppgifter om en person som misstänks för eller har utsatts för ett terroristbrott eller ett annat grovt brott.

I artikel 22.2 finns det bestämmelser om formen hos de Eurodac-träffar som CIR meddelar om. CIR ska tillhandahålla de utsedda myndigheterna och Europol ett svar i enlighet med artikel 18.2 som anger att Eurodac innehåller uppgifter som motsvarar sökningen. I händelse av en träff ska den utsedda myndigheten eller Europol begära full åtkomst till minst ett av de informationssystem där en träff har genererats. Om full åtkomst i undantagsfall inte begärs ska de utsedda myndigheterna registrera motiveringen till varför en begäran inte gjorts. Motiveringarna ska

kunna spåras till den nationella akten. Europol svarar för att registrera motiveringen i motsvarande ärende.

I det femte kapitlet finns det bestämmelser om MID. Syftet är att spåra multipla identiteter och bekämpa identitetsbedrägerier samt att stödja målen för CIR, in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

Kapitlen innehåller också bestämmelser om lagring av uppgifter och registerföring av loggar, det vill säga bevaring av uppgiftsbehandling.

2.1.3 Länkar mellan uppgifter i EU-informationssystemen

Målet med MID är att skapa och lagra länkar mellan uppgifter i de olika EU-informationssystemen för att spåra multipla identiteter. Syftet med detta är både att underlätta identitetskontroller för resenärer med ärligt uppsåt och att bekämpa identitetsbedrägeri.

I artikel 30 föreskrivs det om en gul länk. När en manuell verifiering av olika identiteter ännu inte har ägt rum, ska en länk mellan uppgifter klassificeras som gul när de länkade uppgifterna a) innehåller samma biometriska uppgifter men har olika eller liknande identitetsuppgifter, b) har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter och den berörda personens biometriska uppgifter inte har lagrats i något av EU-informationssystemen, c) innehåller samma identitetsuppgifter men de biometriska uppgifterna avviker från varandra och d) identitetsuppgifterna är liknande eller olika, och innehåller samma resehandlingsuppgifter men de biometriska uppgifterna avviker från varandra.

I artikel 31 föreskrivs det om en grön länk. En länk mellan uppgifter från två eller flera EU-informationssystem ska klassificeras som grön om de länkade uppgifterna a) har olika biometriska personuppgifter men innehåller samma identitetsuppgifter eller om den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer, b) har olika biometriska personuppgifter och har liknande eller olika identitetsuppgifter samt innehåller samma resehandlingsuppgifter och den myndighet som nämns i led a har konstaterat att de länkade uppgifterna hänvisar till två olika personer och c) har samma resehandlingsuppgifter men olika identitetsuppgifter och den berörda personens biometriska uppgifter inte finns i något av EU-informationssystemen och den myndighet som nämns i de föregående punkterna har konstaterat att uppgifterna hänvisar till två olika personer.

I artikel 32 föreskrivs det om en röd länk. En länk mellan uppgifter från två eller flera EU-informationssystem ska klassificeras som röd när de länkade uppgifterna a) har samma biometriska uppgifter men identitetsuppgifterna är antingen liknande eller olika 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) har samma, liknande eller olika identitetsuppgifter och samma resehandlingsuppgifter, men olika biometriska uppgifter och den myndighet som nämns i led a har konstaterat att de länkade uppgifterna hänvisar till två olika personer, av vilka åtminstone en person olovligen använder en och samma resehandling, c) har samma identitetsuppgifter men har olika biometriska uppgifter och antingen saknar eller har olika resehandlingsuppgifter och den myndighet som nämnas i led a dessutom har konstaterat att de länkade uppgifterna hänvisar till två olika personer på ett oberättigat sätt och d) har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter och den berörda personens biometriska uppgifter inte finns i något av EU-informationssystemen och den myndighet som nämns i led a har konstaterat att de länkade uppgifterna hänvisar till en och samma person på ett oberättigat sätt.

Myndigheten är skyldig att underrätta den berörda personen om förekomsten av multipla olagliga personuppgifter och ge ett identifikationsnummer, en referens till den myndighet som ansvarar för den manuella verifieringen av olika identiteter och webbadressen till webbportalen. Bestämmelserna begränsar dock inte tillämpningen av sådana begränsningar enligt rättsakterna om hanteringen av registreringar i SIS som behövs för att trygga säkerheten och den allmänna ordningen, förebygga och förhindra brott och garantera att ingen nationell utredning äventyras.

I artikel 33 föreskrivs det om en vit länk mellan uppgifter som skapas när de länkade uppgifterna a) innehåller samma biometriska uppgifter och samma eller liknande personuppgifter, b) innehåller samma eller liknande personuppgifter och biometriska uppgifter saknas, c) innehåller samma biometriska uppgifter och resehandlingar och liknande identitetsuppgifter och d) innehåller samma biometriska uppgifter men har liknande eller olika identitetsuppgifter, och den myndighet som ansvarar för verifieringen av olika identiteter har konstaterat att uppgifterna hänvisar till en och samma person.

I artikel 34 föreskrivs det om en akt med identitetsbekräftelse som ska innehålla följande uppgifter: de länkar som avses i artiklarna 30–33, en hänvisning till de EU-informationssystem i vilka de länkade uppgifterna finns, ett identifikationsnummer under vilket uppgifterna finns tillgängliga i systemen, den myndighet som ansvarar för den manuella verifieringen av olika identiteter och datum för skapande och uppdatering av länken. I artikel 35 föreskrivs det om lagring av uppgifter i MID. Uppgifterna och länkarna lagras endast tills de har lagrats i två eller fler EU-informationssystem. Uppgifterna ska raderas automatiskt från MID. ’

Eu-LISA ska föra logg över all uppgiftsbehandling som sker i MID.

2.1.4 Dataskydd

Enligt skäl 53 i ingressen till polisinteroperabilitetsförordningen är förordning (EU) 2016/679 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. Enligt skäl 54 i ingressen är direktiv (EU) 2016/680 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. Enligt skäl 57 i ingressen är förordning (EU) 2018/1725 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. Enligt skäl 55 i ingressen ska på motsvarande sätt 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. De särskilda bestämmelserna om dataskydd i förordning (EU) 2018/1862 och Europaparlamentets och rådets förordning (EU) 2019/816 är enligt skäl 56 i ingressen tillämpliga på behandlingen av personuppgifter i de system som regleras genom dessa förordningar.

Kapitel VII handlar om dataskydd. I artikel 40 föreskrivs det om den personuppgiftsansvariga. De av medlemsstaternas myndigheter som svarar för de biometriska mallar som lagrats i Eurodac, SIS och Ecris-TCN svarar för behandlingen av de uppgifter som finns i den gemensamma biometriska matchningstjänsten (BMS). I artikel 40.2 finns det bestämmelser om de myndigheter som ansvarar för behandlingen av personuppgifter i CIR. De personuppgiftsansvariga för uppgifter i MID är Europeiska gräns- och kustbevakningsbyrån när det gäller den behandling

av personuppgifter som utförs av Etias centralenhet samt de av medlemsstaternas myndigheter som lägger till eller ändrar uppgifter i akten med identitetsbekräftelse.

I artikel 41 föreskrivs det personuppgiftsbiträdet, som i den gemensamma biometriska matchningstjänsten, CIR och MID är eu-LISA.

I artikel 42 föreskrivs det om säkerhet vid behandling. I artikel 42.1 föreskrivs det att eu-LISA, Etias centralenhet, Europol och medlemsstaternas myndigheter ska säkerställa säkerheten vid den behandling av personuppgifter som äger rum enligt förordningen samt samarbeta kring säkerhetsrelaterade uppgifter. Eu-LISA svarar för interoperabilitetskomponenternas och den relaterade kommunikationsinfrastrukturens säkerhet. Dessutom gör eu-LISA upp planer för säkerhet och verksamhetens kontinuitet samt en katastrofplan.

Medlemsstaterna och unionsbyråerna ska se till att varje myndighet som har åtkomsträtt till interoperabilitetskomponenterna iakttar bestämmelserna i denna förordning och vid behov samarbetar med tillsynsmyndigheterna. Det föreskrivs dessutom om den personuppgiftsansvarigas egenkontroll. I artikel 45 föreskrivs det om sanktioner för behandling av uppgifter i strid med förordningen, och dessa sanktioner bestäms i enlighet med nationell rätt.

Varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en sådan åtgärd från en medlemsstats, Europols, Europeiska gräns- och kustbevakningsbyråns eller eu-LISA:s sida som är lagstridig eller oförenlig med denna förordning ska ha rätt till ersättning från medlemsstaten eller byrån i fråga. Medlemsstaten eller byrån ska helt eller delvis undantas från sitt skadeståndsansvar om den bevisar att den inte är ansvarig för skadan.

I artikel 47 föreskrivs det om rätten till information för den som är föremål insamlingen av personuppgifter i fråga om den gemensamma biometriska matchningstjänsten, CIR och MID. Informationen ska ges på ett klart språk som personen förstår samt till minderåriga enligt åldersnivå. Dessutom ska bestämmelserna om rätten till information i unionens tillämpliga dataskyddsregler tillämpas på personuppgifter som har registrerats i Ecris-TCN och behandlas i enlighet med denna förordning.

I artikel 48 föreskrivs det om rätten till åtkomst till, rättelse och radering av samt begränsning av behandlingen av personuppgifter som lagras i MID.

I artikel 49 föreskrivs det om inrättandet av en webbportal. Syftet med webbportalen är att underlätta utövandet av rätten till åtkomst till, rättelse, radering eller begränsning av behandlingen av personuppgifter.

I artikel 51 föreskrivs det om tillsynsmyndigheternas övervakning. Varje medlemsstat ska se till att dess myndigheter behandlar personuppgifter lagenligt på det sätt som föreskrivs i förordningen. Enligt definitionen i artikel 4.4 i förordningen avses med tillsynsmyndighet 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.

Enligt artikel 52 ska Europeiska datatillsynsmannen säkerställa att tillsynen av behandlingen av personuppgifter genomförs med iakttagande av internationella tillsynsstandarder minst vart fjärde år. I artikel 53 föreskrivs det om samarbete mellan tillsynsmyndigheterna och Europeiska datatillsynsmannen.

2.1.5 Olika aktörers ansvarsområden

I förordningen definieras de olika aktörernas ansvarsområden noggrant. Till eu-LISA:s uppgifter hör att säkerställa att den centrala infrastrukturen för interoperabilitetskomponenterna fungerar på det sätt som anges i förordningen, att hysa in interoperabilitetskomponenterna vid sina tekniska anläggningar samt att utveckla och anpassa dem. Dessutom ska eu-LISA fastställa den fysiska utformningen av interoperabilitetskomponenterna samt utveckla och implementera dem.

Eu-LISA ansvarar också för förvaltningen av interoperabilitetskomponenterna och kommunikationsinfrastrukturen, tillsynen över sekretessbestämmelserna för personal som arbetar med lagrade uppgifter, kvalitetskontroller av lagrade uppgifter och tillhandahållandet av utbildning om teknisk användning.

Medlemsstaterna ansvarar för anslutningen till ESP:s och CIR:s kommunikationsinfrastruktur, integrationen av de befintliga nationella systemen och infrastrukturerna med ESP, CIR och MID och andra tekniska skyldigheter. Medlemsstaterna svarar också för den manuella verifieringen av olika identiteter samt förbinder sig till efterlevnad av reglerna i varje informationssystem i fråga om personuppgifternas säkerhet och integritet och till att avhjälpa eventuella brister som konstateras. Till medlemsstaternas ansvar hör också att ansluta sina utsedda myndigheter till CIR.

