Anpassningar av svensk rätt till EU:s förordningar om interoperabilitet

Ds 2022:21

Regeringskansliet
Justitiedepartementet

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Omslag: Regeringskansliets standard
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2022

ISBN 978-91-525-0462-8 (tryck)
ISBN 978-91-525-0463-5 (pdf)
ISSN 0284-6012

Innehåll

Innehåll **1**

Förkortningar **5**

Sammanfattning **13**

1 Författningsförslag **15**

1.1 Förslag till lag om ändring i utlänningslagen (2005:716) 15

1.2 Förslag till lag om ändring i utlänningsdatalagen (2016:27) 18

1.3 Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete 22

1.4 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område 26

1.5 Förslag till lag om ändring i lagen (2022:700) om särskild kontroll av vissa utlänningar 29

1.6 Förslag till förordning om ändring i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten 31

1.7 Förslag till förordning om ändring i förordningen (2017:504) om internationellt polisiärt samarbete 34

2 Ärendet **39**

3 Interoperabilitet mellan EU-informationssystem **41**

3.1 Informationsutbyte som en del av Schengensamarbetet 41
3.2 EU:s förordningar om interoperabilitet..... 48
3.3 Regeringens uppdrag till berörda myndigheter 54

4 Utgångspunkter för promemorians bedömningar 57
4.1 IOF är direkt tillämpliga i Sverige..... 57
4.2 Grundläggande fri- och rättigheter 58
4.3 Hänvisningsteknik..... 60

5 Förordningarnas inledande bestämmelser..... 61

6 En europeisk sökportal 63

7 En gemensam biometrisk matchningstjänst 67

8 En gemensam databas för id-uppgifter..... 69
8.1 Bestämmelser om CIR:s tekniska utveckling och innehåll..... 69
8.2 Åtkomst till CIR för spårning av multipla identiteter och för brottsbekämpande syften 71
8.3 Registerföring av loggar 74

9 Åtkomst till CIR i identifieringssyfte 75
9.1 Förutsättningar för åtkomst till CIR enligt artikel 20 i IOF..... 75
9.1.1 Tillämpningen av artikel 20 i IOF förutsätter nationella lagstiftningsåtgärder 75
9.1.2 Sökningar får endast göras av en polismyndighet..... 77
9.2 Polismyndighetens hemställan 78
9.3 Sökningar enligt artikel 20 i IOF inom ramen för en brottsutredning..... 78

9.4 Sökningar enligt artikel 20 i IOF vid upprätthållande av allmän ordning och säkerhet 85

9.5 Användning av CIR på utlänningsrättens område 89
9.5.1 Inre utlänningskontroller 89
9.5.2 Verkställighet av beslut om avvisning och utvisning enligt utlänningslagen 98
9.5.3 Verkställighet av beslut om utvisning i kvalificerade säkerhetsärenden 104
9.5.4 In- och utresekontroller 109

9.6 Sökningar enligt artikel 20 i IOF vid naturkatastrofer, olyckor och terrordåd 112

10 Detektorn för multipla identiteter 121

11 Åtgärder till stöd för interoperabilitet 127

12 Dataskydd och personuppgiftsansvar 129

12.1 IOF:s förhållande till allmän dataskyddsreglering 129

12.2 Personuppgiftsansvar 132

12.3 Säkerhetsfrågor, egenkontroll och överföring av uppgifter till tredjeland 135

12.4 De registrerades rättigheter 137

12.5 Tillsyn 140

12.6 Efterföljande behandling av biometriska uppgifter som tagits upp vid verkställighet av ett beslut om avvisning eller utvisning enligt utlänningslagen 142

12.7 Efterföljande behandling av biometriska uppgifter som tagits upp vid en inre utlänningskontroll 147

12.8 Efterföljande behandling av biometriska uppgifter som tagits upp vid verkställighet av ett beslut om utvisning i ett kvalificerat säkerhetsärende 150

13 Sekretess 153

14 Sanktioner och skadestånd 161

15 IOF:s avslutande bestämmelser 167

15.1 Ansvarsområden 167

15.2 Ändringar av andra EU-rättsakter 168

15.3 Slutbestämmelser 171

16 Ikraftträdande- och övergångsbestämmelser 173

17 Konsekvenser 175

18 Författningskommentar 181

18.1 Förslaget till lag om ändring i utlänningslagen (2005:716) 181

18.2 Förslaget till lag om ändring i utlänningsdatalagen (2016:27) 184

18.3 Förslaget till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete 187

18.4 Förslaget till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område 191

18.5 Förslaget till lag om ändring i lagen (2022:700) om särskild kontroll av vissa utlänningar 193

Bilaga 1 Förordning (EU) 2019/817 195

Bilaga 2 Förordning (EU) 2019/818 253

Förkortningar

I denna promemoria används bl.a. följande förkortningar:

Barnkonventionen	Förenta nationernas konvention om barnets rättigheter
Dataskyddsdirektivet, EU:s dataskyddsdirektiv	Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF
Dataskyddsförordningen, EU:s dataskyddsförordning	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

Dataskyddslagen	lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
Ecris-TCN	EU:s system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer
EU:s förordning om Ecris-TCN	Europaparlamentets och rådets förordning (EU) 2019/816 av den 17 april 2019 om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN) för att komplettera det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726
Etias	EU:s system för reseuppgifter och resetillstånd
Etias-förordningen	Europaparlamentets och rådets förordning 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226
EU:s funktionsfördrag	Fördraget om Europeiska unionens funktionssätt
Eu-LISA	Europeiska byrån för den operativa förvaltningen av

	stora it-system inom området frihet, säkerhet och rättvisa
Eurodac	EU:s informationssystem med fingeravtryck på alla personer över 14 år som sökt asyl i ett EU-land
Eurodac-förordningen	Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodac-uppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning)
Europakonventionen	Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna

Europol	Europeiska unionens byrå för samarbete inom brottsbekämpning
Europolförordningen	Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF
EU:s rättighetsstadga	Europeiska unionens stadga om de grundläggande rättigheterna
Förordningen om ändring i gränskodexen	Europaparlamentets och rådets förordning (EU) 2017/2225 av den 30 november 2017 om ändring av förordning (EU) 2016/399 vad gäller användningen av in- och utresesystemet
Gränsförordningen	Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006
Gränskodexen, kodexen om Schengengränserna	Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en

	unionskodex om gränspassage för personer (kodex om Schengengränserna)
In- och utreseförordningen	Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) nr 1077/2011
In- och utresesystemet	EU:s in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser
IOF, EU:s förordningar om interoperabilitet	Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU)

	2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF, och Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816
Kommissionen	Europeiska kommissionen
OSL	offentlighets- och sekretesslagen (2009:400)
Polisens brottsdatalag	lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område
Polisförordningen	Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU
RF	Regeringsformen
SIS	Schengens informationssystem

SIS-förordningarna	samlingsnamn för polisförordningen, gränsförordningen och återvändandeförordningen
SIS II-förordningen	Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II)
UtlL	utlänningslagen (2005:716)
UtlF	utlänningsförordningen (2006:97)
VIS	informationssystemet för viseringar
Viseringskodexen	Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex)
VIS-förordningen	Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen)
VIS-rådsbeslutet	rådets beslut 2008/633/RIF om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott

Återvändandeförordningen	Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna

Sammanfattning

I maj 2019 antog EU två förordningar som innebär att vissa EU-gemensamma it-system ska kunna kommunicera med varandra, s.k. interoperabilitet. Det handlar om system som används på områdena gränser och visering, polissamarbete och straffrättsligt samarbete, samt asyl och migration. Genom förordningarna inrättas ett antal nya tekniska komponenter bl.a. en ny gemensam databas för identitetsuppgifter (CIR). Komponenterna är avsedda 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). Genom dessa åtgärder kommer det att bli lättare att fastställa en persons identitet och kontrollera om en uppgiven identitet är riktig.

De två EU-förordningarna gäller direkt som lag i Sverige. De är dock valfria för medlemsstaterna att tillämpa såvitt avser möjligheten för myndigheter att söka i CIR endast i syfte att identifiera en person. I denna promemoria föreslås vissa författningsändringar för att anpassa svensk rätt till förordningarna. Det föreslås att Sverige ska tillämpa förordningarna även i valfria delar. I förslagen fastställs därför förutsättningarna för att svenska myndigheter ska kunna söka i CIR i syfte att identifiera en person. Det föreslås vidare att en utlänning ska vara skyldig att lämna fingeravtryck och låta sig bli fotograferad för att sådana sökningar ska kunna genomföras. Förslagen innebär också att det tydliggörs hur regelverket förhåller sig till annan dataskyddsreglering.

Författningsändringarna föreslås träda i kraft den dag som EU:s förordningar om interoperabilitet ska börja tillämpas fullt ut. Eftersom detta datum ännu inte är fastställt föreslås lagändringarna träda i kraft den dag som regeringen bestämmer.

1 Författningsförslag

1.1 Förslag till lag om ändring i utlänningslagen (2005:716)

Härigenom föreskrivs i fråga om utlänningslagen (2005:716) att det ska införas tre nya paragrafer, 1 kap. 4 f §, 9 kap. 8 j och 13 a §§, och närmast före 1 kap. 4 f § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	Förordning (EU) 2019/817 och förordning (EU) 2019/818
	4 f § *Med förordning (EU) 2019/817 avses i denna lag Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF.*

Med förordning (EU) 2019/818 avses i denna lag Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816.

9 kap.

8 j §

En polisman eller en tjänsteman vid Kustbevakningen får vid en kontroll enligt 9 § genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och artikel 20.1–20.3 i förordning (EU) 2019/818. En utlänning är skyldig att låta en polisman eller en tjänsteman vid Kustbevakningen fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

När en sökning enligt första stycket har genomförts ska det fotografi och de fingeravtryck som har tagits för sökningen omedelbart förstöras om det framkommer att utlänningen har rätt att vistas i Sverige.

13 a §

En polisman får i ett ärende om verkställighet av ett beslut om

avvisning eller utvisning genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och artikel 20.1–20.3 i förordning (EU) 2019/818. En utlänning är skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

Denna lag träder i kraft den dag som regeringen bestämmer.

1.2 Förslag till lag om ändring i utlänningsdatalagen (2016:27)

Härigenom föreskrivs att 5 och 15 §§ utlänningsdatalagen (2016:27) ska ha följande lydelse.

Lydelse enligt SFS 2022:243	*Föreslagen lydelse*

5 §

Denna lag gäller inte när personuppgifter behandlas med stöd av

1. lagen (2006:444) om passagerarregister,

2. Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex),

3. Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning),

4. Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna,

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

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

7. lagen (2021:1187) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem och föreskrifter som har meddelats i anslutning till den lagen, *eller*

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

7. lagen (2021:1187) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem och föreskrifter som har meddelats i anslutning till den lagen,

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

9. Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av

Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF, eller

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

15 §

Migrationsverket får föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 *och* 8 h §§ utlänningslagen (2005:716).

Migrationsverket får föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8, 8 h *och 8 j* §§ utlänningslagen (2005:716).

Med begränsning av de ändamål som annars gäller enligt 11 och 13 §§ får uppgifter om fingeravtryck eller fotografier i registren användas endast

1. vid prövning av ansökningar om uppehållstillstånd där skäl som anges i 4 kap. 1–2 a §§ utlänningslagen åberopas,

2. i ärenden om avvisning och utvisning,

3. i testverksamhet,

4. om det behövs för att kontrollera identiteten av en person på ett fotografi som kommit in till Migrationsverket,

5. om det behövs för att Migrationsverket ska kunna kontrollera ett fingeravtryck mot fingeravtrycks- och signalementsregister som Polismyndigheten för enligt 5 kap. 11 § lagen (2018:1693) om

polisens behandling av personuppgifter inom brottsdatalagens område, eller

6. vid kontroll av utlänningar under vistelsen i Sverige.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om vilka uppgifter som får behandlas i registren över fingeravtryck och fotografier, och

2. föreskrifter om gallring.

Denna lag träder i kraft den dag som regeringen bestämmer.