Europol ansvarar för att säkerställa att sökningar i Europoluppgifter behandlas. Europol svarar också för användningen av och åtkomsten till ESP. Europol ska dessutom föra en förteckning över den personal som har åtkomst till uppgifterna.

Etias centralenhet ansvarar för den manuella verifieringen av olika identiteter samt spårningen av multipla identiteter bland de uppgifter som lagras i olika system.

2.1.6 Delegerade akter och kommittéförfarande

På det sätt som anges närmare i artikel 69 i förordningen ges kommissionen befogenhet att anta delegerade akter. Kommissionen ska biträdas av en kommitté med företrädare för medlemsstaterna.

Kommissionen kan anta delegerade akter med stöd av artiklarna 28.5, 39.5, 49.6, 63.2 och 65.8 i förordningarna.

I artikel 28 föreskrivs det om resultaten av en spårning av multipla identiteter. Med stöd av artikel 28.5 ska kommissionen anta delegerade akter för att fastställa förfarandena för att avgöra ärenden där identitetsuppgifter kan anses vara desamma eller liknande.

I artikel 39 föreskrivs det om den centrala databasen för rapporter och statistik (CRRS). Enligt artikel 39.5 ska kommissionen anta en delegerad akt för att fastställa detaljerade bestämmelser om driften av CRRS, inbegripet särskilda skyddsåtgärder för behandlingen av personuppgifter och de säkerhetsregler som är tillämpliga på databasen.

Genom artikel 49 inrättas en webbportal för att underlätta utövandet av rätten till åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter. Enligt artikel 49.6 ska kommissionen anta en delegerad akt för att fastställa närmare bestämmelser om driften av webbportalen, inklusive användargränssnittet, de språk på vilka webbportalen ska finnas tillgänglig och e-postmallen.

I artikel 63 föreskrivs det om övergångsperioden för användningen av ESP. Enligt artikel 63.2 ges kommissionen befogenhet att anta en delegerad akt för att ändra denna förordning genom att förlänga den period som avses ovan 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 idrifttagningen av ESP skulle ha för organisationen och varaktigheten av in- och utresekontroller.

I artikel 65 föreskrivs det om övergångsperioden för spårningen av multipla identiteter. Enligt artikel 65.8 ges kommissionen befogenhet att anta en delegerad akt för att ändra denna förordning genom att förlänga den period som avses ovan med sex månader, vilken kan förlängas två gånger med sex månader i taget.

Tre delegerade akter har antagits. I den första (artikel 28.5) fastställs de fall där personuppgifterna anses vara desamma eller liknande. Den andra (artikel 39.5) gäller detaljerade bestämmelser om driften av den centrala databasen för rapporter och statistik (CRRS). Genom den tredje (artikel 49.6) fastställs närmare bestämmelser om driften av webbportalen, inklusive användargränssnittet, de språk på vilka webbportalen ska finnas tillgänglig och e-postmallen. Beredningen av delegerade akter i det kommittéförfarande som Finland har deltagit i avslutades hösten 2020 och akterna antas under 2021.

Enligt förordningarna har kommissionen också getts befogenhet att anta genomförandeakter. Dessa akter kan gälla

– de tekniska detaljerna 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 biometriska matchningstjänsten,

– mekanismer, förfaranden och indikatorer för automatiserad kontroll av uppgiftskvalitet,

– utveckling av UMF-standarden,

– samarbetsförfaranden som ska användas i händelse av säkerhetsincidenter, och

– specifikationer för den tekniska lösningen för medlemsstaternas hantering av åtkomstbegäranden från användare.

Hittills har det antagits åtta genomförandeakter, men flera akter bereds fortfarande.

Kommissionen har också tilldelats genomförandebefogenheter att fastställa de datum när ESP, den gemensamma biometriska matchningstjänsten, CIR, MID och CRRS ska tas i drift.

2.1.7 Ikraftträdande och tillämpning

Ikraftträdandet av förordningen och inledandet av tillämpningen av den har skilts åt. Förordningen offentliggjordes i Europeiska unionens officiella tidning den 22 maj 2019 och den trädde i kraft tjugo dagar från detta datum.

Interoperabilitetskomponenterna tas dock i drift först när kommissionen har fastställt datumen för idrifttagningen av dem. Först efter att interoperabilitetskomponenterna har tagits i drift blir det möjligt med interoperabilitet mellan informationssystemen på EU-nivå.

Enligt kommissionens uppskattade tidsplan tas av interoperabilitetskomponenterna först i drift den gemensamma biometriska matchningstjänsten i början av 2022, därefter CIR i slutet av 2022 och sedan ESP och MID.

I förordningen konstateras det ytterligare separat att den i förhållande till Eurodac tillämpas från och med den dag då omarbetningen av förordning (EU) nr 603/2013 blir tillämplig.

2.2 Gränsinteroperabilitetsförordningen

Gränsinteroperabilitetsförordningen har antagits för inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar. Dessa informationssystem är i synnerhet VIS, in- och utresesystemet och Etias.

Artiklarna i gräns- och polisinteroperabilitetsförordningarna är i övrigt huvudsakligen enhetliga.

De delegerade akterna och kommittéförfarandet samt ikraftträdandet och tillämpningen är desamma i båda förordningarna.

3 Nuläge och bedömning av nuläget

EU-informationssystemen SIS, VIS och Eurodac står för närvarande inte i förbindelse med varandra. Detta gör att det är splittrat, komplicerat, långsamt och svårt att använda systemen. Systemen är inte sinsemellan enhetliga, vilket innebär ett omfattande behov av introduktion och utbildning för att informationssystemen ska kunna utnyttjas fullt ut. Dessutom har informationssystemen olika personuppgiftsansvariga, vilket bidrar till att till exempel förvaltningen av åtkomsträttigheter inte sker centraliserat. Det finns en risk för att alla tillgängliga uppgifter inte upptäcks eller att de inte kan utnyttjas fullt ut i brådskande situationer. De brottsbekämpande myndigheterna har inte alltid tillgång till användbar information, vilket delvis kan försämra medborgarnas säkerhet och skapa skuggområden. Utöver de ovannämnda systemen är in- och utresesystemet, Etias och Ecris-TCN under uppbyggnad.

Gränsbevakare och poliser kommer på EU-nivå i kontakt med en komplex helhet av informationssystem som förvaltas på många olika sätt. Dessutom är alla EU-medlemsstater inte delaktiga i alla EU-informationssystem. Informationen blir splittrad och samma ärende sköts med hjälp av flera olika kanaler för informationsutbyte, vilket kräver resurser och kan skapa förvirring. För närvarande finns det ett stort antal olika typer av kanaler för internationellt och europeiskt brottsbekämpningssamarbete som i huvudsak kompletterar varandra, och i vissa fall anses kanalerna utesluta varandra. Interoperabilitet mellan EU-informationssystem kan för sin del i betydande grad eliminera nuvarande skuggområden där personer kan registrera sig med olika täcknamn i olika informationssystem som inte är i förbindelse med varandra.

I anslutning till identifiering av en person har en polisman för närvarande med stöd av 2 kap. 1 § i polislagen (872/2011) rätt att för utförande av ett visst uppdrag av var och en få veta dennes namn och personbeteckning eller, om sådan saknas, födelsedatum och medborgarskap samt var personen i fråga är anträffbar. Om en person vägrar lämna dessa uppgifter och om personen inte kan identifieras på annat sätt har polismannen rätt att utreda identiteten med hjälp av signalement. Enligt 3 mom. i samma paragraf har en polisman rätt att för identifiering gripa en person som vägrar lämna uppgifter enligt 1 mom. eller som lämnar sannolikt falska uppgifter om de nämnda omständigheterna, förutsatt att gripandet är nödvändigt för att klarlägga identiteten.

I 7 § i lagen om utredande av dödsorsak (459/1973) finns det bestämmelser om de situationer där polisen ska verkställa en undersökning för utredande av dödsorsak. Utredande av dödsorsak omfattar inhämtande av de uppgifter på basis av vilka ett dödsfall kan konstateras och tidpunkten för det kan bedömas, den avlidnes identitet kan fastställas, en uppfattning om de förhållanden som rådde vid dödsfallet och omständigheterna kring dödsfallet fås, dödsorsak och dödsklass fastställas och de handlingar som hör till utredande av dödsorsak upprättas. Polisen svarar för rättsmedicinsk utredning av dödsorsak. Identifieringen av offer utgör en del av utredningen av dödsorsak. Polisen har en enhet för identifiering av offer, det vill säga en DVI-enhet (Disaster Victim Identification), som utför identifieringen av offer bland annat i sådana fall av olyckor eller brott där antalet offer är stort, offren är svåra att identifiera eller offren saknas. Enheten för identifiering av offer bistår vid behov den lokala polisen i verksamheten för att identifiera offer oberoende av antalet offer och fallets karaktär, även i enskilda fall.

Enheten för identifiering av offer utför vid behov identifiering av offer även i sådana fall där en eller flera finska medborgare har dött utomlands. På begäran kan enheten för identifiering av offer delta i identifieringsuppgifter också utomlands, även om det inte finns några finska medborgare bland offren.

För utredande av identiteten har en gränsbevakningsman enligt 36 § 1 mom. i gränsbevakningslagen (578/2005) för utförande av ett enskilt uppdrag som ankommer på gränsbevakningsväsendet rätt att av var och en få veta namn, personbeteckning, eller om sådan saknas, födelsedatum och nationalitet samt var personen i fråga kan anträffas. En gränsbevakningsman har också med stöd av 28 § 1 mom. 3 punkten i gränsbevakningslagen rätt att i samband med gränskontroll, för att genomföra gränskontroller enligt kodexen om Schengengränserna, utan brottsmisstanke vidta åtgärder enligt artikel 8.2 i kodexen om Schengengränserna, till vilka hör bland annat kontroll av identitet och medborgarskap samt av äktheten och giltigheten hos den resehandling som berättigar till gränspassage. Dessutom har en gränsbevakningsman i sådana polisuppdrag som avses i 33 § i gränsbevakningslagen de befogenheter som avses i 2 och 3 kap. i polislagen.

Enligt 17 § i tullagen (304/2016) har en tullman för utförande av en viss tullåtgärd rätt att av var och en få veta dennes namn och personbeteckning eller, om sådan saknas, födelsedatum och medborgarskap samt var personen i fråga är anträffbar. Med tullåtgärd avses enligt 2 § 7 punkten i tullagen samtliga tjänsteåtgärder som hör till Tullens uppgifter, med undantag för förundersökning av tullbrott samt in- och utresekontroller. Om en person vägrar lämna ovannämnda uppgifter eller lämnar sannolikt falska uppgifter om dem, har en tullman rätt att för klarläggande av identiteten gripa personen, förutsatt att gripandet är nödvändigt för att klarlägga identiteten. Om identiteten inte kan klarläggas på något annat sätt, har en tullman rätt att klarlägga identiteten med hjälp av signalement.

Bestämmelser om rätten för en tullman inom tullbrottsbekämpningen att identifiera personer finns däremot i 2 kap. 15 § i lagen om brottsbekämpning inom Tullen (623/2015). Enligt bestämmelsen har en tullman inom tullbrottsbekämpningen för utförande av ett visst uppdrag som

ankommer på Tullen rätt att av var och en få veta dennes namn, personbeteckning eller, om sådan saknas, födelsedatum och medborgarskap samt var personen i fråga är anträffbar. Om någon vägrar lämna uppgifter och personen inte kan identifieras på annat sätt, har en tullman inom tullbrottsbekämpningen rätt att utreda identiteten med hjälp av signalement samt med stöd av de uppgifter som avses i 7 och 8 § i lagen om behandling av personuppgifter inom Tullen (650/2019) och i 5, 6, 11 och 12 § i lagen om behandling av personuppgifter i polisens verksamhet (616/2019). En tullman har dessutom rätt att för identifiering gripa den som vägrar lämna ovannämnda uppgifter eller som lämnar sannolikt falska uppgifter om dessa omständigheter, förutsatt att gripandet är nödvändigt för att klarlägga identiteten.

I 129 a § i utlänningslagen föreskrivs det om övervakning av utlänningar, och med detta avses övervakning av efterlevnaden av utlänningslagen och de bestämmelser som utfärdats med stöd av den och bekämpning av olaglig vistelse i landet. Enligt 129 b § 1 mom. 1 punkten i utlänningslagen har polisen och Gränsbevakningsväsendet, om det för övervakningen av utlänningar är motiverat att utreda en utlännings identitet, medborgarskap, rätt att vistas i landet eller rätt att arbeta, rätt att av den som övervakas få uppgifter och kontrollera behövliga handlingar om personens identitet och medborgarskap samt om personens rätt att vistas i landet och rätt att arbeta. Enligt 131 § 1 mom. 5 punkten i utlänningslagen får polisen eller gränskontrollmyndigheten för verifiering av identitet, för behandling, beslut och övervakning av utlänningars inresa och utresa samt vistelse och arbete och för tryggande av statens säkerhet ta fingeravtryck, fotografier och andra signalement på en utlänning vars identitet är oklar.

Poliser, gränsbevakare och tullmän har således redan en omfattande lagstadgad rätt att kontrollera en persons identitet. Aktiveringen av artikel 20 i polis- och gränsinteroperabilitetsförordningarna effektiviserar identifieringen av personer ytterligare och möjliggör dessutom att en person inte nödvändigtvis längre bör gripas för att utreda ärendet.

Tillämpningen av polis- och gränsinteroperabilitetsförordningarna förutsätter kompletterande nationell lagstiftning om en medlemsstat vill utnyttja den möjlighet som ges i artikel 20 i polis- och gränsinteroperabilitetsförordningarna att utfärda nationella bestämmelser om att de polismyndigheter som avses i artikel 4.19 i förordningen får åtkomst till den gemensamma databasen för identitetsuppgifter i syfte att identifiera personer.

Genom den föreslagna lagen kompletteras bestämmelserna i förordningarna till den del det är nödvändigt för att det nationellt ska vara möjligt att utnyttja den möjlighet att kontrollera en persons identitet som förordningarna ger.

Den kompletterande nationella reglering som förordningarna föranleder utfärdas som en egen lag, eftersom det inte är ändamålsenligt att införliva regleringen i befintlig lagstiftning.

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

4.1.1 Interoperabilitetskomponenter

Det viktigaste förslaget i polis- och gränsinteroperabilitetsförordningarna är inrättandet av fyra interoperabilitetskomponenter.

1. En europeisk sökportal (ESP) där man kan söka i flera informationssystem samtidigt, inklusive biometriska uppgifter, såsom ansiktsbilder och fingeravtryck.

2**.** En gemensam biometrisk matchningstjänst som gör det möjligt att jämföra biometriska uppgifter som lagras i ett system med fingeravtryck och ansiktsbilder som lagras i andra system.

3**.** En gemensam databas för identitetsuppgifter (CIR) där sådana personuppgifter, biometriska uppgifter och resehandlingsuppgifter om tredjelandsmedborgare som ingår olika EU-informationssystem lagras.

4**.** En detektor för multipla identiteter (MID) som kontrollerar om det finns personer med samma personuppgifter, biometriska uppgifter eller resehandlingsuppgifter i andra system, för att man ska kunna upptäcka olika identiteter som anknyter till samma biometriska uppgifter.

Med hjälp av dessa komponenter görs EU:s befintliga informationssystem (SIS, VIS och Eurodac) samt de system som är under uppbyggnad (in- och utresesystemet, Etias och Ecris-TCN) interoperabla. Detta innebär att dessa system kompletterar varandra för att underlätta korrekt identifiering av personer, däribland okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor. Interoperabiliteten mellan informationssystemen bidrar dessutom till att bekämpa identitetsbedrägeri, förbättrar och harmoniserar kvalitetskraven på uppgifterna i respektive EU-informationssystem, rationaliserar åtkomsten till in- och utresesystemet, VIS, Etias och Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott och stöder syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

Det föreskrivs om interoperabilitetskomponenterna i polis- och gränsinteroperabilitetsförordningarna. Rättsakterna förutsätter inte nationell kompletterande lagstiftning. Alla medlemsstater ska ta varje interoperabilitetskomponent i drift samtidigt.

Användningen av biometriska uppgifter

Biometriska uppgifter (fingeravtryck, ansiktsbilder, handavtryck) är mycket mer tillförlitliga vid identifieringen av personer än alfanumeriska uppgifter. Samtidigt är biometriska uppgifter sådana känsliga personuppgifter som hör till de särskilda kategorier av personuppgifter som avses i EU:s dataskyddslagstiftning.

Av de befintliga informationssystemen på EU-nivå innehåller SIS, VIS och Eurodac biometriska uppgifter. Även in- och utresesystemet och Ecris-TCN, som är under uppbyggnad, kommer att innehålla biometriska uppgifter. Systemet SIS är det enda system där man också kan lagra uppgifter om handavtryck. Systemet SIS innehåller dessutom DNA-profiler. Eftersom dessa uppgifter inte lagras i andra system, har uppgifter om handavtryck och DNA-profiler inte beaktats och används inte heller i interoperabilitetskomponenterna i enlighet med de principer om nödvändighet och proportionalitet som hänför sig till behandlingen av personuppgifter.

Bland interoperabilitetskomponenterna är syftet med den gemensamma biometriska matchningstjänsten att underlätta identifieringen av personer som eventuellt har registrerats i flera informationssystem på EU-nivå. Alla automatiska fingeravtrycksidentifieringssystem 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. De hålls logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör. Detta underlättar jämförelser mellan systemen med användning av biometriska mallar.

I propositionen föreslås det inga ändringar i den reglering som gäller förutsättningarna för behandling av biometriska uppgifter i nationella register och utlämnande av dem till EU-informationssystemen.

4.1.2 Länkar mellan EU-informationssystemen

Av interoperabilitetskomponenterna inrättas MID för en korrekt identifiering av de personer vars personuppgifter lagras EU-informationssystemen.

Syftet med MID är att 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 ska begränsas 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.

Det finns fyra olika länkar: en gul länk, en grön länk, en röd länk och en vit länk.

Med gul länk avses att det i två eller flera EU-informationssystem finns uppgifter om antingen olika personer, men att uppgifterna till vissa delar är sammanfallande, eller om samma person, men att uppgifterna i de olika systemen avviker från varandra. Efter att uppgifterna har kontrollerats framgår det dock att det är fråga om olika personer eller samma person, men att situationen inte är oklar och att den registrerade personen inte har lämnat felaktiga uppgifter om sig själv.

Med grön länk avses att det i två eller flera EU-informationssystem finns uppgifter om olika personer, men att uppgifterna till vissa delar är sammanfallande och att den myndighet som ansvarar för den manuella verifieringen av uppgifterna har konstaterat att de länkade uppgifterna hänvisar till två olika personer.

En röd länk innebär att det i två eller flera EU-informationssystem finns olika uppgifter om en person och att den myndighet som ansvarar för den manuella verifieringen av uppgifterna har konstaterat att de länkade uppgifterna hänvisar till en och samma person på ett oberättigat sätt.

En vit länk innebär att det i två eller flera EU-informationssystem finns uppgifter om samma person och att uppgifterna inte är oklara.

Bestämmelserna om länkarna förutsätter inte nationell kompletterande lagstiftning.

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

De utsedda myndigheter som avses i artikel 22 i polis- och gränsinteroperabilitetsförordningarna ges i specifika fall rätt att söka i CIR, när det behövs för att behövs för att förebygga, förhindra, upptäcka eller utreda grova brott.

Enligt artikel 22 i polisinteroperabilitetsförordningen får de utsedda myndigheterna och Europol i specifika fall söka i CIR för att få information om huruvida det finns uppgifter om en viss person i Eurodac när det finns rimliga skäl att anta att en sökning i EU-informationssystemen 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.

Artikel 22 i gränsinteroperabilitetsförordningen har samma innehåll med den skillnaden att den gäller uppgifter som har lagrats i in- och utresesystemet, VIS eller Etias.

Om resultatet av sökningen är ett svar som anger att uppgifter om personen i fråga förekommer i Eurodac, in- och utresesystemet, VIS eller Etias får svaret 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. Polis- och gränsinteroperabilitetsförordningarna ger således inte åtkomst till de ovannämnda informationssystemen, utan rätten att få åtkomst till dem bestäms enligt den rättsliga grunden för systemet i fråga. Det bör dock beaktas att redan uppgiften om att en person är registrerad i något informationssystem är en personuppgift.

Artikel 22 i polis- och gränsinteroperabilitetsförordningarna förutsätter inte nationell kompletterande lagstiftning.

4.1.4 Åtkomst till databasen för identitetsuppgifter (CIR) för identifiering av en person

Artikel 20 i polis- och gränsinteroperabilitetsförordningarna förutsätter att en medlemsstat som vill tillämpa artikeln ska anta nationell lagstiftning om detta.

I artikeln ges polismyndigheter möjlighet att få åtkomst till CIR för identifiering av personer när det är fråga om att bidra till att förebygga och bekämpa olaglig invandring eller att bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, inbegripet att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier. Medlemsstaterna ska utse de behöriga polismyndigheterna, och fastställa förfaranden, villkor och kriterier för identifiering.

Enligt förordningarna avses med polismyndighet en sådan behörig myndighet som definieras i artikel 3.7 i direktiv (EU) 2016/680 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.

Sådana myndigheter är

a) offentliga myndigheter som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller

b) andra organ eller andra enheter som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten.

Om en medlemsstat dessutom vill möjliggöra att en polismyndighet 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, får söka i CIR med dessa personers biometriska uppgifter, ska medlemsstaten utfärda bestämmelser om detta genom nationell lagstiftning.

Enligt förslaget ska Finland utfärda nationell lagstiftning för att genomföra artikel 20 i polis- och gränsinteroperabilitetsförordningarna. Genom den föreslagna lagstiftningen kompletteras bestämmelserna i förordningarna till den del det är nödvändigt. Den kompletterande nationella

reglering som förordningarna föranleder utfärdas som en egen lag, eftersom det med hänsyn till förordningarnas syfte inte är ändamålsenligt att införliva regleringen i befintlig lagstiftning.

I Finland är polisen, Gränsbevakningsväsendet och Tullen de myndigheter som ska ges åtkomst till CIR för identifiering av personer.

Dessutom föreslås det att polisen vid en naturkatastrof, olycka eller ett terrordåd, ska få rätt att med biometriska uppgifter utföra sökningar i CIR för att identifiera okända offer som inte kan identifiera sig eller identifiera oidentifierade mänskliga kvarlevor.