1.3 Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

Härigenom föreskrivs i fråga om lagen (2017:496) om internationellt polisiärt samarbete

dels att 1 kap. 2 och 3 §§ ska ha följande lydelse,

dels att det ska införas ett nytt kapitel, 11 kap., av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §	
Lagen innehåller bestämmelser om operativt samarbete (2–5 kap.) och uppgiftsutbyte (6–*10* kap.).	Lagen innehåller bestämmelser om operativt samarbete (2–5 kap.) och uppgiftsutbyte (6–*11* kap.).
3 §[1]	
I lagen avses med	
– *Schengenkonventionen*: konventionen om tillämpning av Schengenavtalet av den 14 juni 1985,	
– *avtalet med Danmark*: avtalet av den 6 oktober 1999 mellan Konungariket Sveriges regering och Konungariket Danmarks regering om polisiärt samarbete i Öresundsregionen,	
– *Öresundsförbindelsen*: den fasta förbindelsen över Öresund som den definieras i artikel 2 i avtalet med Danmark,	
– *Prümrådsbeslutet*: rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet,	
– *Atlasrådsbeslutet*: rådets beslut 2008/617/RIF av den 23 juni 2008 om förbättrat samarbete i krissituationer mellan Europeiska unionens medlemsstaters särskilda insatsgrupper,	
– *avtalet med Norge*: avtalet av den 4 september 2018 mellan Sveriges regering och Norges regering om ömsesidigt bistånd mellan polisens särskilda insatsgrupper i krissituationer,	
– *referensuppgifter*: registeruppgifter som inte röjer identiteten på en person, antingen i form av en sifferbeteckning och ett	

[1] Senaste lydelse 2020:80.

fingeravtryck eller en sifferbeteckning och en dna-profil från den ickekodifierande delen av personens dna,

– *CBE-direktivet*: Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott, i den ursprungliga lydelsen,

– *VIS-rådsbeslutet*: rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott, *och*

– *avtalet med USA*: avtalet av den 16 december 2011 mellan Konungariket Sveriges regering och Amerikas förenta staters regering om ett förstärkt samarbete för att förebygga och bekämpa brottslighet.

– *VIS-rådsbeslutet*: rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott,

– *avtalet med USA*: avtalet av den 16 december 2011 mellan Konungariket Sveriges regering och Amerikas förenta staters regering om ett förstärkt samarbete för att förebygga och bekämpa brottslighet,

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

– förordning (EU) 2019/818: Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816.

11 kap. Uppgiftsutbyte enligt förordning (EU) 2019/817 och förordning (EU) 2019/818

Sökningar i EU:s gemensamma databas för identitetsuppgifter (CIR)

1 § Den myndighet som regeringen bestämmer får genomföra sökningar enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och artikel 20.1–20.3 i förordning (EU) 2019/818 i syfte att utreda brott. Sådana sökningar får genomföras med fotografi eller fingeravtryck som har tagits med stöd av 28 kap. 14 § rättegångsbalken.

2 § Den myndighet som regeringen bestämmer får genomföra sökningar enligt artikel 20.4 i förordning (EU) 2019/817 och artikel 20.4 i förordning (EU) 2019/818 om det behövs för att fastställa en avlidens identitet i samband med en naturkatastrof, olycka eller terrordåd. Sådana sökningar får genomföras med fotografi eller fingeravtryck som har tagits vid en rättsmedicinsk undersökning.

Föreskrifter

3 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare

föreskrifter om uppgiftsutbyte enligt förordning (EU) 2019/817 och förordning (EU) 2019/818.

Denna lag träder i kraft den dag som regeringen bestämmer.

1.4 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

Härigenom föreskrivs att 1 kap. 2 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område ska ha följande lydelse.

Lydelse enligt SFS 2022:244	*Föreslagen lydelse*

1 kap.

2 §

Denna lag gäller inte vid behandling av personuppgifter enligt

1. vapenlagen (1996:67),
2. lagen (1998:620) om belastningsregister,
3. lagen (1998:621) om misstankeregister,
4. lagen (2006:444) om passagerarregister,
5. lagen (2014:400) om Polismyndighetens elimineringsdatabas,
6. Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna,
7. Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006,
8. Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU,
9. lagen (2021:1187) med kompletterande bestämmelser

9. lagen (2021:1187) med kompletterande bestämmelser

till EU:s förordningar om Schengens informationssystem och föreskrifter som har meddelats i anslutning till den lagen, *eller*

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

till EU:s förordningar om Schengens informationssystem och föreskrifter som har meddelats i anslutning till den lagen,

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

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

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

Denna lag träder i kraft den dag som regeringen bestämmer.

1.5 Förslag till lag om ändring i lagen (2022:700) om särskild kontroll av vissa utlänningar

Härigenom föreskrivs att det i lagen (2022:700) om särskild kontroll av vissa utlänningar ska införas en ny paragraf, 5 kap. 31 §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 kap.
	31 §
	En polisman får i ett ärende om verkställighet av ett beslut om utvisning genomföra en sökning enligt artikel 20.1–20.3 i Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF och artikel 20.1–20.3 i Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt

samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816. En utlänning är skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

Denna lag träder i kraft den dag som regeringen bestämmer.

1.6 Förslag till förordning om ändring i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten

Härigenom föreskrivs att 4 § förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §[1]

Myndigheten är nationell tillsynsmyndighet enligt

– artikel 44 i Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) och artikel 60 i rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II),

– artikel 24 i rådets beslut 2009/917/RIF av den 30 november 2009 om användning av informationsteknik för tulländamål (TIS-rådsbeslutet),

– artikel 37 i rådets förordning (EG) 515/97 av den 13 mars 1997 om ömsesidigt bistånd mellan medlemsstaternas administrativa myndigheter och om samarbete mellan dessa och kommissionen för att säkerställa en korrekt tillämpning av tull- och jordbrukslag-stiftningen (förordning 515/97),

– artikel 42 i Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF,

– artikel 30.5 i rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet),

[1] Senaste lydelse 2019:1267.

– artikel 41 i Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS- förordningen),

– artikel 7.1 och 7.2 i Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott (CBE-direktivet), i den ursprungliga lydelsen,

– artikel 8.5 i rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott (VIS-rådsbeslutet),

– artikel 30 och 33.2 i Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning), *och*

– artikel 30 och 33.2 i Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning),

– artikel 42 i Europaparlamentets och rådets förordning (EU) nr 2018/1727 av den 14 november 2018 om Europeiska unionens byrå för straffrättsligt samarbete (Eurojust) och om ersättning och upphävande av rådets beslut 2002/187/RIF.	– artikel 42 i Europaparlamentets och rådets förordning (EU) nr 2018/1727 av den 14 november 2018 om Europeiska unionens byrå för straffrättsligt samarbete (Eurojust) och om ersättning och upphävande av rådets beslut 2002/187/RIF,
	– artikel 51 i Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF, och
	– artikel 51 i Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816.

Denna förordning träder i kraft den xx.

1.7 Förslag till förordning om ändring i förordningen (2017:504) om internationellt polisiärt samarbete

Härigenom föreskrivs i fråga om förordningen (2017:504) om internationellt polisiärt samarbete

dels att 1 kap. 1 och 2 §§ ska ha följande lydelse,

dels att det ska införas ett nytt kapitel, 10 kap., av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
1 §	
I denna förordning finns bestämmelser om polisiärt samarbete mellan Sverige och andra stater.	
Bestämmelserna i 2–8 kap. ansluter till lagen (2017:496) om internationellt polisiärt samarbete. Bestämmelserna i 9 kap. kompletterar Eurodacförordningen.	Bestämmelserna i 2–8 *och 10* kap. ansluter till lagen (2017:496) om internationellt polisiärt samarbete. Bestämmelserna i 9 kap. kompletterar Eurodacförordningen.
2 §[1]	
I förordningen avses med	
– *Schengenkonventionen*: konventionen om tillämpning av Schengenavtalet av den 14 juni 1985,	
– *avtalet med Danmark*: avtalet av den 6 oktober 1999 mellan Konungariket Sveriges regering och Konungariket Danmarks regering om polisiärt samarbete i Öresundsregionen,	
– *Prümrådsbeslutet*: rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet,	
– *Atlasrådsbeslutet*: rådets beslut 2008/617/RIF av den 23 juni 2008 om förbättrat samarbete i krissituationer mellan Europeiska unionens medlemsstaters särskilda insatsgrupper,	

[1] Senaste lydelse 2020:82.

– *avtalet med Norge*: avtalet av den 4 september 2018 mellan Sveriges regering och Norges regering om ömsesidigt bistånd mellan polisens särskilda insatsgrupper i krissituationer,

– *CBE-direktivet*: Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott, i den ursprungliga lydelsen,

– *VIS-rådsbeslutet*: rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott,

– *avtalet med USA*: avtalet av den 16 december 2011 mellan Konungariket Sveriges regering och Amerikas förenta staters regering om ett förstärkt samarbete för att förebygga och bekämpa brottslighet, *och*

– *Eurodacförordningen*: Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av

– *avtalet med USA*: avtalet av den 16 december 2011 mellan Konungariket Sveriges regering och Amerikas förenta staters regering om ett förstärkt samarbete för att förebygga och bekämpa brottslighet,

– *Eurodacförordningen*: Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av

förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, i den ursprungliga lydelsen.

förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, i den ursprungliga lydelsen,

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

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

10 kap. Uppgiftsutbyte enligt förordning (EU) 2019/817 och förordning (EU) 2019/818

Sökningar i EU:s gemensamma databas för identitetsuppgifter (CIR)

1§ Polismyndigheten, Säkerhetspolisen och Tullverket får genomföra sökningar enligt 11 kap. 1 § lagen (2017:496) om internationellt polisiärt samarbete.

2 § Polismyndigheten, Säkerhetspolisen och Rättsmedicinalverket får genomföra sökningar enligt 11 kap. 2 § lagen om internationellt polisiärt samarbete.

Ytterligare föreskrifter

3 § Polismyndigheten får meddela ytterligare föreskrifter om verkställigheten av bestämmelserna om uppgiftsutbyte enligt förordning (EU) 2019/817 och förordning (EU) 2019/818.

Denna förordning träder i kraft den xx.

2 Ärendet

Den 20 maj 2019 antog Europaparlamentet och rådet två förordningar om inrättande av en ram för interoperabilitet mellan EU-informationssystem dels på området gränser och viseringar (förordning [EU] 2019/817), dels på området polissamarbete och straffrättsligt samarbete, asyl och migration (förordning [EU] 2019/818). Förordningarna är i stor utsträckning likalydande och benämns därför gemensamt IOF i denna promemoria. Om endast en av förordningarna åsyftas kommer hänvisning att göras till den förordningen. Förordningarna i de ursprungliga lydelserna finns i *bilaga 1* och *2*. Sedan antagandet har det gjorts vissa ändringar i förordningarna (se förordning [EU] 2021/1150, 2021/1151 och 2021/1152). Promemorian utgår från IOF:s lydelser efter dessa ändringar.

Förordningarna trädde i kraft den 11 juni 2019 och vissa bestämmelser tillämpas från det datumet. Övriga delar ska börja tillämpas i samband med att de olika komponenterna tas i drift, vilket beräknas ske före utgången av juni 2024. I förhållande till Eurodac kommer dock IOF tillämpas från och med den dag då den omarbetade Eurodac-förordningen (förordning [EU] 603/2013) blir tillämplig.

Enligt artikel 20 i IOF får medlemsstaternas polismyndigheter i vissa situationer göra sökningar i EU:s nya databas för identitetsuppgifter (CIR) i identifieringssyfte. För att sådana sökningar ska vara tillåtna krävs att medlemsstaterna har antagit nationella lagstiftningsåtgärder. Polismyndigheten har därför lämnat in en hemställan till regeringen den 8 december 2020 (Ju2020/04544) om att det ska ske en författningsöversyn för att Sverige ska utnyttja förordningarnas möjlighet i denna del.

I promemorian föreslås nödvändiga anpassningar av svensk rätt till IOF. Vidare lämnas nödvändiga författningsförslag för att möjliggöra sökningar enligt artikel 20 i IOF.