4.1.5 Sökningar i och åtkomst till CIR i andra uppgifter

Finländska tjänstemän kan använda de informationssystem som ingår i interoperabilitetsramen för olika ändamål. Exempelvis en polis- eller tullman kan genomföra in- och utresekontroller enligt kodexen om Schengengränserna och en gränsbevakningsman kan utföra brottsbekämpningsuppdrag. Bestämmelser om polisens gränskontrolluppgifter och befogenheter i anslutning till dem finns i 2 kap. 21 § i polislagen och bestämmelser om Tullens uppgifter och befogenheter i anslutning till in- och utresekontroller i 31 § i tullagen. Enligt paragraferna har en polisman och en tullman rätt att genomföra in- eller utresekontroller med de befogenheter som föreskrivs för en gränsbevakningsman i bland annat 28 § i gränsbevakningslagen.

Rätten att få åtkomst till uppgifterna i interoperabilitetsramen är bunden till uppgiften. Vid in- och utresekontrolluppgifter får en polisman, gränsbevakningsman och tullman rätt att få åtkomst till de register som interoperabilitetsramen innehåller och som behövs för genomförandet av in- och utresekontroller. Systemet ger åtkomst till de uppgifter som behövs automatiskt när en individpost lagras i in- och utresesystemet. Samma mekanism gäller också utfärdande av viseringar.

I brottsbekämpningsuppdrag får samma polis-, gränsbevaknings- eller tullman rätt till uppgifter endast genom artiklarna 20 och 22.

4.2 De huvudsakliga konsekvenserna

4.2.1 Konsekvenser för myndigheternas verksamhet

Nationellt genomförande och nationell styrning av interoperabilitetshelheten

Inrikesministeriet inrättade i samarbete med justitieministeriet, utrikesministeriet och finansministeriet ett nationellt interoperabilitetsprojekt för att säkerställa och samordna genomförandet av interoperabilitetsförordningarna i Finland.

Med hjälp av projektet samordnas det nationella deltagandet i utvecklingen av EU:s centraliserade informationssystem, till den del riktlinjerna inverkar på det praktiska genomförandet av interoperabiliteten samt säkerställs att de ändringar som interoperabiliteten medför genomförs i rätt tid.

Genom projektet följs också de nationella projekt som inrättats i fråga om informationssystemen på EU-nivå. Varje ansvarig myndighet (polisen, Gränsbevakningsväsendet, Tullen, Migrationsverket, Rättsregistercentralen och utrikesministeriet) ansvarar dock för det praktiska genomförandet av interoperabiliteten, för att nationella ändringar och åtgärder genomförs i rätt tid och för resurserna för dem.

Polisen, Tullen och Gränsbevakningsväsendet

I och med reformen är EU:s nuvarande och kommande informationssystem i förbindelse med varandra. EU:s informationsarkitektur i anslutning till gränssäkerhet och inre säkerhet kommer inte att vara splittrad längre. Förordningarna om informationssystemens interoperabilitet bildar en förbindelse till befintliga EU-informationssystem och möjliggör sökning av personuppgifter via en enda portal.

De brottsbekämpande myndigheternas informationssökning underlättas på många olika sätt, eftersom EU:s databaser kan användas på ett effektivare och säkrare sätt än tidigare. Interoperabiliteten mellan informationssystemen erbjuder polisen, Tullen och Gränsbevakningsväsendet möjlighet att med full respekt för deras åtkomsträttigheter och för ändamål som hänför sig till deras uppgifter utföra sökningar i flera informationssystem samtidigt så att de samlade resultaten presenteras i samma vy. Dessutom förbättras uppgifternas integritet när eventuella inmatningsfel kan upptäckas och avlägsnas redan när uppgifterna matas in.

Informationssökningen sker så att säga i två faser, när en myndighets sökning i en sökportal ger en träff i något system kan myndigheten begära riktad åtkomst till det berörda systemet i enlighet med de regler och begränsningar som gäller för detta. Interoperabiliteten mellan EU-informationssystemen ändrar således inte de regler som gäller åtkomst till EU-informationssystemen eller begränsning av användningsändamålet. Interoperabilitet mellan EU-informationssystem förenklar och effektiviserar myndigheternas åtkomst till EU-informationssystemen, men skapar inga nya befogenheter i sig. Åtkomsträttigheterna baserar sig på den rättsliga grunden för respektive informationssystem och på motsvarande nationella bestämmelser.

I brottmål som Tullen utreder är en stor del av de brottsmisstänkta utländska medborgare eller i Finland bosatta personer som är medborgare i andra länder. När man utreder brott samt skaffar fram och samlar in bevis behövs ofta information om hur personen har rört sig vid EU:s yttre gränser och om den gripne över huvud taget är den person som framgår av resedokumenten. Vid brottsutredningar finns det ofta också ett behov av att snabbt upprätta kontakt med utländska brottsbekämpande myndigheter och begära att tvångsmedelsåtgärder vidtas enligt en brådskande tidtabell, så att bevis inte undanröjs och att återvinningen av vinningen av brott kan tryggas. I samband med detta underlättar och påskyndar interoperabilitet mellan EU-informationssystem Tullens brottsutredning genom att möjliggöra sökning av personuppgifter via en enda portal.

När det gäller den avslöjande verksamheten inom Tullen sammanförs i analysen information om målpersonen från flera olika informationskällor. I den avslöjande verksamheten kan man genom interoperabilitet mellan EU-informationssystem säkerställa en tillräcklig rättssäkerhet för målpersonen, när identiteten kan fastställas på ett tillförlitligt sätt i samband med åtgärder som begränsar de grundläggande fri- och rättigheterna.

En av Tullens uppgifter när det gäller övervakningen av internationell handel och godstrafik är att säkerställa unionens och dess invånares säkerhet. I artikel 3 i Europaparlamentets och rådets förordning (EU) nr 952/2013 om fastställande av en tullkodex för unionen föreskrivs att det är tullmyndigheternas uppgift att vidta åtgärder i anslutning till detta. I flera speciallagar finns det också bestämmelser om Tullens övervakningsuppgifter i anslutning till import och export av varor. Till exempel i 16 § i strålningslagen (859/2018) föreskrivs det om Tullens övervakningsuppgifter vid import och export av strålkällor och radioaktivt avfall. I samband med kontrollen av godsförsändelser kan man bli tvungen att utreda identiteten hos den som transporterar godset. Det är särskilt behövligt att utreda identiteten när en resenär i sin kropp misstänks föra in förbjudna ämnen i landet. Då har det inte nödvändigtvis ännu inletts en förundersökning av brott,

eftersom det enligt 18 § 3 mom. i tullagen får utföras en sådan kroppsbesiktning eller kroppsvisitation som avses i 8 kap. 30 § i tvångsmedelslagen utan att förundersökning inleds, förutsatt att de föreskrivna förutsättningarna uppfylls. En tillförlitlig utredning av identiteten med hjälp av EU:s gemensamma informationssystem kan minska behovet av att i onödan ingripa i de grundläggande fri- och rättigheterna för de personer som blir föremål för tullkontroller, därutöver blir genomförandet tullkontroller snabbare, vilket kan vara till stor nytta för exempelvis resenärer.

Interoperabiliteten mellan EU-informationssystemen förutsätter i fråga om SIS manuell verifiering av länkar, det vill säga identiteter, som skapats i MID. När det alltså är fråga om 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. Finlands Sirenekontor är förlagt till centralkriminalpolisen.

Länkarna kan uppstå mellan en SIS-registrering och vilket annat informationssystem som helst inom interoperabilitetshelheten. Detta innebär att det kan uppstå en länk mellan en personregistrering som har matats in av Finland och till exempel en uppgift i in- och utresesystemet som har matats in av en annan medlemsstat, det vill säga antalet länkar är inte direkt beroende av antalet registreringar i Finland.

Effektiv samkörning, analys, insamling och spridning av information med moderna hjälpmedel och uppdaterad lagstiftning är av största vikt. Bekämpning av gränsöverskridande brottslighet lyckas endast om informationsutbytet mellan brottsbekämpande myndigheter fungerar i realtid, smidigt och utan onödig byråkrati i samband med processerna. Förordningarna svarar delvis på utmaningar inom det internationella polissamarbetet genom att möjliggöra och effektivisera modeller och system för flermyndighetssamarbete.

Polismyndigheternas åtkomst till CIR i enlighet med artiklarna 20 och 22 är ett nytt verktyg för att utreda en persons identitet. I och med interoperabilitetsförordningarna blir det således lättare och snabbare att identifiera personer och det behövs nödvändigtvis inte ett ingripande i de grundläggande fri- och rättigheterna på samma sätt som vid gripande.

Migrationsverket

Uppgifter som inverkar på Migrationsverkets verksamhet är i vissa situationer uppgifter som hänför sig till gula länkar och manuell verifiering av olika identiteter enligt artiklarna 21, 26 och 29 i gränsinteroperabilitetsförordningen. Eventuella konsekvenser kan också uppstå i samband med bistånd till andra myndigheter för skötseln av deras uppgifter som följer av förordningarna.

De mest betydande ändringarna gäller koncentreringen av vissa registersökningar och verifieringar av uppgifter vid Migrationsverket via ESP. Migrationsverket ska i fortsättningen ha åtkomst för att utföra sökningar i uppgifterna i VIS, in- och utresesystemet, Etias, SIS och Eurodac med hjälp av ESP. Migrationsverket har planerat att genomföra dessa sökningar automatiserat i så hög grad som möjligt och att till denna del också integrera sig i polisens Renki-system.

Utrikesministeriet

Inom utrikesministeriets förvaltningsområde kommer interoperabilitetshelheten att orsaka betydande process- och systemförändringar i det nationella informationssystemet för viseringar (viseringssystemet VISA). Tekniskt sett ska VISA integreras med interoperabilitetskomponenterna (ESP och CIR). Dessutom ska hänsyn tas till ändringar i gränssnitt och processer i VIS. Vid behandlingen av ansökningar om viseringar och det tekniska genomförandet ska man beakta situationer där ett förfarande i MID som inletts i samband med lagringen av personuppgifter ger upphov till multipla identiteter (länkar) från flera system.

Rättsregistercentralen

Förordningen om Ecris-TCN (EU 2019/816) har trätt i kraft den 11 juni 2019. I förordningen föreskrivs det om inrättande av ett centraliserat informationssystem som innehåller identifieringsuppgifter om tredjelandsmedborgare som fått en fällande brottmålsdom i en EU-medlemsstat. Samtidigt trädde ett direktiv (EU 2019/884) i kraft som ändrar rambeslutet om EU-utbyte av uppgifter ur kriminalregister och ersätter det så kallade Ecris-beslutet.

Informationsutbytet i Ecris sker via medlemsstaternas centralmyndigheter. I Finland är centralmyndigheten Rättsregistercentralen, som även för närvarande spelar en central roll i samarbetet mellan medlemsstaterna i fråga om utbyte av uppgifter ur kriminalregister. Det centraliserade systemet Ecris-TCN som innehåller identifieringsuppgifter om tredjelandsmedborgare tas i drift vid slutet av 2022. Med stöd av artikel 29.1–29.3 i polisinteroperabilitetsförordningen svarar Rättsregistercentralen nationellt för den manuella verifieringen av olika identiteter i samband träffar som uppstår vid registrering eller ändring av uppgifter i Ecris-TCN i enlighet med artikel 5 eller 9 i förordningen. Rättsregistercentralen räknas dock inte som en nationellt behörig polismyndighet i identifieringsuppgifter enligt artikel 20.

Samarbete och kanaler för informationsutbyte mellan de nationella förundersökningsmyndigheterna, Sirenekontoret och andra myndigheter som svarar för den manuella verifieringen av olika identiteter ska säkerställas.