3 Interoperabilitet mellan EU-informationssystem

3.1 Informationsutbyte som en del av Schengensamarbetet

De flesta av EU:s medlemsländer, och ett antal andra europeiska länder, deltar i dag i det s.k. Schengensamarbetet. Schengensamarbetet syftar i huvudsak till att uppnå fri rörlighet inom Schengenområdet genom att människor ska kunna resa utan att behöva visa pass när de passerar gränserna mellan de länder som anslutit sig.

Sverige är sedan mars 2001 anslutet fullt ut till Schengensamarbetet.

För att uppnå målet att människor ska kunna resa fritt inom Schengenområdet har Schengenländerna enats om gemensamma regler i ett stort antal frågor. Vissa av dessa regler tar direkt sikte på att säkerställa den fria rörligheten av personer inom Schengenområdet, t.ex. genom att avskaffa personkontroller vid de inre gränserna. Andra regler handlar i stället om att motverka de negativa bieffekter som en fri rörlighet av personer kan föra med sig, i form av t.ex. gränsöverskridande brottslighet och olaglig invandring. Som exempel på sådana regler kan nämnas enhetliga regler om visum och inresekontroller mot länder utanför Schengenområdet. Här ingår emellertid också åtgärder som syftar till att stärka Schengenländernas operativa samarbete i frågor om bl.a. brottsbekämpning och immigrationskontroll. Informationsutbyte genom gemensamma it-lösningar utgör en del av det samarbetet.

EU:s storskaliga it-system på området frihet, säkerhet och rättvisa

I syfte att effektivisera informationsutbytet mellan Schengenstaterna har EU utvecklat eller håller på att utveckla ett antal gemensamma it-system på områdena gränskontroll, migrationshantering och brottsbekämpning. Några av dessa system används av Schengenländerna sedan länge, vissa är under vidareutveckling medan andra är nya och under uppbyggnad. Systemens huvudsakliga användningsområden varierar men gemensamt är att de har till syfte att stärka medlemsstaternas gränskontroll, brottsbekämpning och immigrationskontroll. Nedan följer en beskrivning av de system som berörs av IOF. Systemen kommer i denna promemoria att gemensamt benämnas ”underliggande system”. De EU-rättsakter som reglerar de underliggande systemen kommer gemensamt benämnas ”underliggande rättsakter”.

Schengens informationssystem (SIS): SIS är ett informationssystem som medlemsstaterna använder för att utbyta information med varandra inom ramen för polissamarbete och straffrättsligt samarbete samt migrationskontroll. I systemet kan medlemsstaterna exempelvis registrera uppgifter om eftersökta personer och lämna information om personer som ska nekas inresa i Schengen. Sedan en tid tillbaka kan medlemsstaterna även registrera fingeravtryck i systemet. SIS består dels av ett centralt datasystem, dels av nationella datasystem i de deltagande medlemsstaterna. Medlemsstaterna använder sitt nationella system för sökning mot centrala SIS eller mot den nationella kopian. Polismyndigheten ansvarar för den svenska nationella delen av SIS. Polismyndigheten har även fått uppgiften att vara s.k. Sirenekontor, vilket bl.a. innebär att myndigheten är kontaktpunkt för Sverige mot andra medlemsstater för utbyte av ytterligare information om registreringar i SIS. Det centrala systemet administreras av Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA).

Schengens informationssystem regleras idag på EU-nivå av ett rådsbeslut (rådets beslut 2007/533/RIF) och två EU-förordningar (förordning [EU] 2006/1986 och 2006/1987), det s.k. SIS II-regelverket. Rådsbeslutet har genomförts i svensk rätt genom lagen (2000:344) om Schengens informationssystem och förordningen

(2000:836) om Schengens informationssystem. EU har dock antagit tre nya direkt tillämpliga förordningar (förordning [EU] 2019/1860, 2019/1861 och 2019/1862) som kommer att börja tillämpas stegvis och ersätta SIS II-regelverket fullt ut vid ett datum som kommissionen ska fastställa. Systemet kommer då att få en rad nya funktioner. För närvarande pågår arbete med att anpassa svensk rätt till det nya EU-rättsliga regelverket om SIS (se Ds 2019:27, prop. 2020/21:6 och prop. 2020/21:222). Riksdagen har bl.a. antagit en ny lag (2021:1187) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem som ska ersätta den nu gällande lagen (2000:344) om Schengens informationssystem. Den nya lagen ska träda i kraft den dag som regeringen bestämmer.

European Asylum Dactoscopy (Eurodac): Eurodac är ett informationssystem med fingeravtryck på alla personer över 14 år som sökt asyl i ett EU-land. Syftet med Eurodac är att jämföra fingeravtryck för att se om asylsökande tidigare har sökt asyl i något annat EU-land och därför ska hänvisas dit, enligt principen om första asylland. Sverige anslöt sig till Eurodac i januari 2003. Sedan 2013 är det möjligt för brottsbekämpande myndigheter och för Europol att få tillgång till uppgifter i Eurodac för brottsbekämpande ändamål. Uppgifterna lagras i en central databas som hanteras av eu-LISA. De nationella myndigheter som har till uppgift att hantera asylansökningar har tillgång till databasen.

Eurodac regleras idag av en direkt tillämplig EU-förordning (förordning [EU] nr 603/2013). Förordningen har kompletterats med nationella bestämmelser. För närvarande pågår arbete inom EU med att ta fram en omarbetad Eurodacförordning.

Visa Information System (VIS): VIS är ett informationssystem för utbyte av uppgifter om visum mellan EU:s medlemsländer. VIS innehåller personuppgifter som samlats in och registrerats i samband med visumansökningsprocessen. Utöver de personuppgifter som anges i visumansökan registreras även exempelvis sökandens fingeravtryck och ansiktsfoto. Uppgifter lagras i en central databas som hanteras av eu-LISA. Olika aktörer som utfärdar visum och personal vid gränskontroller har åtkomst till uppgifterna. Under vissa förutsättningar kan även andra myndigheter få åtkomst till uppgifter i VIS för brottsbekämpande ändamål.

VIS har inrättats genom rådets beslut 2004/512/EG av den 8 juni 2004 om inrättande av Informationssystemet för viseringar (VIS). Det EU-rättsliga regelverket om VIS finns även i den s.k. VIS-förordningen (förordning [EU] 767/2008) och det s.k. VIS-rådsbeslutet (rådets beslut 2008/633/RIF). Den senare rättsakten har genomförts i svensk rätt genom bestämmelser i lagen (2017:496) respektive förordningen (2017:504) om internationellt polisiärt samarbete.

VIS-förordningen har ändrats vid ett antal tillfällen och den 7 juli 2021 antogs en ny förordning i syfte att reformera VIS (förordning [EU] 2021/1134). Den nya förordningen innebär bl.a. att de bakgrundskontroller som genomförs innan beslut fattas om beviljande av visering stärks. För närvarande pågår ett arbete med att se över behovet av anpassningar av svensk rätt till den nya förordningen.

In- och utresesystemet: För närvarande pågår uppbyggnaden av ett nytt europeiskt in- och utresesystem. Det är ett system för elektronisk registrering av uppgifter om tredjelandsmedborgares in- och utresa och uppgifter om nekad inresa för dem som passerar de yttre gränserna för kortare vistelser. Genom in- och utresesystemet avskaffas medlemsstaternas stämpling av tredjelandsmedborgares resehandlingar vid in- och utresa och ersätts med en elektronisk registrering. Systemet registrerar tidpunkt och plats för in- och utresa, beräknar längden på den tillåtna vistelsen och varnar myndigheterna när tiden för den tillåtna vistelsen har löpt ut. Systemet ska bestå av bl.a. ett centralt system, som ska inhysas vid eu-LISA:s tekniska enheter, ett enhetligt nationellt gränssnitt i varje medlemsstat och säkra kommunikationskanaler som gör det möjligt att på ett säkert sätt ansluta in- och utresesystemets centrala system till de nationella gränsinfrastrukturerna och till VIS. Målen med systemet är bl.a. att effektivisera in- och utresekontrollerna, ge bättre möjligheter att identifiera personer som inte uppfyller villkoren för vistelse inom medlemsstaternas territorium och bidra till brottsbekämpningen.

In- och utresesystemet regleras i två direkt tillämpliga EU-förordningar (förordning [EU] 2017/2225 och 2017/2226) som ska börja tillämpas fullt ut den dag som kommissionen ska fastställa. Vid samma tillfälle tas systemet i bruk. För närvarande pågår ett arbete

med att anpassa svensk rätt till EU:s regelverk om in- och utresesystemet (se Ds 2021:9 och prop. 2021/22:81).

European Travel Information and Authorisation System (Etias): Inom EU utvecklas för närvarandet ett nytt system för registrering av tredjelandsmedborgare som är undantagna från kravet på visering för kortare vistelse för att passera de yttre gränserna. Genom Etias ska en tredjelandsmedborgare som är undantagen från kravet på visering ansöka och få ett beslut om resetillstånd, innan han eller hon avreser till Schengenområdet. Tredjelandsmedborgaren ska själv lämna information via en online-service, vilket ska möjliggöra en bedömning av om personens vistelse på medlemsstaternas territorium innebär en säkerhetsrisk, en risk för olaglig invandring eller en hög epidemirisk. För den här kategorin resenärer kommer ett giltigt resetillstånd att vara ett krav för inresa till och vistelse på medlemsstaternas territorium. Förutom att bidra till högre säkerhet, förebygga och förhindra olaglig invandring och skydda folkhälsan, ska systemet bidra till att underlätta in- och utresekontroller, stödja målen för Schengens informationssystem och bidra till en korrekt identifiering av personer. Systemet ska dessutom bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott.

Etias regleras dels av den s.k. Etias-förordningen (förordning [EU] 2018/1240), dels av förordningar med följdändringar i andra rättsakter med anledning av Etias-förordningen (förordning [EU] 2021/1150, 2021/1151 och 2021/1152). Förordningarna ska börja tillämpas fullt ut och systemet tas i bruk den dag kommissionen bestämmer. För närvarande pågår arbete med att anpassa svensk rätt till Etias-förordningen (se Ds 2021:19).

European Criminal Records Information System - Third Country Nationals (Ecris-TCN): Sedan 2012 finns inom EU ett decentraliserat europeiskt informationssystem för utbyte av uppgifter ur kriminalregister (Ecris). Sverige anslöt sig till systemet under 2013. Polismyndigheten är för svenskt vidkommande centralmyndighet för samarbetet. Ecris-systemet utesluter i princip ett utbyte av uppgifter om dömda tredjelandsmedborgare, dvs. personer som inte är unionsmedborgare. I syfte att möjliggöra ett effektivt utbyte mellan medlemsstaterna även av kriminalregister-

uppgifter om tredjelandsmedborgare pågår för närvarande ett arbete inom EU med att inrätta ett centraliserat system för identifiering av medlemsstater som innehar fällande domar mot tredjelandsmedborgare och statslösa personer, Ecris-TCN. Ecris-TCN är inte avsett att ersätta det befintliga Ecris, utan kommer att fungera som ett komplement. Ecris-TCN kommer inte att innehålla några uppgifter om domar, utan endast sådana uppgifter som krävs för att identifiera de medlemsstater som innehar kriminalregisteruppgifter om tredjelandsmedborgare. Begäran om kriminalregisteruppgifter från de stater som har sådana får sedan ske via Ecris.

Ecris-TCN regleras EU-rättsligt bl.a. av en direkt tillämplig förordning (förordning [EU] 2019/816) och ett direktiv (direktiv [EU] 2019/884). Systemet ska tas i bruk i samband med att förordningen ska börja tillämpas fullt ut vilket kommissionen ska fastställa genom beslut. För närvarande pågår ett arbete med att anpassa svensk rätt till EU:s regelverk om Ecris-TCN (se SOU 2021:20 och prop. 2021/22:172). Riksdagen har bl.a. beslutat om en ny lag (2022:733) med kompletterande bestämmelser till EU:s förordning om Ecris-TCN. Lagen ska träda i kraft den dag som regeringen bestämmer.

Behovet av nya tekniska åtgärder

Efter terrordåden i Paris i november 2015 och Bryssel i mars 2016 publicerade kommissionen i april 2016 meddelandet Starkare och smartare informationssystem för gränser och säkerhet, KOM(2016) 205. Meddelandet beskrev bristerna hos de EU-gemensamma informationssystemen på områdena gränskontroll, migrationshantering och brottsbekämpning och behandlade övergripande hur systemen bättre skulle kunna stödja skyddet av de yttre gränserna och den inre säkerheten. Ökad enhetlighet i informationshanteringen och ett effektivare utnyttjande av redan existerande information angavs som nyckelåtgärder. Man ville också underlätta för berörda aktörer att få tillgång till existerande information när den behövs genom utveckling av multifrågefunktioner och genom att åtgärda bristande överblick över informationen som beror på olika organisatoriska, rättsliga och politiska förutsättningar. Genom att få systemen att kommunicera med varandra, s.k. interoperabilitet,

menade kommissionen att informationen kan utnyttjas bättre, att kvaliteten hos informationen kan öka och att kostnaderna kan minska. Med begreppet interoperabilitet avses alltså informationssystemens kapacitet att utbyta uppgifter och dela information med varandra. Vid rådets möte för rättsliga och inrikes frågor, även kallat RIF-rådet, den 8 juni 2017 antogs rådsslutsatser om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabilitet mellan EU:s informationssystem. Mot den bakgrunden presenterade kommissionen den 12 december 2017 ett förslag till två nya förordningar om interoperabilitet mellan EU-informationssystemen SIS, Eurodac, VIS, in- och utresesystemet, Etias och Ecris-TCN. Sedan kommissionens förslag behandlats av rådet och Europaparlamentet antogs i maj 2019 två nya EU-förordningar, hädanefter gemensamt kallade IOF eller EU:s förordningar om interoperabilitet, nämligen

- Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF, samt
- Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816.

IOF trädde i kraft den 11 juni 2019. Vissa bestämmelser i förordningarna ska tillämpas från det datumet medan andra ska börja tillämpas vid datum som ska fastställas av kommissionen.

3.2 EU:s förordningar om interoperabilitet

Allmänt om förordningarnas syfte och tillämpningsområde

Huvudsyftet med IOF är att komma till rätta med strukturella brister i befintliga EU-informationssystem som hindrar de nationella myndigheternas arbete och att säkerställa att gränskontrolltjänstemän, tullmyndigheter, poliser och rättsliga myndigheter har tillgång till den information de behöver när de utför sina uppgifter inom områdena säkerhet, gränser och migrationshantering (skäl 1 i IOF). Avsikten med en kapacitet för underliggande system att utbyta uppgifter och dela information med varandra (interoperabilitet) är att de ska komplettera varandra bl.a. för att underlätta korrekt identifiering av personer samt bidra till att bekämpa identitetsbedrägerier (skäl 10 i IOF).

Förordningarna är till stora delar likalydande och ska läsas som en helhet. Orsaken till att interoperabiliteten mellan underliggande system har reglerats i två separata EU-förordningar är att EU:s medlemsstaters deltagande i Schengensamarbetet varierar beroende på vilket område det handlar om. Därför antogs en förordning som gäller gränser och viseringar (hädanefter benämnd förordning [EU] 2019/817) samt en förordning som gäller polissamarbete och straffrättsligt samarbete, asyl och migration (hädanefter benämnd förordning [EU] 2019/818). Förordningarna reglerar de underliggande system som hör till respektive förordnings rättsområde. Det innebär att förordning (EU) 2019/817 ska tillämpas på in- och utresesystemet, VIS, Etias och SIS medan förordning (EU) 2019/818 ska tillämpas på Eurodac, Ecris-TCN och SIS. Att SIS regleras i båda författningarna beror på att det systemet faller in under flera rättsområden (straffrättsligt och polisiärt samarbete, gränskontroll och immigrationskontroll).

IOF har efter antagandet justerats genom ändringar till följd av den rättsliga regleringen av underliggande system. Vidare har de kompletterats genom rättsakter som antagits av kommissionen utifrån dess bemyndigande i förordningarna. Denna promemoria utgår från IOF:s ändrade lydelser. Nedan går IOF:s bestämmelser igenom översiktligt.

Kapitel I – IOF:s inledande bestämmelser

I förordningarnas första kapitel finns allmänna bestämmelser om syfte (artikel 1), mål (artikel 2) och tillämpningsområde (artikel 3). Vidare finns en bestämmelse med definitioner av begrepp som används i förordningarna (artikel 4) samt en bestämmelse om icke-diskriminering och grundläggande rättigheter (artikel 5). I artikel 1 fastslås ramarna för interoperabiliteten, dvs. underliggande systems kapacitet att utbyta uppgifter och dela information med varandra. Denna ska bl.a. utgöras av följande nya tekniska komponenter (hädanefter gemensamt kallade IO-komponenterna)

- en europeisk sökportal (ESP),
- en gemensam biometrisk matchningstjänst (sBMS),
- en gemensam databas för id-uppgifter (CIR) och
- en detektor för multipla identiteter (MID).

IOF innehåller även bestämmelser om krav på uppgifters kvalitet, ett universellt meddelandeformat (UMF) och en central databas för rapporter och statistik (CRRS). Det fastslås vidare att genom IOF anpassas också förfarandena och villkoren för att de utsedda myndigheterna och Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) ska få åtkomst till underliggande system i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. Vidare fastställs ramar för verifiering av personers identitet och för identifiering av personer.

IOF har flera ändamål, nämligen att förbättra ändamålsenligheten och effektiviteten hos in- och utresekontrollerna vid de yttre gränserna (artikel 2.1 a), bidra till att förebygga och bekämpa olaglig invandring (artikel 2.1 b), bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, bl.a. att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier (artikel 2.1 c), förbättra genomförandet av den gemensamma viseringspolitiken (artikel 2.1 d), bistå vid prövningen av en ansökan om internationellt skydd (artikel 2.1 e), bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott (artikel 2.1 f) samt

underlätta identifieringen av okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor vid en naturkatastrof, olycka eller ett terrordåd (artikel 2.1 g).

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 5.

Kapitel II - Den europeiska sökportalen

I förordningarnas andra kapitel (artiklarna 6–11) regleras den nya europeiska sökportalen (ESP). Av artikel 6 i IOF framgår att ESP ska inrättas för att underlätta bl.a. medlemsstaternas myndigheters möjligheter att få snabb, kontinuerlig, effektiv, systematisk och kontrollerad åtkomst till underliggande system, Europoluppgifter och Interpols databaser som krävs för att de ska kunna utföra sina uppgifter, i enlighet med sina åtkomsträttigheter och målen för och syftena med underliggande system. Genom att göra det möjligt att utföra parallella sökningar i alla relevanta EU-informationssystem, Europoluppgifter och Interpols databaser är det tänkt att ESP ska fungera som en gemensam kontaktpunkt eller meddelandehanterare för att söka i de olika centrala systemen och smidigt hämta den nödvändiga informationen, med full respekt för de underliggande systemens åtkomstkontroll och dataskyddskrav (skäl 13).

Användningen av ESP ska förbehållas de myndigheter i medlemsstaterna och de unionsbyråer som har åtkomst till åtminstone ett av underliggande system i enlighet med de rättsliga instrument som reglerar dessa, till CIR och MID i enlighet med IOF, till Europoluppgifter i enlighet med förordning (EU) 2016/794 (Europolförordningen) eller till Interpols databaser i enlighet med unionsrätten eller nationell rätt avseende sådan åtkomst. Dessa myndigheter i medlemsstaterna och unionsbyråer får använda ESP och de uppgifter som tillhandahålls genom den endast för de mål och syften som fastställs i de rättsliga instrument som reglerar underliggande system, i Europolförordningen och IOF (artikel 7.1).

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 6.

Kapitel III - En gemensam biometrisk matchningstjänst

Kapitel III (artiklarna 12–16) reglerar inrättandet och användningen av en gemensam biometrisk matchningstjänst för lagring av biometriska mallar som erhållits från biometriska uppgifter lagrade i den nya gemensamma databasen för id-uppgifter (CIR) och SIS. Den gemensamma biometriska matchningstjänsten (sBMS) ska vara ett tekniskt verktyg för att stärka och underlätta arbetet för de relevanta EU-informationssystemen och de andra IO-komponenterna. Huvudsyftet med den gemensamma biometriska matchningstjänsten är att underlätta identifiering av en person som har registrerats i flera databaser, genom att använda en enda teknisk komponent för att matcha den personens biometriska uppgifter mellan olika system, i stället för flera komponenter (skäl 18).

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 7.

Kapitel IV - En gemensam databas för identitetsuppgifter

Kapitel IV (artiklarna 17–24) hanterar en ny gemensam databas för id-uppgifter (CIR). I CIR skapas en personakt för varje person som är registrerad i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN. Databasen kommer att innehålla vissa närmare angivna personuppgifter (artikel 18), bl.a. för att underlätta och bistå vid en korrekt identifiering av personer som är registrerade i de underliggande systemen. Om uppgifter läggs till, ändras eller raderas i något av de underliggande EU-informationssystemen ska uppgifterna automatiskt läggas till, ändras eller raderas i personakten i CIR (artikel 19). Varje uppsättning av uppgifter i personakten kommer att innehålla en hänvisning till den konkreta uppgiftspost i det underliggande system som uppgifterna tillhör (artikel 18.2).

De myndigheter som har åtkomst till CIR ska handla i enlighet med sina åtkomsträttigheter enligt de EU-rättsliga och nationella bestämmelser som reglerar underliggande system samt i enlighet med sina åtkomsträttigheter enligt artiklarna 20–22 i IOF (artikel 18.3). I de sistnämnda artiklarna finns särskilda regler för åtkomst till CIR i identifieringssyfte (artikel 20), för spårning av multipla identiteter (artikel 21) och för sökningar i CIR i syfte att förebygga,

förhindra, upptäcka eller utreda terroristbrott eller andra grova brott (artikel 22).

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 8 och 9.

Kapitel V - En detektor för multipla identiteter

I kapitel V (artiklarna 25–36) regleras detektorn för multipla identiteter (MID). MID:s huvudsakliga syfte är att underlätta identitetskontroller och bekämpa identitetsbedrägerier. Genom MID spåras multipla identiteter i samband med att registreringar görs i underliggande system (artikel 27). Resultatet av spårningen visas genom länkar mellan uppgifter i de underliggande systemen som får olika färger (grön, gul, vit eller röd) utifrån kriterier som fastställs i IOF (artiklarna 30–33). Spårningen sker inledningsvis automatiskt men resultatet kommer i vissa fall att kräva manuell verifiering (artikel 29). Enligt artikel 4.5 i IOF avses med verifiering förfarandet att jämföra en uppsättning uppgifter med en annan för att fastställa om en påstådd identitet är riktig (s.k. one-to-one-check). Beroende på utfallet av spårningen kommer det skapas och lagras akter med identitetsbekräftelse i MID, som bl.a. ska innehålla uppgifter om länkar (artiklarna 34 och 35).

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 10.

Kap VI - Åtgärder till stöd för interoperabilitet

I kapitel VI finns bestämmelser om tekniska åtgärder som ska vidtas för att stödja kapaciteten för underliggande system och databasen CIR att utbyta uppgifter och dela information med varandra. Bland annat fastslås att eu-LISA ska inrätta automatiska mekanismer och förfaranden för kontroll av kvaliteten på de uppgifter som lagras i systemen (artikel 37). Vidare ska det inrättas en standard för ett gemensamt meddelandeformat (UMF). Formatet är tänkt att definiera vokabulär och standarder för vissa innehållselement i det gränsöverskridande informationsutbytet (se skäl 50 och artikel 38). I artikel 39 fastslås vidare att det ska inrättas en central databas för rapporter och statistik (CRRS) som bl.a. ska tillhandahålla

systemöverskridande statistiska uppgifter och analysrapporter. Uppgifterna i CRRS ska inte möjliggöra identifiering av enskilda personer.

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 11.