4.2.2 Ekonomiska konsekvenser

Interoperabilitetsförordningarna förutsätter ändringar i nationella informationssystem som gäller flera förvaltningsområden och ämbetsverk (Polisstyrelsen, Gränsbevakningsväsendet, Migrationsverket, Tullen, utrikesministeriet, justitieministeriet och Rättsregistercentralen). Utöver detta ska det sörjas för behövliga ändringar i datanätsmiljöerna. Utöver de tekniska ändringarna medför interoperabilitetsförordningarna även ändringar för dessa myndigheters funktioner och personalresurser.

De behov av anslag som föranleds av interoperabilitetsförordningarna har behandlats som en del av beredningen av planen för de offentliga finanserna 2022–2025 samt som en del av beredningen av tilläggsbudgetarna för 2021 och budgeten för 2022.

Utvecklingen och genomförandet på nationell nivå av EU-informationssystemen har understötts av Fonden för inre säkerhet (ISF) under programperioden 2014–2020. Kommissionen anvisade medlemsstaterna tilläggsfinansiering för EU-informationssystemen (in- och utresesystemet, Etias, SIS III och allmän ICT-utveckling). Finlands andel av tilläggsfinansieringen uppgick till sammanlagt cirka 13,3 miljoner euro. Under programperioden 2021–2027 hör interoperabiliteten till tillämpningsområdet för EU:s fonder för inrikes frågor. De nationella programmen för

fonderna för perioden 2021–2027 bereds och fonderna utnyttjas i genomförandet av interoperabilitetsförordningarna i den utsträckning det är möjligt.

Myndigheternas behov av anslag är enligt nuvarande uppskattningar sammanlagt 21,4 miljoner euro enligt följande fördelning:

Anslagsbehov 1000 €	**Uppskattning 2021**	**Uppskattning 2022**	**Uppskattning 2023**	**Uppskattning 2024**	**Uppskattning 2025**
Polisstyrelsen	482	1 638	1 173	658	170
Centralkriminalpolisen				1 600	1 600
Migrationsverket	605	1 158	1 803	1 399	92
Gränsbevakningsväsendet		750	150	100	
Justitieministeriet	88	151	123	43	43
Utrikesministeriet	260	1 990	1 300	1 300	
Tullen	75	225	175		
Utgifter för förvaltning (gemensamma)	312	514	452	462	472
Sammanlagt	**1 822**	**6 426**	**5 176**	**5 562**	**2 377**

Polisförvaltningen

Arbetsvolymen för Sirenekontoret, som är förlagt till centralkriminalpolisen, kommer att öka, eftersom kontoret kommer att vara den myndighet som ansvarar för den manuella verifieringen av olika identiteter. Länkar mellan registreringar som upprättats i EU-informationssystem kan uppstå mellan en SIS-registrering och vilket annat informationssystem som helst inom interoperabilitetshelheten. Detta innebär att det kan uppstå en länk mellan en personregistrering som har matats in av Finland och till exempel en uppgift i in- och utresesystemet som har matats in av en annan medlemsstat, det vill säga antalet länkar är inte direkt beroende av antalet registreringar i Finland.

I regeringens proposition om SIS (RP 35/2021 rd) konstateras att det till de registreringar som matas in i SIS inte längre inom ramen för den nationella lagstiftningen kan fogas biometriska kännetecken, bland annat registreringar om förbud mot tillbakasändning och inreseförbud, som lagrats i de nationella registren med stöd av utlänningslagen (301/2004), passlagen (671/2006) eller lagen om identitetskort (663/2016). Avsaknaden av biometriska kännetecken i SIS-registreringarna kommer att medföra fler begäranden om ytterligare informationsutbyte och öka arbetsvolymen i fråga om behandlingen av sådana länkar mellan SIS och andra EU-informationssystem som inom ramen för interoperabiliteten verifieras manuellt.

Det är svårt att i detta skede bedöma antalet länkar som ska verifieras manuellt och de ekonomiska konsekvenserna av detta, eftersom både de tekniska lösningarna för eu-LISA och mängden länkar inverkar.

Det finns ännu inte någon uppskattning eller preciserad information om antalet länkar som kommer att behandlas manuellt. Förslaget har eventuellt betydande konsekvenser för resurserna i form av ökad arbetsvolym.

Gränsbevakningsväsendet

Vid Gränsbevakningsväsendet pågår två stora reformer av EU-informationssystem, in- och utresesystemet och EU-systemet för reseuppgifter och resetillstånd Etias. Avsikten är att dessa tas i drift 2022. Idrifttagningen av in- och utresesystemet innebär betydande ändringar av den nationella processen för in- och utresekontroller. En del av de tekniska ändringar som interoperabilitetsförordningarna förutsätter kan beaktas i utvecklingen av in- och utresesystemet och Etias, men idrifttagningen av interoperabilitetskomponenterna förutsätter också betydande ändringar av den nationella gränskontrollapplikationen så att de sökningar som behövs stöds, de uppgifter som sökningen ger upphov till kan behandlas på ett ändamålsenligt sätt och bland annat att de uppgifter om individen som behövs ska kunna länkas.

Den mest betydande ändringen av idrifttagningen av interoperabilitetsförordningarna som ger upphov till ekonomiska konsekvenser hänför sig till den ökade arbetsvolymen. År 2019, det vill säga det sista året före coronaviruspandemin, passerade sammanlagt 16,78 miljoner personer Finlands yttre gräns. Av dessa var 10,52 miljoner utlänningar vars uppgifter lagras i de informationssystem som ingår i interoperabilitetsramen, särskilt i in- och utresesystemet, VIS, och Etias. Den manuella utredningen av de gula länkarna kommer att öka gränskontrollanternas arbetsvolym och användningen av ESP och MID kan förlänga varaktigheten för in- och utresekontrollerna, och då minskar genomströmningskapaciteten vid gränsövergångsställena i Finland. Att bevara genomströmningskapaciteten på nuvarande nivå förutsätter en ökning av antalet anställda och en strukturell utveckling av gränsövergångsställena.

I detta skede har Gränsbevakningsväsendet inte tillräckliga grunder för att bedöma antalet gula länkar och den ökning av arbetsvolymen som utredningen av dem medför eller hur mycket långsammare processen blir till följd av ESP:s och MID:s verksamhet. De första bedömningarna kan göras tidigast när arbetet med att utveckla komponenterna har framskridit till prototyp- eller testningsstadiet. Andra än tekniska tilläggsbehov till följd av idrifttagningen av funktionerna behandlas som en del av planeringen av Gränsbevakningsväsendets verksamhet och ekonomi.

Tullen

Interoperabilitetsförordningarna förutsätter vissa ändringar och åtgärder i Tullens informationssystem. Tullen kommer att använda ESP och tillhörande interoperabilitetskomponenter via Polisens Renki-system. Tullen har redan rätt att använda Renki-systemet, och därför bör Tullens åtkomsträttigheter i detta sammanhang endast kompletteras så att de utvidgas till att gälla också nya sökportaler och system. Tullens mål inom den närmaste tiden är att skapa en integration till Renki-systemet via ärendehanteringssystemet. Kostnadskalkylen för arbetet är cirka 100 000 euro. I kostnadskalkylen ingår integrationen av ärendehanteringen i Renki-systemet samt eventuella ekonomiska konsekvenser i anslutning till Renki-användargränssnittet. Idrifttagningen av systemet har även ekonomiska konsekvenser när det gäller förvaltningen av systemet och utbildningen av personalen i användningen av systemet. I fråga om Tullen är antagandet att interoperabiliteten mellan EU-informationssystemen kommer att påskynda processerna och minska det manuella utredningsarbetet och därigenom uppnå ekonomiska besparingar på lång sikt.

Migrationsverket

De ekonomiska konsekvenser som interoperabilitetsförordningarna medför för Migrationsverket hänför sig i huvudsak till ändringar i informationssystemen och personalkostnader i anslutning till genomförandet av dem. Dessutom har Migrationsverket bedömt att behovet av permanent personalökning i anslutning till EU:s gemensamma informationssystem och förvaltningen av dem är ett årsverke från och med 2026.

Utrikesministeriet

Utrikesförvaltningens arbetsvolym ökar på grund av verifieringen av olika identiteter och den manuella utredningen av länkarna som gäller dem. Det är svårt att i detta skede bedöma antalet länkar och det behov av tilläggsresurser som detta medför. De ekonomiska konsekvenserna för utrikesförvaltningen orsakas framför allt av arbetet med att utveckla informationssystemet, deltagandet i de officiella testningar som eu-LISA kräver och den nationella testningen.

Justitieministeriet

Ecris-TCN används genom ESP i vissa användningssituationer. Att ansluta ESP nationellt kräver att Rättsregistercentralen vidtar åtgärder som hänför sig till utvecklingen av och interoperabiliteten hos informationssystemet CRIS. Syftet är att göra det möjligt att använda ESP, som ingår i interoperabiliteten mellan informationssystemen på EU-nivå (IO-helheten), i samband med sökningar i Ecris-TCN genom att använda det nationella systemet CRIS för att utföra sökningar. Funktionen bör vara klar att tas i drift i samband med idrifttagningen av Ecris-TCN under 2022–2023. Tills vidare vet man inte exakt hurdana ändringar i informationssystemen som krävs för anslutning till ESP och således måste kostnadernas storlek ännu preciseras i takt med att interoperabilitetsprojektet framskrider. Även idrifttagningen av andra interoperabilitetskomponenter förutsätter ändringar i synnerhet i det nationella systemet CRIS samt integration med CIR och MID. Dessutom ökar Rättsregistercentralens arbetsvolym på grund av den manuella verifieringen av olika identiteter och hanteringen av säkerhetstillbud på det sätt som förutsätts i artikel 43 i förordningarna, men det är svårt att i detta skede bedöma det eventuella behov av tilläggsresurser som dessa medför.

Genomförandet av förordningarna om interoperabilitet medför i någon mån ytterligare tillsynsuppgifter för dataombudsmannen. I synnerhet tillsynen över de uppgifter som överförts nationellt till interoperabilitetskomponenterna samt de uppgifter ur komponenterna som behandlas nationellt medför extra arbete. Trots att det i huvudsak är Europeiska datatillsynsmannen som utövar tillsyn över de interoperabla EU-informationssystemen i fråga, ökar de nationella myndigheternas uppgifter särskilt på grund av lagstiftningslösningar och karaktären av de tekniska lösningarna. Även samarbetet mellan EU:s tillsynsmyndigheter har vissa konsekvenser. Enligt en preliminär uppskattning medför genomförandet extra arbete på högst 1 årsverke.

4.2.3 Konsekvenser av förändringar i informationshanteringen

I lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan informationshanteringslagen) finns det bestämmelser bland annat om ordnandet och beskrivningen av informationshantering, interoperabilitet mellan informationslager, genomförandet av tekniska gränssnitt och elektroniska förbindelser samt genomförandet av informationssäkerhet. Genom informationshanteringslagen säkerställs en enhetlig förvaltning och en informationssäker behandling av myndigheternas informationsmaterial som ett led i genomförandet av offentlighetsprincipen.

Ett gemensamt användargränssnitt för sökningar som kallas Renki bereds av polisen för nationella behov. Syftet är att slutanvändaren via detta gränssnitt ska få åtkomst till de informationssystem som han eller hon har lagstadgad rätt till genom att utföra en enda sökning. Avsikten är att den åtkomst till ESP som interoperabilitetsförordningarna förutsätter ska integreras i Renki.

Till följd av interoperabilitetsförordningarna blir man i Gränsbevakningsväsendets informationssystem tvungen att utveckla en gränskontrollapplikation och dess egenskaper för att de ska stödja de funktioner som interoperabilitetsförordningarna förutsätter, inte bara när det gäller de centraliserade sökningar som görs och ändringar i de svar som fås av dem, utan också när det gäller att genomföra nya egenskaper med tanke på behandlingen av de svar som fåtts. Ändringarna hänför sig till behandlingen av länkar som gäller identitet, ändringar av utbyte och förbindelser i fråga om ESP-sökningar samt informationsförmedlingslösningar när det gäller behandlingen av länkar. I lösningarna kommer man att utnyttja de lösningar som har genomförts i fasen för in- och utresesystemet och Etias samt befintliga genomföranden i den mån det är möjligt, men ändringar måste göras i gränskontrollapplikationen Ratas samt i sökmotorn Ulkonet i fråga om genomförandet av ESP-sökningarna. Utöver de befintliga genomförandena fortsätter samarbetet och samutnyttjandet med andra myndigheter i fråga om systemen och lösningarna i anslutning till informationshanteringen i tillämpliga delar, till exempel när det gäller användningen av Renki.

Tullen kommer att ansluta sig till ESP via Renki-systemet på samma sätt som polisen. Tullen har redan rätt att använda Renki-systemet och använder systemet enligt egna befogenheter på samma sätt som polisen. Under de kommande åren kommer Tullen att förnya sina informationssystem och då kommer en anslutning till ESP att bedömas på nytt.

Utrikesministeriet kommer att genomföra ändringar och nya egenskaper i viseringssystemet VISA för att det ska stödja de funktioner som förutsätts i interoperabilitetsförordningarna. Via viseringssystemet VISA är det möjligt att inleda en sökning i flera informationssystem via den nya ESP-sökportalen i enlighet med slutanvändarnas rättigheter. I systemet förverkligas dessutom behandlingen av länkar som gäller olika identiteter och förmedlingen av information. För att genomföra dessa funktioner krävs det ändringar av utbyte och förbindelser mellan viseringssystemet VISA och de nya centralsystemkomponenterna. Funktioner och processer för behandling och visning av uppgifter planeras så att de effektivt stöder de myndigheter som använder viseringssystemet VISA.

Inom Migrationsverkets förvaltningsområde kommer interoperabilitetshelheten för informationssystemen att orsaka betydande process- och systemförändringar ärendehanteringssystemet för utlänningsärenden UMA.

Varje ämbetsverk bedömer för sin del om de ändringar som görs i de informationssystem som de ansvarar för förutsätter ett genomförande av utlåtandeförfarandet enligt 9 § i informationshanteringslagen.

I propositionen föreslås inga ändringar i de gällande bestämmelserna om offentlighet och sekretess i fråga om handlingar.

5 Alternativa handlingsvägar

5.1 Handlingsalternativen och deras konsekvenser

Interoperabilitetsförordningarna är direkt tillämplig rätt. I artikel 20 i förordningarna föreskrivs det om åtkomst till CIR för identifiering av personer. Enligt artikeln är det möjligt att få åtkomst

i två olika situationer som det föreskrivs om i artikel 20.1 och 20.4. Den behöriga myndigheten kan få åtkomst till CIR endast om det särskilt har föreskrivits om det genom nationell lag. I Finland föreslås det att det utfärdas kompletterande nationell lagstiftning när det gäller artikel 20. Till övriga delar ger förordningarna inte möjlighet att utfärda nationella bestämmelser om saken.

5.2 Handlingsmodeller som planeras eller används i andra medlemsstater

I början av 2021 tillfrågades de andra medlemsstaterna om de har för avsikt att införa artikel 20 i polis- och gränsinteroperatilitetsförordningarna och utfärda nationell lagstiftning i fråga om artikeln.

Sverige, Polen, Lettland, Tyskland, Belgien och Cypern meddelade att de håller på att införa artikel 20 i interoperabilitetsförordningarna och att de utfärdar nationell lagstiftning om detta.

Tjeckien och Spanien ansåg att deras nationella lagstiftning redan är tillräcklig för att ge de behöriga myndigheterna åtkomst till CIR. Även i Kroatien har de behöriga myndigheterna åtkomst till CIR, trots att det inte direkt har konstaterats i den nationella lagen om behandling av biometriska uppgifter (Biometric Data Processing Act).

Österrike, Cypern, Ungern och Frankrike här ännu inte fattat något slutgiltigt beslut.

Enligt fördragen ska Irland meddela om sin vilja att genomföra interoperabilitetsförordningarna (så kallat opt-in). Irland har för avsikt att agera på detta vis och efter det utfärda nationell lagstiftning som gör det möjligt för de behöriga myndigheterna att få åtkomst till CIR i enlighet med artikel 20 i interoperabilitetsförordningarna.

6 Remissvar

Utlåtanden om utkastet till proposition gavs av utrikesministeriet, justitieministeriet, finansministeriet, inrikesministeriets migrationsavdelning och gränsbevakningsavdelning, dataombudsmannens byrå, Polisstyrelsen, centralkriminalpolisen, skyddspolisen, Migrationsverket, Tullen och Rättsregistercentralen.

I utlåtandena föreslogs inga ändringar till det valda tillvägagångssättet, det vill säga att Finland utnyttjar det nationella handlingsutrymmet i interoperabilitetsförordningarna så att man genom reglering gör det möjligt för de behöriga myndigheterna att få åtkomst till EU:s gemensamma databas för identitetsuppgifter.

Justitieministeriet och dataombudsmannens byrå fäste uppmärksamhet vid behovet av att precisera förslaget om polisens rätt att vid en naturkatastrof, olycka eller ett terrordåd utföra sökningar i den gemensamma databasen för identitetsuppgifter för att identifiera okända personer som inte kan identifiera sig eller att utföra sökningar med biometriska uppgifter för att identifiera oidentifierade mänskliga kvarlevor. I den fortsatta beredningen preciserades den berörda föreslagna paragrafen och dess motivering. Dessutom kompletterades propositionen genom att det fogades hänvisningar till de bestämmelser som tillämpas på behandlingen av personuppgifter.

Inrikesministeriets gränsbevakningsavdelning föreslog att 3 § 2 mom. i lagförslaget preciseras så att inte bara Tullen utan också Gränsbevakningsväsendet ska ha möjlighet att utnyttja identifieringen av personer enligt artikel 20 i de situationer som avses i momentet, när Gränsbevak-

ningsväsendet sköter tulluppgifter i enlighet med 24 och 34 § i gränsbevakningslagen. Propositionen ändrades i enlighet med detta. På framställning av inrikesministeriets gränsbevakningsavdelning och migrationsavdelning preciserades motiveringarna genom att till dem fogades ett omnämnande om övervakningen av utlänningar enligt utlänningslagen.

Skyddspolisen föreslog att tillämpningsområdet för 3 § i lagförslaget utvidgas så att polisen och Gränsbevakningsväsendet kan använda den gemensamma databasen för identitetsuppgifter för att identifiera en person när det behövs för att förhindra sådana aktiviteter och planer som kan utgöra ett hot mot rikets yttre eller inre säkerhet. I lagförslaget har man noggrant hållit sig till de mål som nämns i EU-förordningen. Det är fråga om användning av personuppgifter, inklusive biometriska uppgifter, och därför har man strävat efter att tolka förordningen restriktivt till den del som medlemsstaterna har getts möjlighet att föreskriva om saken nationellt. Därför föreslås det att tillämpningsområdet inte utvidgas.

7 Specialmotivering

1 §. *Tillämpningsområde.* I paragrafen föreslås en bestämmelse om lagens tillämpningsområde. Av paragrafen framgår det att lagen innehåller kompletterande bestämmelser om tillämpningen av polis- och gränsinteroperabilitetsförordningarna i Finland.

2 §. *Behörig myndighet.* I paragrafen föreslås bestämmelser om behöriga myndigheter i de situationer som nämns i artikel 20 i polis- och gränsinteroperabilitetsförordningarna. I artikel 20 föreskrivs det om åtkomst till EU:s gemensamma databas för identitetsuppgifter (CIR) för identifiering av en person. I artikel 20 används termen polismyndighet och dess innehåll definieras i artikel 4.19 i förordningarna. Definitionen är mycket omfattande och inbegriper brottsbekämpande myndigheter och rättsliga myndigheter. I denna lag används termen behörig myndighet, eftersom termen polismyndighet i Finland har en etablerad betydelse som inte överensstämmer med definitionen i polis- och gränsinteroperabilitetsförordningarna. I Finland föreslås endast polisen, Gränsbevakningsväsendet och Tullen bli behöriga myndigheter. Skötseln av dessa myndigheters uppgifter kan förutsätta att det för identifieringen av en person ska kunna utföras en sökning i CIR.

I CIR lagras uppgifter från in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN. Enligt polis- och gränsinteroperabilitetsförordningarna bör CIR lagra de personuppgifter som behövs för att göra det möjligt att mer korrekt identifiera de personer vars uppgifter lagras i de ovannämnda systemen, inklusive deras identitetsuppgifter, resehandlingsuppgifter, och biometriska uppgifter. Endast de personuppgifter som är absolut nödvändiga för att utföra en korrekt identitetskontroll bör lagras i CIR. I praktiken fungerar systemet så att när ovannämnda uppgifter lagras i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN, lagras dessa uppgifter automatiskt i CIR. Uppgifter lagras alltså inte enbart i CIR.

Identifiering enligt artikel 20 kan utnyttjas till exempel i polisens verksamhet i situationer där en person behöver identifieras för genomförande av en enskild uppgift och personen vägrar låta sin identitet utredas. När polisen kan använda uppgifter från CIR för att identifiera en person blir identifieringen lättare och snabbare och det behövs nödvändigtvis inte ett ingripande i de grundläggande fri- och rättigheterna på samma sätt som vid gripande.

I Gränsbevakningsväsendets verksamhet kan identifiering enligt artikel 20 utnyttjas till exempel i situationer där det vid riksgränsen har upptäckts olovlig gränspassage och det vid den efterspaning som inleds till följd av situationen påträffas en tredjelandsmedborgare som promenerar längs vägnätet nära gränsen och som inte kan visa upp resedokument eller andra identitetshandlingar. Genom att använda uppgifter från CIR kan man identifiera såväl personer som lagligen

vistas inom EU (in- och utresesystemet, Eurodac) som personer vars inresa till EU-området har förbjudits (SIS).

Tullen kan utnyttja identifieringen av personer enligt artikel 20 när det behövs för att avslöja eller förhindra olaglig införsel, utförsel eller transitering av sådana föremål eller ämnen som orsakar fara. Det kan vara fråga om till exempel vapen, kemikalier som orsakar fara, radioaktivt avfall eller en situation där en person i kroppen misstänks föra olagliga ämnen över gränsen och personen vägrar låta sin identitet utredas. Att identifiera personen med hjälp av den gemensamma databasen för identitetsuppgifter påskyndar identifieringen och gör kontrollprocessen smidigare.

3 §. *Åtkomst till den gemensamma databasen för identitetsuppgifter.* Om en medlemsstat vill ge polismyndigheten rätt utföra sökningar i EU:s gemensamma databas för identitetsuppgifter i syfte att identifiera en person, ska det enligt artikel 20.5 i polis- och gränsinteroperabilitetsförordningarna i de nationella författningar som gäller detta anges de exakta syftena med identifieringen inom ramen för de mål som avses i artikel 2.1 b och c i polis- och gränsinteroperabilitetsförordningarna. Enligt dessa led ska sådana mål vara att bidra till att förebygga och bekämpa olaglig invandring samt att bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, inbegripet att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier.