Kapitel VII - Dataskydd

Särskilda bestämmelser om dataskydd finns i kapitel VII. Det gäller bl.a. regler om personuppgiftsansvar och personuppgiftsbiträde (artiklarna 40 och 41), särskilda åtgärder för att garantera att uppgifter i systemen behandlas på ett säkert sätt (artikel 42), motåtgärder som ska vidtas vid s.k. säkerhetstillbud (artikel 43), skyldigheten för medlemsstaterna och unionsbyråerna att se till att varje myndighet som har åtkomsträtt till IO-komponenterna vidtar nödvändiga åtgärder för att övervaka efterlevnaden av kraven i IOF (artikel 44) samt om sanktioner och skadestånd (artiklarna 45 och 46). Vidare finns särskilda regler om enskildas rätt till information (artikel 47) och om rätten till åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter i MID (artikel 48). Enligt artikel 49 ska en webbportal inrättas för att underlätta utövandet av rätten till åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter. Artikel 50 reglerar överföring av personuppgifter till tredjeländer, internationella organisationer och privata parter. I artiklarna 51–53 finns regler om tillsyn.

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 12 och 14.

Kapitel VIII – Ansvarsområden

I kapitel VIII (artiklarna 54–57) finns bestämmelser som reglerar unionsbyråernas och medlemsstaternas respektive ansvar. Eu-LSA ska ha det huvudsakliga ansvaret för IO-komponenternas utveckling och för de anpassningar som krävs för att upprätta en kapacitet mellan dessa och de underliggande systemen att utbyta uppgifter och dela information med varandra (artikel 54–55). I artikel 56 fastslås medlemsstaternas ansvar. Enligt den artikeln ansvarar

medlemsstaterna bl.a. för integration av de befintliga nationella systemen och infrastrukturerna med ESP, CIR och MID. Vidare ansvarar medlemsstaterna för förvaltningen av och föreskrifter om åtkomst för vederbörligen bemyndigad personal till ESP, CIR och MID. Medlemsstaterna ansvarar även för efterlevnaden av reglerna för varje underliggande system beträffande personuppgifternas säkerhet och integritet.

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 15.

Kapitel IX och X – Ändringar av andra unionsinstrument och slutbestämmelser

I kapitel IX finns bestämmelser om ändringar i andra EU-rättsakter till följd av möjliggörandet för underliggande systemen att utbyta uppgifter och dela information med varandra. IOF reglerar ändringar av de rättsakter som faller inom respektive förordnings rättsområde.

IOF:s slutbestämmelser finns i kapitel X. Här regleras bl.a. förordningarnas ikraftträdande och tillämplighet samt driftstart för IO-komponenterna. Vidare finns särskilda övergångsbestämmelser för användning av ESP, åtkomst till den gemensamma databasen för identitetsuppgifter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott och spårning av multipla identiteter. I kapitlet finns även särskilda regler om rapportering och statistik, övervakning och utvärdering, kostnader och underrättelser. Vidare regleras hur kommissionen ska utöva sina delegerade befogenheter och anta genomförandeakter.

Överväganden om behovet av anpassningar av nationell rätt med anledning av dessa bestämmelser finns i avsnitt 15.

3.3 Regeringens uppdrag till berörda myndigheter

Den 29 maj 2019 beslutade regeringen att uppdra åt Polismyndigheten att leda samordningen av berörda myndigheters genomförande av IOF (Ju2019/02044). Regeringen uppdrog samtidigt åt Migrationsverket, Säkerhetspolisen, Tullverket och Kustbevakningen att delta i arbetet och lämna underlag till

Polismyndigheten för den löpande nationella uppföljningen och rapporteringen.

Uppdraget innebär att Polismyndigheten ska leda och planera arbetet i en gemensam samordningsgrupp för genomförandet av IOF på myndighetsnivå och löpande, genom återkommande samordnad rapportering, hålla Regeringskansliet underrättat om arbetet med genomförandet på myndighetsnivå. I den myndighetsgemensamma samordningsgruppen ska ingå företrädare för Polismyndigheten, Migrationsverket, Säkerhetspolisen, Tullverket och Kustbevakningen. Varje myndighet ansvarar för genomförandet och samordningen inom sitt sakområde.

Senast den 29 mars 2024 ska Polismyndigheten lämna en slutrapport över uppdraget till Justitiedepartementet.

4 Utgångspunkter för promemorians bedömningar

4.1 IOF är direkt tillämpliga i Sverige

Enligt artikel 288 i EU:s funktionsfördrag är en EU-förordning till alla delar bindande och direkt tillämplig i alla medlemsstater. Det betyder att en förordning ska tillämpas direkt av alla nationella myndigheter på samma sätt som lagar och andra nationella föreskrifter. Medlemsstaterna är skyldiga att se till att det inte finns nationella bestämmelser som står i strid med en EU-förordning. En fråga som är reglerad i en EU-förordning får som huvudregel inte regleras nationellt. Bestämmelserna får dock återges om det är nödvändigt för att den nationella regleringen ska bli begriplig eller sammanhållen. En EU-förordning kan även leda till behov av kompletterande bestämmelser i nationell rätt.

IOF gäller alltså som lag i Sverige och ska som utgångspunkt tillämpas direkt av svenska myndigheter utan att bestämmelserna återges i nationella föreskrifter. Det behöver dock göras en översyn av nationell rätt för att bedöma om det finns ett behov av kompletterande bestämmelser på nationell nivå för att tillämpningen av IOF ska fungera på ett ändamålsenligt sätt och för att Sverige ska uppfylla sina åtaganden enligt förordningarna.

I promemorian lämnas de förslag till författningsändringar som bedöms nödvändiga för att Sverige ska kunna uppfylla sina åtaganden enligt IOF. Som nämns i avsnitt 9 får medlemsstaternas polismyndigheter enligt artikel 20 i IOF i vissa situationer göra sökningar i EU:s nya databas för id-uppgifter (CIR) i identifieringssyfte. För att sådana sökningar ska vara tillåtna krävs dock att medlemsstaterna har antagit nationella lagstiftningsåtgärder. Bestämmelserna i artikel 20 är således, till skillnad från övriga bestämmelser i IOF, fakultativt utformade. I promemorian

övervägs vilka lagstiftningsåtgärder som behövs för att möjliggöra sökningar enligt artikel 20 i IOF.

4.2 Grundläggande fri- och rättigheter

Regleringen i IOF och de förslag till kompletterande nationella bestämmelser som lämnas i avsnitten 9.3, 9.5 och 9.6 innebär att personuppgifter kommer att behandlas, även barns personuppgifter. Vidare kommer fotografier och fingeravtryck att tas i fler fall – eller i vart fall för fler syften – än i dag. Därmed aktualiseras frågor om enskildas grundläggande fri- och rättigheter.

Var och en har ett skydd mot påtvingat kroppsligt ingrepp från det allmännas sida (2 kap. 6 § första stycket regeringsformen). Fotografering räknas inte som ett kroppsligt ingrepp (prop. 2017/18:35 s. 12). Det gör däremot fingeravtryckstagning. Var och en har alltså ett skydd mot att lämna fingeravtryck. Av 2 kap. 6 § andra stycket följer att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet enligt 2 kap. 6 § regeringsformen är inte absolut. Det får begränsas i lag, bl.a. enligt 2 kap. 25 § regeringsformen som reglerar skyddet för utländska medborgares fri- och rättigheter.

Ett skydd mot integritetsintrång av olika slag följer även av den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Enligt artikel 8.1 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv. Det inbegriper en rätt till skydd mot att bli fotograferad. Likaså får det antas att fingeravtryckstagning omfattas av skyddet (prop. 2014/15:32 s. 26). Inskränkningar i skyddet godtas bara om de har stöd i lag och är nödvändiga med hänsyn till vissa uppräknade ändamål, däribland statens säkerhet, den allmänna säkerheten eller förebyggande av oordning eller brott (artikel 8.2). Europakonventionen gäller som lag i Sverige (se lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). Enligt 2 kap. 19 § regeringsformen gäller

vidare att lagar eller andra föreskrifter inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Bestämmelser om grundläggande fri- och rättigheter finns även i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga). Var och en har enligt stadgan rätt till respekt för sitt privat- och familjeliv och till skydd av de personuppgifter som rör honom eller henne (artiklarna 7.1 och 8.1). Enligt artikel 52.1 i stadgan måste varje begränsning i utövandet av de fri- och rättigheter som erkänns i stadgan vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter.

I sammanhanget bör även Förenta nationernas konvention om barnets rättigheter (barnkonventionen) nämnas. Barnkonventionen inkorporerades i svensk rätt den 1 januari 2020 och gäller därmed som lag i Sverige. Av konventionen följer bl.a. att barnets bästa är det som i första hand ska beaktas vid alla åtgärder som rör barn och att barn ska skyddas från godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv (artiklarna 3 och 16).

EU-regelverket och de regler som föreslås i promemorian om den enskildes lämnande och myndigheternas användning av fingeravtryck och andra personuppgifter är omgärdade av andra detaljerade bestämmelser som syftar till att ge skydd för den enskilde, exempelvis i dataskyddsförordningen och dataskyddsdirektivet med kompletterande regelverk. I artikel 5 i IOF anges vidare att behandling av personuppgifter enligt de förordningarna inte får leda till diskriminering av personer på någon grund, såsom kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till en nationell minoritet, förmögenhet, börd, funktionsnedsättning, ålder eller sexuell läggning. Den ska vidare ske med fullständig respekt för mänsklig värdighet och integritet samt grundläggande rättigheter, inbegripet rätten till respekt för privatlivet och skydd av personuppgifter. Särskild hänsyn ska tas till barn, äldre, personer med funktionsnedsättning och personer i behov av internationellt skydd. Barnets bästa ska komma i främsta rummet.

EU-lagstiftaren har gjort bedömningen att bestämmelserna i IOF är förenliga med de grundläggande rättigheter och de principer som erkänns i synnerhet i EU:s rättighetsstadga. Det förutsätts även att IOF ska tillämpas i enlighet med dessa rättigheter och principer (se skäl 40 i IOF samt skäl 83 i förordning [EU] 2019/817 och skäl 79 i förordning [EU] 2019/818).

4.3 Hänvisningsteknik

Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse medan en dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen.

De underliggande systemen regleras av EU-rättsakter som kan antas bli föremål för översyn och ändras och kompletteras löpande. Som anges i avsnitt 3.1 är t.ex. Eurodacförordningen föremål för omarbetning. Det kan därmed antas att även IOF kommer bli föremål för översyn. Därutöver är den svenska reglering som föreslås, där hänvisningar till EU-rättsakter görs, huvudsakligen beroende av hur EU:s reglering av de aktuella systemen kommer att se ut. För att minska risken för framtida oklarheter eller brister i lagstiftningen och för att säkerställa att ändringar i EU-regleringen får omedelbart genomslag finns det anledning att utforma hänvisningarna så att de avser EU-bestämmelsen i den vid varje tidpunkt gällande lydelsen. Det är därför lämpligt att de hänvisningar som görs till IOF i kompletterande nationella bestämmelser är dynamiska. Hänvisningarna kommer alltså att omfatta eventuella ändringar i förordningarna.

5 Förordningarnas inledande bestämmelser

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om syfte, mål, tillämpningsområde och definitioner kräver inte några författningsändringar. Inte heller bestämmelserna om icke-diskriminering och grundläggande rättigheter kräver några författningsändringar.

Skälen för bedömningen: IOF:s första kapitel, artiklarna 1–5, innehåller bestämmelser om syfte, mål och tillämpningsområde. I kapitlen finns även bestämmelser om definitioner och om icke-diskriminering och grundläggande rättigheter. När det gäller syftet framgår bl.a. att det genom förordningarna skapas en ram för att EU-informationssystemen in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN ska kunna utbyta uppgifter och dela information med varandra. Denna ram ska omfatta ett antal IO-komponenter, nämligen ESP, en gemensam biometrisk matchningstjänst, CIR och MID (artikel 1). Förordningarnas mål är bl.a. att förbättra effektiviteten hos in- och utresekontrollerna vid de yttre gränserna, att bidra till att förebygga och bekämpa olaglig invandring, att bistå vid prövningen av en ansökan om internationellt skydd och att bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott (artikel 2).

Förordning (EU) 2019/817 ska enligt artikel 3 tillämpas på in- och utresesystemet, VIS, Etias och SIS. Den ska även tillämpas på personer vars personuppgifter får behandlas i dessa EU-informationssystem och vilkas uppgifter samlas in för vissa ändamål som fastställs i rättsakter som reglerar dessa system. Förordning (EU) 2019/818 ska enligt artikel 3 tillämpas på Eurodac, SIS och Ecris-TCN samt på Europoluppgifter i en utsträckning som gör det

möjligt att söka i dem samtidigt som i dessa EU-informationssystem. Den ska även tillämpas på personer vars personuppgifter får behandlas i de EU-informationssystem och Europoluppgifter som förordningen är tillämplig på.

I artikel 4 finns definitioner av vissa begrepp som används i förordningarna. Artikel 5 reglerar icke-diskriminering och grundläggande rättigheter vid behandling av personuppgifter enligt förordningarna.

Bestämmelserna om syfte, mål, tillämpningsområde och definitioner är direkt tillämpliga och kräver inte några författningsändringar. Detsamma gäller bestämmelserna om icke-diskriminering och grundläggande rättigheter.

6 En europeisk sökportal

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om den europeiska sökportalen kräver inte några författningsändringar.

Skälen för bedömningen

Den europeiska sökportalen

Av artikel 6 i IOF framgår att en europeisk sökportal ska inrättas, ESP. Sökportalen ska bl.a. underlätta för medlemsstaternas myndigheter att få snabb, kontinuerlig, effektiv, systematisk och kontrollerad åtkomst till de underliggande informationssystemen, Europoluppgifter och Interpols databaser. Genom sökportalen ska medlemsstaternas myndigheter och behöriga EU-organ kunna göra nödvändiga sökningar för att utföra sina uppgifter, i enlighet med sina åtkomsträttigheter och målen för och syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. En nationell uppkoppling till respektive underliggande system ska dock behållas som en teknisk reserv.

För att det ska vara möjligt att använda ESP ska eu-LISA i samarbete med medlemsstaterna skapa en profil för varje kategori av ESP-användare (artikel 8.1 i IOF). Varje profil ska, i enlighet med unionsrätten och nationell rätt, inbegripa information bl.a. om vilka system och vilka specifika uppgifter som ska kunna vara föremål för sökningar samt de system som ska tillhandahålla användaren ett svar.

I artikel 9.1 i IOF anges att användarna av ESP ska inleda en sökning genom att mata in alfanumeriska eller biometriska uppgifter i ESP. När en sökning har inletts ska ESP, i enlighet med användarprofilen, söka i underliggande system med uppgifter som

användaren matat in. ESP får dock inte tillhandahålla någon information om uppgifter i systemen som användaren saknar åtkomst till enligt tillämplig unionsrätt och nationell rätt (artikel 9.4).

Behörigheten att söka i ESP följer av regleringen av respektive system

Av artikel 56.1 d i IOF framgår att varje medlemsstat ansvarar för förvaltning av och föreskrifter för åtkomst till vederbörligen bemyndigad personal vid de behöriga nationella myndigheterna till ESP, CIR och MID i enlighet med respektive förordning och upprättande och regelbunden uppdatering av en förteckning över denna personal och deras profiler.

Enligt artikel 7.1 i IOF ska användningen av ESP förbehållas de myndigheter i medlemsstaterna och de unionsbyråer som har åtkomst till åtminstone ett av de underliggande systemen. Åtkomst till underliggande system ges dock i enlighet med de rättsakter som reglerar respektive system. Därutöver ges tillgång till CIR och MID i enlighet med IOF, Europoluppgifter i enlighet med Europolförordningen och Interpols databaser i enlighet med unionsrätten eller nationell rätt avseende sådan åtkomst.

Inrättandet av sökportalen påverkar inte myndigheters eller unionsorgans behörighet till uppgifter i de underliggande systemen. Enligt artikel 9.4 i IOF får ESP inte tillhandahålla någon information om uppgifter i underliggande system, Europoluppgifter och Interpols databaser som användaren saknar åtkomst till enligt tillämplig unionsrätt och nationell rätt. Sökningar genom ESP får alltså endast göras utifrån den behörighet till underliggande system som användaren har. Denna behörighet följer av regleringen för respektive system. Det ankommer på respektive myndighet att i enlighet med artikel 56.1 d i IOF föra en förteckning över personal med behörighet till ESP. Eftersom detta följer direkt av förordningarna behövs det inte några kompletterande nationella bestämmelser i lag eller förordning i denna del.

Den tekniska utvecklingen av ESP kräver inte några nationella författningsändringar

ESP ska bestå av en central infrastruktur, inbegripet en sökportal, och en säker kommunikationskanal mellan sökportalen, medlemsstaterna och de unionsbyråer som har rätt att använda den. Vidare ska det finnas en säker kommunikationsinfrastruktur mellan ESP och in- och utresesystemet, VIS, Etias, Eurodac, centrala SIS, Ecris-TCN, Europoluppgifter och Interpols databaser samt mellan ESP och de centrala infrastrukturerna för CIR och MID.

Enligt artikel 54 i IOF ansvarar eu-LISA för IO-komponenternas utveckling och de anpassningar som krävs för att de underliggande systemen, ESP, sBMS, CIR, MID och CRRS ska kunna utbyta uppgifter och dela information med varandra.

Varje medlemsstat ansvarar för anslutning av sökportalens kommunikationsinfrastruktur och integration av de befintliga nationella systemen och ESP:s infrastrukturer (artikel 56.1 a och b i IOF). Som nämns i avsnitt 3.3 har regeringen i beslut den 29 maj 2019 gett berörda svenska myndigheter (Polismyndigheten, Migrationsverket, Säkerhetspolisen, Tullverket och Kustbevakningen) i uppdrag att samordna det nationella genomförandet av IOF.

Mot den bakgrunden behövs det inte några nationella författningsåtgärder för den tekniska utvecklingen av ESP.

Kravet på registerföring av loggar följer av förordningarna

Av artikel 10.1 i IOF framgår att, utan att det påverkar tillämpningen av loggningsbestämmelserna i de underliggande rättsakterna, eu-LISA ska föra loggar över all uppgiftsbehandling i ESP. Dessa loggar ska omfatta följande:

- Den medlemsstat eller unionsbyrå som inlett sökningen och den ESP-profil som används.
- Datum och tidpunkt för sökningen.
- De EU-informationssystem och de av Interpols databaser som varit föremål för sökning.

Varje medlemsstat ska föra loggar över sökningar som utförs av dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda ESP (artikel 10.2).

Bestämmelserna i artikel 10 i IOF är direkt tillämpliga och kräver inte några nationella författningsändringar.

7 En gemensam biometrisk matchningstjänst

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om en gemensam biometrisk matchningstjänst kräver inte några författningsändringar.

Skälen för bedömningen

En gemensam biometrisk matchningstjänst

I kapitel III i IOF, artiklarna 12–16, finns bestämmelser om en gemensam biometrisk matchningstjänst, sBMS. Av artikel 12 i IOF följer att det ska inrättas en gemensam biometrisk matchningstjänst som ska lagra biometriska mallar som den ska få från biometriska uppgifter som finns lagrade i CIR och SIS. Detta för att möjliggöra sökningar med biometriska uppgifter i flera EU-informationssystem för att stödja CIR och MID och målen för in- och utresesystemet, VIS, Eurodac, SIS och Ecris-TCN. Tjänsten ska bestå av en central infrastruktur och en säker kommunikationsinfrastruktur. Den ska utvecklas av eu-LISA, som också ska säkerställa den tekniska förvaltningen. Huvudsyftet med tjänsten är att underlätta identifiering av en person som har registrerats i flera databaser, genom att använda en enda teknisk komponent för att matcha den personens biometriska uppgifter mellan olika system, i stället för flera komponenter (skäl 18). Matchningstjänsten ska fungera som ett stöd till CIR och MID och användarna kommer inte att göra några sökningar direkt i tjänsten. Biometriska uppgifter definieras i förordningarna som fingeravtrycksuppgifter eller ansiktsbilder, eller båda (artikel 4.11 i IOF).

Enligt artikel 13.1 i IOF ska matchningstjänsten lagra biometriska mallar som den ska få från de biometriska uppgifter som räknas upp i artikeln. Uppräkningen omfattar bestämmelser om biometriska uppgifter i vissa underliggande rättsakter. Förordning (EU) 2019/817 hänvisar till bestämmelser i in- och utreseförordningen, VIS-förordningen, gränsförordningen och återvändandeförordningen, medan förordning (EU) 2019/818 hänvisar till bestämmelser i polisförordningen och EU:s förordning om Ecris-TCN. Artikel 13 innehåller även tekniska bestämmelser om lagringen av biometriska mallar i matchningstjänsten (artikel 13.1 andra stycket och 13.2) och kvalitetskrav i samband med lagringen (artikel 13.3 och 13.4).

Artikel 14 i IOF, som reglerar sökningar i sBMS, anger bl.a. att CIR och SIS ska använda de biometriska mallar som lagrats sBMS för att söka på biometriska uppgifter som lagrats i CIR och SIS. Enligt artikel 15 gäller att de uppgifter som avses i artikel 13.1 och 13.2 endast ska lagras i matchningstjänsten under den tid som motsvarande biometriska uppgifter lagras i CIR eller SIS och att uppgifterna automatiskt ska raderas i tjänsten.

Artiklarna 12–15 i IOF är direkt tillämpliga och kräver inte några författningsändringar.

Kravet på registerföring av loggar följer av förordningarna

Av artikel 16.1 i IOF framgår att, utan att det påverkar tillämpningen av loggningsbestämmelserna i de underliggande rättsakterna, ska eu-LISA föra loggar över all uppgiftsbehandling i sBMS. Av bestämmelsen framgår även vad loggarna ska omfatta.

Varje medlemsstat ska föra loggar över sökningar som utförs av dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda sBMS (artikel 16.2).

Bestämmelserna i artikel 16 är direkt tillämpliga och kräver inte några nationella författningsåtgärder.

8 En gemensam databas för id-uppgifter

8.1 Bestämmelser om CIR:s tekniska utveckling och innehåll

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om den tekniska utvecklingen av den gemensamma databasen för id-uppgifter, om lagring samt om tillägg, ändring och radering av uppgifter i databasen kräver inte några författningsändringar.

Skälen för bedömningen: Enligt artikel 17 i IOF ska det inrättas en gemensam databas för identitetsuppgifter, CIR, varigenom det skapas en personakt för varje person som är registrerad i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN. Detta för att underlätta och bistå vid en korrekt identifiering av personer som är registrerade i dessa EU-informationssystem, 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. Eu-LISA ska utveckla CIR och säkerställa den tekniska förvaltningen (artikel 17).

I artikel 18.3 fastslås att de myndigheter som har åtkomst till CIR ska handla i enlighet med sina åtkomsträttigheter enligt de rättsliga instrument som reglerar EU-informationssystemen och enligt nationell rätt och i enlighet med sina åtkomsträttigheter enligt IOF för de syften som avses i artiklarna 20, 21 och 22. Syftet med CIR är alltså inte att ge medlemsstaternas myndigheter en utökad behörighet till uppgifter i de underliggande systemen, utöver vad

som följer av artiklarna 20–22. Komponenten utgör en nödvändig teknisk åtgärd för att möjliggöra sökningar för identifiering enligt artikel 20 och för brottsbekämpande myndigheters sökningar enligt artikel 22 i IOF. Enligt artikel 20 i IOF får medlemsstaternas polismyndigheter i vissa situationer göra sökningar i CIR i identifieringssyfte. För att sådana sökningar ska vara tillåtna krävs enligt artikel 20 att medlemsstaterna har antagit nationella lagstiftningsåtgärder (se avsnitt 9). Vidare är CIR nödvändig för inrättandet av MID som alltså ska kunna använda uppgifterna i CIR för spårningen av multipla identiteter (se artikel 21 i IOF och avsnitt 10).