I paragrafens *1 mom.* föreslås det att polisen och Gränsbevakningsväsendet i syfte identifiera en person ska ha rätt att använda CIR för att bidra till att förhindra och bekämpa olaglig invandring eller upprätthålla den allmänna ordningen och säkerheten. Det nationella tillämpningsområdet är således mer begränsat än vad polis- och gränsinteroperabilitetsförordningarna möjliggör. Det föreslås att möjligheten att söka i CIR lämnas utanför tillämpningsområdet när målet är att bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen. Användningen av CIR ska också vara nödvändig för identifieringen av personen. Rätten ska också gälla användningen av biometriska fingeravtryck och ansiktsbilder.

Vid förhindrandet och bekämpandet av olaglig invandring är det väsentligt att utreda den riktiga identiteten hos personer som kommer till landet och som vistas i landet, om identiteten är oklar. I sådana fall är det motiverat att söka i CIR. Likaså är det vid upprätthållandet av den allmänna ordningen och säkerheten viktigt att den behöriga myndigheten kan försäkra sig om en persons riktiga identitet. En sökning i CIR kan behövas när den behöriga myndigheten 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.

I paragrafens *2 mom.* föreskrivs det om Tullens rätt söka i CIR för att identifiera en person, när det används för att avslöja och förhindra olaglig införsel, utförsel eller transitering av sådana varor eller ämnen som är till fara för människor eller miljön. Användningen av CIR ska också vara nödvändig för identifieringen av personen. Rätten ska också gälla användningen av biometriska fingeravtryck och ansiktsbilder. De användningsändamål som föreslås för Tullen baserar sig på det mål för förordningarna som nämns i artikel 2.1 c i polis- och gränsinteroperabilitetsförordningarna och som är att trygga säkerheten på medlemsstaternas territorier. Även Gränsbevakningsväsendet har motsvarande rätt när väsendet sköter tulluppgifter i enlighet med 24 och 34 § i gränsbevakningslagen.

I paragrafens *3 mom.* hänvisas det närmare till artikel 20.2 och 20.3 i interoperabilitetsförordningarna, där det föreskrivs närmare om de förfaranden som de behöriga myndigheterna ska

iaktta när de utför sökningar i CIR. En polis, tullman eller gränsbevakare ska inleda ett förfarande för identifiering av en person i den berörda personens närvaro. Sökningar får inte utföras för identifiering av minderåriga under 12 år, såvida de inte görs för barnets bästa. Den behöriga myndigheten överväger när det bästa för minderåringen under 12 år är att hans eller hennes identitet fastställs. En sådan situation kan uppstå om en myndighet till exempel har fått en uppfattning om att barnet är ett brottsoffer.

Om en sökning som utförts i CIR visar att det har lagrats uppgifter om den berörda personen i CIR, har myndigheten rätt att få åtkomst till dessa uppgifter. Myndigheten får alltså endast åtkomst till uppgifterna i CIR. I CIR finns sådana personuppgifter om tredjelandsmedborgare som lagrats i VIS, Eurodac, in- och utresesystemet, Etias och Ecris-TCN samt biometriska uppgifter och resehandlingsuppgifter. När en myndighet utför en sökning i CIR får myndigheten också uppgifter om i vilket eller vilka av de ovannämnda informationssystemen det finns närmare uppgifter om den berörda personen. Åtkomst till dessa uppgifter fås på de villkor som anges i den rättsliga grunden för det berörda informationssystemet.

Om en persons biometriska uppgifter inte kan användas eller om en sökning med dem misslyckas, kan sökningen utföras med den berörda personens identitetsuppgifter tillsammans med resehandlingsuppgifterna eller med de identitetsuppgifter som den berörda personen lämnat.

Enligt paragrafens *4 mom.* har polisen rätt att vid en naturkatastrof, olycka eller ett terrordåd utföra sökningar i CIR med biometriska uppgifter för att identifiera ett sådant offer som inte kan identifiera sig. Dessutom ska polisen i sådana situationer ha rätt att utföra sökningar med biometriska uppgifter för att identifiera oidentifierade mänskliga kvarlevor. Bestämmelsen grundar sig på artikel 20.4 och 20.6 i interoperabilitetsförordningarna. Utförandet av sökningar ska vara begränsat till endast sådana situationer där det är nödvändigt.

Polisen har redan i nuläget en omfattande rätt att utreda en okänd persons eller avliden persons identitet. Den rättsmedicinska utredningen av dödsorsak hör till polisens uppgifter. Identifieringen av offer utgör en del av utredningen av dödsorsak. Under vissa förutsättningar kan också biometriska uppgifter som lagrats i polisens nationella register användas för att identifiera ett offer. Enligt 15 § 2 mom. i lagen om behandling av personuppgifter i polisens verksamhet får biometriska uppgifter som behandlas för utförande av de uppgifter som föreskrivs i lagen om identitetskort och passlagen användas för andra ändamål än det ursprungliga ändamålet med behandlingen av uppgifterna om det är nödvändigt för att identifiera ett offer för en naturkatastrof, storolycka eller någon annan katastrof eller ett offer för ett brott eller ett offer som annars förblivit oidentifierat. Enligt 4 mom. i den paragrafen får även biometriska uppgifter som behandlas för utförande av uppgifter enligt 131 § i utlänningslagen användas för andra ändamål än det ursprungliga ändamålet med behandlingen av uppgifterna i de fall som avses i 2 mom.

I momentet föreslås rätten att söka i CIR endast för polisen, eftersom polisen redan nu svarar för identifieringen av personer i de situationer som avses i momentet och detta hör inte till Gränsbevakningsväsendets eller Tullens uppgifter.

I *5 mom*. föreskrivs det att endast biometriska uppgifter om sådana offer eller avlidna som avses i 4 mom. får användas för sökningar som utförs för att identifiera okända offer eller avlidna. Den föreslagna avgränsningen grundar sig på artikel 20.4. I momentet preciseras dessutom på motsvarande sätt som i 15 § 2 och 4 mom. i lagen om behandling av personuppgifter i polisens verksamhet att uppgifter som tagits för att göra en jämförelse får användas endast när jämförelsen görs och ska därefter omedelbart förstöras.

4 §. *Behandling av personuppgifter.* Genom interoperabilitetsförordningarna ändras inte de regler som gäller åtkomst till EU:s gemensamma informationssystem. Åtkomsträttigheterna till systemen baserar sig på motsvarande sätt som för närvarande på den rättsliga grunden för respektive informationssystem och på de nationella bestämmelser som kompletterar den. I *1 mom.* föreslås en informativ hänvisning till lagen om behandling av personuppgifter i polisens verksamhet, lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019) och lagen om behandling av personuppgifter inom Tullen. I dessa lagar ingår kompletterande nationell reglering om EU:s gemensamma informationssystem bland annat när det gäller rätten att få uppgifter för brottsbekämpande ändamål, utlämnande av personuppgifter, tillgodoseende av de registrerades rättigheter och personuppgiftsansvaret för systemen.

Det föreslagna *2 mom.* innehåller en informativ hänvisning till den allmänna lagstiftningen om behandling av personuppgifter. I enlighet med ingressen till interoperabilitetsförordningarna är den allmänna dataskyddsförordningen (EU) 2016/679 tillämplig på de nationella myndigheternas behandling av personuppgifter i interoperabilitetssyfte, förutom om behandlingen görs av medlemsstaternas utsedda myndigheter eller centrala kontaktpunkter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. Den allmänna dataskyddsförordningen kompletteras av dataskyddslagen (1050/2018) som nationell allmän lag. Den behandling av personuppgifter som avses i den föreslagna lagen sker för att fullgöra myndigheternas lagstadgade skyldigheter, varvid den behandling av personuppgifter som omfattas av tillämpningsområdet för den allmänna dataskyddsförordningen grundar sig på artikel 6.1 c i dataskyddsförordningen. Direktiv (EU) 2016/680, som genomförts nationellt genom lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018), är tillämpligt när behandlingen av personuppgifter utförs av de behöriga myndigheterna i interoperabilitetssyfte i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

5 §. *Ikraftträdande.* I lagen föreslås en sedvanlig ikraftträdandebestämmelse.

8 Ikraftträdande

Lagen föreslås träda i kraft den 1 september 2022.

Av interoperabilitetskomponenterna tas enligt kommissionens nuvarande tidsplan först i drift den gemensamma biometriska matchningstjänsten 2022 och därefter CIR i slutet av 2022. Dessutom pågår då beredningen av artiklarna 20 och 22 i interoperabilitetsförordningarna, vilka inverkar på det lagförslag som nu föreslås. Eftersom lagen ska träda i kraft vid ingången av september 2022, ska de myndigheter som deltar i det nationella genomförandet redan vara godkända när CIR tas i drift.

9 Verkställighet och uppföljning

Enligt artikel 74 i polisinteroperabilitetsförordningen och artikel 78 i gränsinteroperabilitetsförordningen skulle eu-LISA senast den 12 december 2019 och därefter var sjätte månad under interoperabilitetskomponenternas utvecklingsfas 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. Dessutom ska eu-LISA fyra år efter det att respektive interoperabilitetskomponent har tagits i drift och därefter vart fjärde år rapportera till

Europaparlamentet, rådet och kommissionen om interoperabilitetskomponenternas tekniska funktion, inbegripet ur säkerhetssynpunkt. Ett år efter varje rapport från eu-LISA ska kommissionen utarbeta en övergripande utvärdering av interoperabilitetskomponenterna, där tillämpningen av förordningarna bedöms ur olika synvinklar.

Varje år fram till dess att de rättsakter som genomför interoperabilitetskomponenterna har antagits ska kommissionen lägga fram en rapport för Europaparlamentet och rådet om läget i fråga om förberedelserna för ett fullständigt genomförande av förordningarna. Denna rapport ska även innehålla detaljerad information om de kostnader som uppkommit och information om eventuella risker som kan påverka de totala kostnaderna.

Två år efter idrifttagningen av MID ska kommissionen göra en granskning av hur MID påverkar rätten till icke-diskriminering.

Efter det att CIR har tagits i drift ska medlemsstaterna och Europol 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.

10 Förhållande till budgetpropositionen

Propositionen hänför sig till budgetpropositionen för 2022 och avses bli behandlad i samband med den. I budgetpropositionen för 2022 beräknas genomförandet av de ändringar som polis- och gränsinteroperabilitetsförordningarna förutsätter öka utgifterna med 6 426 000 euro.

11 Förhållande till grundlagen samt lagstiftningsordning

Polis- och gränsinteroperabilitetsförordningarna är EU-rättsakter som till alla delar är förpliktande och direkt tillämplig lagstiftning i samtliga medlemsstater. Enligt EU-domstolens etablerade rättspraxis har unionens lagstiftning företräde framom nationell rätt i enlighet med de förutsättningar som definierats i rättspraxis (GrUU 20/2017 rd, s. 6 och GrUU 51/2014 rd, s. 2/II). Enligt EU-domstolens etablerade rättspraxis är det inte tillåtet att lagstifta nationellt inom förordningens tillämpningsområde, om inte förordningen explicit förpliktar eller bemyndigar till nationell reglering eller andra beslut (mål 34/73, Variola, dom 10.10.1973, mål 50/76, Amsterdam Bulb, dom 2.2.1977, 33 punkten).

Den föreslagna regleringen grundar sig på internationella förpliktelser som är bindande för Finland. Grundlagsutskottet har konstaterat att ett sådant samband är en omständighet som stöder godtagbarheten av regleringen (exempelvis GrUU 38/2012 rd, s. 3).