Enligt artikel 18.1 ska CIR lagra de uppgifter som räknas upp i artikeln, logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör. Uppräkningen omfattar bestämmelser i vissa underliggande rättsakter om uppgifter som ska registreras i respektive underliggande system. Förordning (EU) 2019/817 hänvisar till bestämmelser i in- och utreseförordningen, VIS-förordningen och Etias-förordningen, medan förordning (EU) 2019/818 hänvisar till bestämmelser i EU:s förordning om Ecris-TCN. CIR ska alltså lagra uppgifter från in- och utresesystemet, VIS, Etias och Ecris-TCN. Bland de uppgiftstyper som ska lagras finns bl.a. namn, medborgarskap, födelsedatum, kön, resehandlingsuppgifter, ansiktsbilder och fingeravtryck.

Av artikel 19.1 i de båda förordningarna följer att om uppgifter läggs till, ändras eller raderas i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN ska de uppgifter som avses i artikel 18 och som lagras i personakten i CIR automatiskt läggas till, ändras eller raderas. Uppgifterna ska raderas automatiskt från CIR i enlighet med bestämmelserna om lagring av uppgifter i aktuella underliggande rättsakter. Personakten ska lagras i CIR endast så länge de motsvarande uppgifterna lagras i minst ett av de EU-informationssystem vars uppgifter finns i CIR. Skapandet av en länk ska inte påverka lagringsperioden för varje post av de länkade uppgifterna (artikel 23).

Bestämmelserna i artiklarna 17–19 och 23 är direkt tillämpliga och kräver inte några författningsändringar.

8.2 Åtkomst till CIR för spårning av multipla identiteter och för brottsbekämpande syften

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om åtkomst till den gemensamma databasen för id-uppgifter för spårning av multipla identiteter och om sökningar i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott kräver inte några författningsändringar.

Skälen för bedömningen

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

Genom IOF införs en detektor för multipla identiteter (MID). Som framgår i avsnitt 10 är MID:s huvudsakliga syfte att underlätta identitetskontroller och bekämpa identitetsbedrägerier. Genom MID spåras multipla identiteter i samband med att registreringar görs i underliggande system (artikel 27). Resultatet av spårningen visas genom länkar mellan uppgifter i de underliggande systemen som får olika färger (grön, gul, vit eller röd) utifrån kriterier som fastställs i förordningarna (artiklarna 30–33). Spårningen sker inledningsvis automatiskt men resultatet kommer i vissa fall att kräva manuell verifiering (artikel 29).

I artikel 21.1 i IOF anges att om en sökning i CIR resulterar i en gul länk ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter i enlighet med artikel 29 enbart i verifieringssyfte ha åtkomst till de uppgifter som lagrats i CIR och som är kopplade genom länken. Av artikel 29.1 i IOF framgår att ansvaret för den manuella verifieringen ligger på den myndighet som skapat eller uppdaterat de uppgifter som resulterat i att en länk har uppstått. Enligt artikel 29.2 ska, i vissa uppräknade fall, medlemsstaternas s.k. Sirene-kontor alltid vara verifierande myndighet. Vilken myndighet som ska verifiera en gul länk följer därmed direkt av IOF och behöver inte utses i nationell författning (se även avsnitt 10).

Bestämmelsen i artikel 21.1 i IOF om åtkomst till CIR för de verifierande myndigheterna säkerställer att myndigheterna har de uppgifter som krävs för att bedöma en gul länk. Den är direkt tillämplig i medlemsstaterna och kräver inte några nationella författningsåtgärder.

I artikel 21.2 i IOF anges att om en sökning i CIR ger upphov till en röd länk, ska de myndigheter som avses i artikel 26.2 enbart i syfte att bekämpa identitetsbedrägerier ha åtkomst till uppgifter som lagrats i CIR och som är kopplade genom en röd länk. Artikel 26.2 reglerar åtkomst till röda länkar som lagrats i MID. Enligt den bestämmelsen ska myndigheter som har åtkomst till minst ett av de EU-informationssystem som ingår i CIR eller till SIS ha åtkomst till samtliga röda länkar samt uppgift om i vilka EU-informationssystem de länkade uppgifterna finns. Åtkomsten till röda länkar i MID och de länkade uppgifterna i CIR beror således på om en myndighet har åtkomst till minst ett av de underliggande systemen. Detta regleras i sin tur i regelverket för respektive system, antingen i en EU-rättsakt eller i en kompletterande nationell bestämmelse. Eftersom det följer av befintligt regelverk vilka myndigheter som ska ha åtkomst till uppgifter i CIR kopplade till röda länkar behöver detta inte närmare specificeras i nationell författning.

Sökningar i CIR i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott

Artikel 22 i IOF reglerar möjligheten för brottsbekämpande myndigheter att söka i vissa uppgifter i CIR i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. Det gäller uppgifter som lagras i in- och utresesystemet, Etias, VIS och Eurodac. Enligt artikelns första punkt får medlemsstaternas utsedda myndigheter söka i CIR för att få information om huruvida det finns uppgifter om en viss person i underliggande system. Med begreppet ”utsedd myndighet” avses de nationella myndigheter som medlemsstaterna har gett behörighet att begära åtkomst till uppgifter i underliggande system för brottsbekämpande ändamål (jfr artikel 4.20 i IOF). För svenskt vidkommande har t.ex. Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket och Kustbevakningen getts behörighet att begära åtkomst till uppgifter i VIS och Eurodac för sådana ändamål. Såvitt

avser in- och utresesystemet och Etias, vilka är under uppbyggnad, finns förslag på vilka myndigheter som ska kunna begära åtkomst till uppgifter i de systemen för brottsbekämpande ändamål (se Ds 2021:9 och Ds 2021:19).

För att en sökning enligt artikel 22 i IOF ska vara tillåten måste det i ett specifikt fall finnas rimliga skäl att anta att en sökning i EU-informationssystem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. Om en sökning i CIR visar att det finns uppgifter om personen i underliggande system ska CIR tillhandahålla de utsedda myndigheterna ett svar i form av en hänvisning som anger vilka av dessa EU-informationssystem som innehåller motsvarande uppgifter. Svaret får användas endast i syfte att lämna in en begäran om full åtkomst enligt de villkor och förfaranden som fastställs i den rättsliga regleringen för respektive system.

Brottsbekämpande myndigheter har idag möjlighet att begära åtkomst till uppgifter i befintliga underliggande system i enlighet med det regelverk som gäller för respektive system. Sådana processer kan dock ta tid eftersom en begäran om åtkomst oftast behöver ske via en central åtkomstpunkt som bedömer om kriterierna för åtkomst är uppfyllda. Därefter görs sökningarna i det eller de aktuella systemen och uppgifterna vidareförmedlas till den begärande myndigheten. Artikel 22 i IOF är tänkt att förenkla för brottsbekämpande myndigheter att snabbt kunna få svar på om det finns uppgifter om en person i något av de underliggande systemen. Om förutsättningarna i artikel 22 i IOF är uppfyllda kommer sökningar att kunna göras direkt av utsedda myndigheter i CIR som då snabbt kan få uppgift om en person finns i ett visst system. Därefter kan den sökande myndigheten göra en begäran om åtkomst till uppgifter i systemet i vanlig ordning. På så vis undviks onödiga begäran om åtkomst till uppgifter, vilket besparar tid för den sökande myndigheten och den centrala åtkomstpunkten.

Som nämnts ovan kommer det att följa av regelverket för respektive system vilka myndigheter som har rätt att göra sökningar enligt artikel 22. Bestämmelsen kräver därför inte några författningsändringar.

8.3 Registerföring av loggar

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om registerföring av loggar över uppgiftsbehandling i den gemensamma databasen för id-uppgifter kräver inte några författningsändringar.

Skälen för bedömningen: Enligt artikel 24.1–24.4 i IOF är eu-LISA skyldig att föra loggar över den uppgiftsbehandling i CIR som görs med stöd av artiklarna 20, 21 och 22. Vidare gäller enligt artikeln att varje medlemsstat ska föra loggar över sökningar som utförs av dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda CIR i enlighet med artiklarna 20, 21 och 22. Varje unionsbyrå ska föra loggar över sökningar som dess vederbörligen bemyndigade personal utför i enlighet med artiklarna 21 och 22. För all åtkomst till CIR i enlighet med artikel 22 ska varje medlemsstat dessutom föra loggar över referensnummer för den nationella akten, syftet med åtkomsten och, i enlighet med nationella regler, den unika användaridentitet som anger vilken tjänsteman som utförde sökningen och vilken tjänsteman som beordrade sökningen (artikel 24.5). I artikeln regleras även en skyldighet för Europol att föra loggar (artikel 24.6), den närmare hanteringen av loggarna (artikel 24.7) och eu-LISA:s lagring av loggarna (artikel 24.8).

Bestämmelserna i artikel 24 är direkt tillämpliga och kräver inte några nationella författningsåtgärder.

9 Åtkomst till CIR i identifieringssyfte

9.1 Förutsättningar för åtkomst till CIR enligt artikel 20 i IOF

9.1.1 Tillämpningen av artikel 20 i IOF förutsätter nationella lagstiftningsåtgärder

Enligt artikel 20.1 i IOF får medlemsstaternas polismyndigheter i vissa situationer göra sökningar i CIR i identifieringssyfte. Det gäller i sådana situationer där det saknas en resehandling eller annan trovärdig handling som styrker personens identitet, där det föreligger tvivel om de identitetsuppgifter som lämnats av den personen, om resehandlingens eller en annan trovärdig handlings äkthet eller om handlingsinnehavarens identitet, samt där personen inte kan eller vägrar att samarbeta. Sökningar får i så fall göras i CIR endast i syfte att identifiera personen (artikel 20.2). Sådana sökningar är dock inte tillåtna på minderåriga under 12 år, såvida det inte sker för barnets bästa (artikel 20.1).

Sökningarna ska enligt huvudregeln ske med personens biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro (artikel 20.2). I skäl 28 anges bl.a. att fingeravtryck bör tas med hjälp av tekniker för direktscanning. Kan de biometriska uppgifterna inte användas eller om en sökning med dessa uppgifter misslyckas ska sökningen i stället utföras med personens identitetsuppgifter i kombination med resehandlingsuppgifter eller de identitetsuppgifter som personen tillhandahåller (artikel 20.3 i IOF). I IOF definieras biometriska uppgifter som fingeravtrycksuppgifter eller ansiktsbilder, eller båda (artikel 4.11 i IOF). Med

fingeravtrycksuppgifter avses bilder av fingeravtryck och bilder av fingeravtrycksspår som på grund av sin unika karaktär och de referenspunkter som de innefattar möjliggör exakta och entydiga jämförelser för att fastställa en persons identitet. Med ansiktsbild avses digitala bilder av en persons ansikte.

Artikel 20 är fakultativt utformad, dvs. den lämnar till medlemsstaterna att välja om de vill utnyttja de möjligheter som artikeln innebär. För att sökningar i de situationer som räknas upp i artikel 20.1 ska vara tillåtna krävs enligt artikel 20.5 att medlemsstaterna har antagit nationella lagstiftningsåtgärder som anger de exakta syftena med identifieringen. Syftena måste ligga inom ramen för förordningarnas mål att bidra till att förebygga och bekämpa olaglig invandring och att bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa inom unionen, t.ex. att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier. Vidare ska de behöriga polismyndigheterna utses, och förfaranden, villkor och kriterier för sådana kontroller fastställas. När medlemsstaterna antar lagstiftningsåtgärder ska de ta hänsyn till att ingen diskriminering av tredjelandsmedborgare får förekomma.

Utöver möjligheten att söka i CIR i de situationer som anges i artikel 20.1 får medlemsstaterna enligt artikel 20.4 också bemyndiga polismyndigheter att 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. Enligt artikel 20.6 i IOF ska de medlemsstater som vill utnyttja den möjlighet som anges i punkt 4 anta nationella lagstiftningsåtgärder som fastställer förfarandena, villkoren och kriterierna.

Sökningar enligt artikel 20 i IOF ger sökande myndighet åtkomst till sådana uppgifter som avses i artikel 18.1 i IOF, t.ex. namn, medborgarskap, födelsedatum, kön, resehandlingsuppgifter, ansiktsbilder och fingeravtryck. Däremot får myndigheten inte åtkomst till uppgift om vilket underliggande system som informationen härrör från (artikel 18.2 i IOF). För sådan åtkomst måste myndigheterna i stället söka i varje enskilt system utifrån sina behörigheter och enligt de villkor som gäller enligt regleringen för respektive system (se dock artikel 22 i IOF om brottsbekämpande myndigheters sökningar i CIR i vissa fall).