Genom interoperabilitetsförordningarna inrättas en gemensam biometrisk matchningstjänst som skapar en matematisk modell utifrån de biometriska kännetecken som har förts in i informationssystemen på EU-nivå och lagrar modellen i den gemensamma databasen. Genom förordningarna inrättas också en gemensam databas för identitetsuppgifter och en detektor för multipla identiteter, vilka behöver den ovannämnda biometriska matchningstjänsten för att fungera.

De behöriga myndigheternas åtkomst till databasen för identitetsuppgifter för att identifiera en person omfattas i förordningarna av det nationella handlingsutrymmet. Grundlagsutskottet har i sitt utlåtande om interoperabilitetsförordningarna påpekat att det i den mån som EU-lagstiftningen kräver reglering på det nationella planet eller möjliggör sådan ska tas hänsyn till de krav som de grundläggande fri- och rättigheterna och de mänskliga rättigheterna ställer när det nationella handlingsutrymmet utnyttjas (GrUU 11/2018 rd, se även GrUU 25/2005 rd och GrUU 1/2018 rd).

Förordningarna och den nationella reglering som kompletterar dem innebär ingrepp i skyddet för privatlivet och personuppgifter. I sin bedömning av bestämmelser av det här slaget har grundlagsutskottet i allmänhet brukat anse att bestämmelserna måste granskas mot 10 § i grundlagen. Enligt 1 mom. i den paragrafen utfärdas närmare bestämmelser om skydd för personuppgifter genom lag. Grundlagsutskottets vedertagna praxis har varit att lagstiftarens handlingsutrymme begränsas både av denna bestämmelse och av att skyddet för personuppgifter delvis ingår i skyddet för privatlivet som tryggas i samma moment. Sammantaget är det fråga om att lagstiftaren ska trygga denna rättighet på ett sätt som kan anses godtagbart med hänsyn till de grundläggande fri- och rättigheterna som en helhet (se t.ex.GrUU 11/2018 rd, GrUU 13/2016 rd).

I sitt utlåtande om interoperabilitetsförordningarna ansåg grundlagsutskottet att inrättandet av en ram som reglerar interoperabiliteten för informationssystemen på EU-nivå i huvudsak kan anses vara positivt. Med tanke på grundlagen och de grundläggande fri- och rättigheter och mänskliga rättigheter som gäller skyddet för personuppgifter är det motiverat att utöka kompatibiliteten och interoperabiliteten hos olika informationssystem på EU-nivå, eftersom det genom kompatibilitet och interoperabilitet är möjligt att minska de risker som inkompatibiliteten mellan olika system medför för rättssäkerheten samt integritetsskyddet och informationssäkerheten (GrUU 11/2018 rd).

I förordningarna och i den nationella reglering som föreslås i propositionen är det fråga om bestämmelser som delvis gäller känsliga uppgifter. Grundlagsutskottet har lyft fram kravet på ändamålsbegränsning, framför allt i fråga om behandling av känsliga uppgifter. När det gäller till exempel omfattande register med biometriska kännetecken har det enligt grundlagsutskottet funnits orsak att förhålla sig negativt till att uppgifterna används för ändamål som ligger utanför det syfte som de egentligen samlats in och registrerats för (GrUU 14/2009 rd, s. 4/II). I sådana situationer har det på grund av ändamålsbegränsningen då endast kunnat göras exakta undantag som kan karakteriseras som obetydliga och bestämmelserna har inte fått leda till att någon annan verksamhet än den som är förknippad med det ursprungliga ändamålet blir det huvudsakliga eller ens ett viktigt ändamål (GrUU 11/2018 rd, se även t.ex. GrUU 14/2017 rd, s. 5–6).

Grundlagsutskottet har betonat att det ska finnas ett godtagbart samhälleligt intresse i en inskränkning av skyddet för privatlivet och inskränkningen ska stå i rätt proportion till det eftersträvade målet. Det betyder att inskränkningarna måste vara nödvändiga för att ett godtagbart syfte ska nås. En inskränkning av en grundläggande fri- eller rättighet är tillåten enbart om målet inte kan nås med medel som intervenerar mindre i de grundläggande fri- och rättigheterna. En inskränkning får inte vara mer genomgripande än vad som är motiverat med hänsyn till hur tungt vägande det bakomliggande intresset är i relation till det rättsobjekt som ska inskränkas (GrUB 25/1994 rd och t.ex. GrUU 56/2014 rd och GrUU 18/2013 rd).

Grundlagsutskottet har även betonat att skyddet för privatlivet och personuppgifter bör stå i proportion till andra grundläggande och mänskliga rättigheter samt till andra vägande samhälleliga intressen, såsom allmän säkerhet, som i extrema fall kan gå tillbaka på den personliga säkerheten som grundläggande rättighet (GrUU 5/1999 rd, s. 2/II). Lagstiftaren ska garantera skyddet för privatlivet och personuppgifter på ett sätt som är godtagbart med avseende på de samlade grundläggande fri- och rättigheterna. Grundlagsutskottet har ansett att skyddet för privatlivet och personuppgifter inte har företräde framför andra grundläggande fri- och rättigheter. Analysen går ut på att samordna och avväga två eller flera bestämmelser om de grundläggande fri- och rättigheterna (se t.ex. GrUU 14/2018 rd, s. 8, GrUU 26/2018 rd, s. 4, GrUU 54/2014 rd, s. 2/II och GrUU 10/2014 rd, s. 4/II).

I propositionen föreslås det att det nationella handlingsutrymmet i interoperabilitetsförordningarna ska utnyttjas så att bestämmelserna gör det möjligt för de behöriga myndigheterna att få åtkomst till EU:s gemensamma databas för identitetsuppgifter. De föreslagna bestämmelserna gäller biometriska uppgifter som betraktas som känsliga, och behandlingen av dessa uppgifter förutsätter exakta och noggrant avgränsade bestämmelser på grund av de risker som behandlingen medför. På de grunder som beskrivs specialmotiveringen föreslås det att de behöriga myndigheterna avgränsas till polisen, Gränsbevakningsväsendet och Tullen. Åtkomsten ska vara begränsad till endast sådana situationer där det är nödvändigt för att utföra de uppgifter som anges i bestämmelsen.

I propositionen föreslås det inga ändringar i den reglering som gäller förutsättningarna för behandling av biometriska uppgifter i nationella register och utlämnande av dem till EU:s gemensamma informationssystem. Genom interoperabilitetsförordningarna och den kompletterande nationella regleringen ändras inte heller de regler som gäller myndigheternas åtkomst till EU:s gemensamma informationssystem. Åtkomsträttigheterna för dessa system baserar sig på den rättsliga grunden för respektive informationssystem och gällande nationell lagstiftning. Den registrerades intressen tryggas av den registrerades rättigheter enligt gällande dataskyddslagstiftning.

Målet med interoperabilitetsförordningarna är att förbättra ändamålsenligheten och effektiviteten hos in- och utresekontrollerna vid de yttre gränserna, bidra till att förebygga och bekämpa olaglig invandring, bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, inbegripet bevarandet av allmän säkerhet och allmän ordning och tryggandet av säkerheten på medlemsstaternas territorier, förbättra genomförandet av den gemensamma viseringspolitiken, bistå vid prövningen av en ansökan om internationellt skydd, bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott samt att underlätta identifieringen av okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor vid en naturkatastrof, olycka eller ett terrordåd. Bestämmelserna om den behandling av personuppgifter som föreslås i propositionen har bedömts vara en nödvändig och proportionell åtgärd med beaktande av hur tungt vägande de syften som ligger bakom förslagen är i förhållande till den grundläggande fri- och rättighet som ska begränsas.

På de grunder som anges ovan kan lagförslaget behandlas i vanlig lagstiftningsordning.

Kläm

Eftersom Europaparlamentets och rådets förordning (EU) 2019/817 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 och Europaparlamentets och rådets förordning (EU) 2019/818 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 innehåller bestämmelser som föreslås bli kompletterade genom lag, föreläggs riksdagen följande lagförslag:

Lagförslag

Lag

om interoperabilitet mellan Europeiska unionens informationssystem

I enlighet med riksdagens beslut föreskrivs:

1 §

Tillämpningsområde

Genom denna lag utfärdas kompletterande bestämmelser om tillämpningen av Europaparlamentets och rådets förordning (EU) 2019/817 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, nedan *gränsinteroperabilitetsförordningen*, och om tillämpningen av Europaparlamentets och rådets förordning (EU) 2019/818 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, nedan *polisinteroperabilitetsförordningen*.

2 §

Behörig myndighet

De behöriga myndigheter som avses i artikel 20 i gränsinteroperabilitetsförordningen och i artikel 20 i polisinteroperabilitetsförordningen är polisen, Gränsbevakningsväsendet och Tullen.

3 §

Åtkomst till den gemensamma databasen för identitetsuppgifter

Polisen och Gränsbevakningsväsendet har rätt att använda den gemensamma databasen för identitetsuppgifter för att identifiera en person, om de förutsättningar som anges i artikel 20.1 i gränsinteroperabilitetsförordningen och i artikel 20.1 i polisinteroperabilitetsförordningen uppfylls och om det är nödvändigt för att de ska kunna utföra sina lagstadgade uppgifter att förhindra och bekämpa olaglig invandring och upprätthålla den allmänna ordningen och säkerheten.

Tullen och Gränsbevakningsväsendet har rätt att använda den gemensamma databasen för identitetsuppgifter för att identifiera en person, om de förutsättningar som anges i artikel 20.1 i gränsinteroperabilitetsförordningen och i artikel 20.1 i polisinteroperabilitetsförordningen uppfylls och om det är nödvändigt för att avslöja och förhindra olaglig införsel, utförsel eller transitering av sådana varor eller ämnen som är till fara för människor eller miljön.

En behörig myndighet ska utföra sökningarna i den gemensamma databasen för identitetsuppgifter med iakttagande av artikel 20.2 och 20.3 i gränsinteroperabilitetsförordningen och artikel 20.2 och 20.3 i polisinteroperabilitetsförordningen.

Utöver vad som föreskrivs i 1 mom. har polisen vid en naturkatastrof, olycka eller ett terrordåd rätt att med biometriska uppgifter utföra sökningar i den gemensamma databasen för identitetsuppgifter, om det är nödvändigt för att

1) identifiera sådana offer som inte kan identifiera sig,

2) identifiera oidentifierade mänskliga kvarlevor.

De sökningar som avses i 4 mom. får utföras endast med biometriska uppgifter om de personer som avses i det momentet. De uppgifter som tagits för att göra en jämförelse får användas endast när jämförelsen görs och ska därefter omedelbart förstöras.

4 §

Behandling av personuppgifter

Utöver vad som föreskrivs i gränsinteroperabilitetsförordningen och polisinteroperabilitetsförordningen och i denna lag finns det bestämmelser om behandling av personuppgifter i polisens, Gränsbevakningsväsendets och Tullens uppgifter i lagen om behandling av personuppgifter i polisens verksamhet (616/2019), lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019) och lagen om behandling av personuppgifter inom Tullen (650/2019).

Dessutom finns det bestämmelser om behandling av personuppgifter i Europaparlamentets och rådets förordning (EU) 2016/679 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), i dataskyddslagen (1050/2018) och i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018).

5 §

Ikraftträdande

Denna lag träder i kraft den 20 .

Helsingfors den 23 september 2021

Statsminister

Sanna Marin

Inrikesminister Maria Ohisalo