9.1.2 Sökningar får endast göras av en polismyndighet

En förutsättning för att en myndighet ska kunna ges behörighet att söka i CIR enligt artikel 20 är att den kan betraktas som en polismyndighet i den mening som avses i IOF. Begreppet ”polismyndighet” definieras i förordningarna som behörig myndighet enligt definitionen i artikel 3.7 i dataskyddsdirektivet (se artikel 4.19 i IOF). Med behörig myndighet avses i dataskyddsdirektivet 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 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 (artikel 3.7 a och 3.7 b i direktivet).

Dataskyddsdirektivet har i huvudsak genomförts genom brottsdatalagen (2018:1177). I 1 kap. 6 § brottsdatalagen finns en definition av behörig myndighet. Den definitionen skiljer sig något från den i dataskyddsdirektivet så till vida att den svenska definitionen endast omfattar en myndighet eller aktör när den behandlar personuppgifter för vissa syften inom brottskämpning, verkställighet av straff och upprätthållande av allmän ordning och säkerhet (jfr prop. 2017/18:232 s. 100 och 434). Med hänsyn till utformningen av definitionen av ordet polismyndighet i IOF och förordningarnas uttryckliga hänvisning till dataskyddsdirektivet bör dock direktivets definition vara den vägledande för frågan om vilka svenska myndigheter som kan ges rätt att utföra sökningar i CIR. De myndigheter som avses med polismyndighet i artikel 20 är alltså de 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.

9.2 Polismyndighetens hemställan

Polismyndigheten anför i en hemställan till regeringen den 8 december 2020 (Ju2020/04544) att myndigheten ser att en åtkomst enligt artikel 20 i IOF skulle vara av stort värde i många delar av myndighetens verksamhet. Polismyndigheten hemställer därför om att det sker en författningsöversyn för att Sverige ska utnyttja förordningarnas möjlighet i denna del. Polismyndigheten föreslår en översyn på områden kopplade bl.a. till den gränskontrollerande och brottsutredande verksamheten. I hemställan framhålls ett antal situationer då sökningar enligt artikel 20 skulle kunna bidra till myndighetens verksamhet. Vidare redogör Polismyndigheten för relevant nationell lagstiftning på respektive område och för behoven av sökningar i CIR på respektive område. Enligt myndigheten är fastställandet av identiteten på någon som är föremål för en polisiär kontroll nästan alltid helt centralt för att polisen snabbt ska kunna vidta korrekta åtgärder i förhållande till den enskilde. Möjligheten till kontroll av biometriska uppgifter mot EU-informationssystem i identifieringssyfte skulle enligt Polismyndigheten bidra till att den fullgör sitt uppdrag mer effektivt och rättssäkert i situationer där myndigheten redan får ta upp och kontrollera biometriska uppgifter, men även kunna förenkla och effektivisera arbetet där möjlighet till kontroll och upptagning av biometriska uppgifter i dagsläget saknas.

9.3 Sökningar enligt artikel 20 i IOF inom ramen för en brottsutredning

Förslag: Det ska i lagen om internationellt polisiärt samarbete föreskrivas att de myndigheter som regeringen bestämmer ska i identifieringssyfte få utföra sökningar i den gemensamma databasen för id-uppgifter i syfte att utreda brott. Sökningar ska få genomföras med fotografi eller fingeravtryck som tagits enligt reglerna om förundersökning. Det ska i förordning anges att Polismyndigheten, Säkerhetspolisen och Tullverket ska vara behöriga att utföra sådana sökningar.

Skälen för förslaget

Det finns ett behov av att kunna söka i CIR för att identifiera personer inom ramen för en brottsutredning

Polismyndigheten hemställer att det möjliggörs i nationell lagstiftning att de biometriska uppgifter som får tas upp inom ramen för en förundersökning också får användas för sökning i CIR för att fastställa personens identitet. Som skäl anför myndigheten bl.a. att det inom ramen för utredningar av brott som involverar ett större antal personer, t.ex. människohandel och människosmuggling, är särskilt viktigt att polisen tidigt får en säker uppgift om vilka de personer som identifierats som gärningsmän, målsägande och vittnen är. Möjligheten att snabbt fastställa identiteten på de berörda underlättar polisens arbete att vidta rätt åtgärder i förhållande till de inblandade. För att kunna utreda och i förlängningen lagföra dessa grova brott krävs att polisen tidigt kan identifiera målsägande och vittnen och tillsammans med andra samhällsaktörer ge dem behövligt skydd. Polismyndigheten anser att det i samtliga situationer där myndigheten har möjlighet att ta upp biometriska uppgifter, och uppgift om personens identitet är av betydelse för brottsutredningen, finns ett behov av att även få söka med dessa uppgifter mot CIR i identifieringssyfte.

Regeringen har tidigare konstaterat att biometri kan vara ett mycket kraftfullt verktyg i brottsbekämpningen. Även mindre förändringar av regelverket kan leda till påtagliga förbättringar av möjligheterna att identifiera misstänkta. Regeringen har därför gett en särskild utredare i uppdrag att se över förutsättningarna för att använda biometri som verktyg i brottsbekämpningen (dir. 2021:34). Syftet med utredningen är att fler personer som misstänks för brott ska kunna identifieras med hjälp av fingeravtryck, dna, ansiktsbilder eller liknande information om individuella kännetecken. Uppdraget gäller de rättsliga möjligheterna att samla in, lagra och använda sådan information. Uppdraget ska redovisas senast den 20 februari 2023.

Tillgång till fler relevanta register för sökningar med hjälp av biometriska uppgifter kan förbättra Polismyndighetens möjligheter att klara upp allvarliga brott. Mer konkret kan sökningar i CIR göra det möjligt att i vissa fall identifiera och lagföra även sådana personer som inte förekommer i Polismyndighetens fingeravtrycks- och

signalementsregister. Det bedöms därför finnas ett behov för brottsbekämpande myndigheter att kunna söka i CIR inom ramen för en brottsutredning.

Sökningar i CIR i brottsutredande syfte är förenligt med målen för IOF

För att medlemsstaterna ska kunna införa en möjlighet att göra sökningar i CIR enligt artikel 20.1–20.3 i IOF krävs att det sker i enlighet med målen för IOF enligt artikel 2.1 b och c. Enligt artikel 2.1 c i IOF ska förordningarna bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa, bl.a. att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorium. Brottsbekämpning får anses vara en sådan verksamhet som bidrar till en hög säkerhetsnivå inom Schengenområdet. Den tolkningen får stöd av artikel 67.3 i EU:s funktionsfördrag i vilken det anges att unionen ska verka för en hög säkerhetsnivå bl.a. genom förebyggande och bekämpning av brottslighet. Vidare har bl.a. artikel 87 i fördraget, som rör polisiärt samarbete, angetts som rättslig grund för förordning (EU) 2019/818. Enligt nämnda bestämmelse ska unionen utveckla ett polissamarbete mellan alla behöriga myndigheter i medlemsstaterna, inbegripet polisen, tullen och andra brottsbekämpande organ som är specialiserade på att förebygga, upptäcka och utreda brott. Sökningar i CIR inom ramen för en brottsutredning bedöms därför vara i enlighet med de mål som förordningarna ska bidra till.

Biometriska uppgifter får tas upp enligt rättegångsbalkens regler

Som nämns ovan ska sökningar enligt artikel 20.1–20.3 i IOF som huvudregel ske med personens biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro. För att sökningar i CIR ska kunna utföras i den brottsutredande verksamheten krävs således att den myndighet som gör sökningen också har rätt att uppta nödvändiga uppgifter. Bestämmelser om när fingeravtryck och fotografier får tas av personer inom ramen för förundersökningar finns i rättegångsbalken. I 28 kap. 14 § rättegångsbalken anges att fotografi

och fingeravtryck får tas bl.a. av den som är anhållen eller häktad. Kompletterande bestämmelser finns i förordningen (1992:824) om fingeravtryck m.m. Där anges att det är obligatoriskt att ta fotografi och fingeravtryck av den som har häktats och i vissa fall även av den som har anhållits. Om det behövs för att utreda brott på vilket fängelse kan följa får fingeravtryck och fotografi tas även av andra, t.ex. av misstänkta som inte är frihetsberövade. Samma åtgärder får vidtas mot andra personer, om det behövs för att utreda brott på vilket fängelse kan följa. Beslut om dessa åtgärder fattas av förundersökningsledaren, om åtgärden behövs för utredningen, och i andra fall av Polismyndigheten.

Det finns således bestämmelser i nationell rätt som möjliggör upptagning av fingeravtryck och fotografier i en brottsutredning för att identifiera en person.

Målen, förfarandena, villkoren och kriterierna för kontrollerna framgår av befintligt regelverk

I artikel 20.5 i IOF anges att medlemsstater som vill utnyttja möjligheten till sökningar i identifieringssyfte ska anta nationella lagstiftningsåtgärder. När medlemsstaterna gör detta ska de ta hänsyn till att ingen diskriminering av tredjelandsmedborgare får förekomma. I sådana lagstiftningsåtgärder ska de exakta syftena med identifieringen anges inom ramen för de mål som avses i artikel 2.1 b och c i IOF. De behöriga polismyndigheterna ska utses, och förfaranden, villkor och kriterier för sådana kontroller ska fastställas.

Även om det förutsätts nationella lagstiftningsåtgärder för sökningar enligt artikel 20 i IOF behöver bestämmelsen i sig inte införlivas i svensk rätt för att vara tillämplig. Av artikel 288 i EU:s funktionsfördrag följer att IOF har allmän giltighet och att de är till alla delar bindande och direkt tillämpliga. Artikel 20 i IOF ska således likställas med svensk lag under förutsättning att Sverige genom lagstiftningsåtgärder valt att utnyttja möjligheten till sökningar i identifieringssyfte. Om så har skett bedöms de kriterier för sökningar i CIR i identifieringssyfte som anges i artikel 20 vara direkt tillämpliga och behöver därför inte återges i nationell författning. Detta gäller t.ex. kriteriet för under vilka omständigheter sökningar får göras och möjligheten att söka med

uppgifter som rör barn (artikel 20.1 i IOF), kravet på att sökningar görs med biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro (artikel 20.2 i IOF) och möjligheten att utföra sökningen med andra identitetsuppgifter i kombination med resehandlingsuppgifter eller med de identitetsuppgifter som tillhandahållits av personen (artikel 20.3 i IOF). Med identitetsuppgifter avses t.ex. namn och efternamn (se artikel 4.8 i IOF jfr med artikel 27 i IOF).

Villkoret i artikel 20.5 i IOF om nationella lagstiftningsåtgärder bör förstås som att de medlemsstater som vill utnyttja möjligheten till sökningar enligt artikeln också säkerställer att det finns kompletterande bestämmelser på nationell nivå som specificerar syftet med identifieringen. Vidare ska medlemsstaterna peka ut behöriga nationella myndigheter samt säkerställa att det finns rättsligt stöd för att uppta den biometri som krävs för att göra sådana sökningar (jfr skäl 30 i IOF). Som ovan konstaterats ger bl.a. 28 kap. 14 § rättegångsbalken rättsligt stöd för att uppta biometri i syfte att identifiera en person inom ramen för en brottsutredning. Vidare bedöms sökningar i CIR med sådana uppgifter falla inom förordningarnas mål att bibehålla en hög säkerhetsnivå inom unionen. Detta följer av rättegångsbalkens regler om syftet med en förundersökning (se 23 kap. 1 § rättegångsbalken) och behöver inte regleras ytterligare i nationell rätt. Såvitt avser förfarandena, villkoren och kriterierna för kontroller inom ramen för en förundersökning framgår dessa av befintligt nationellt regelverk, främst rättegångsbalken och polislagen (se även kompletterande bestämmelser på förordningsnivå och Polismyndighetens föreskrifter och allmänna råd [PMFS 2022:6, FAP 473-1 om fingeravtryck och annan signalementsupptagning]). Utformningen av aktuella bestämmelser bedöms uppfylla kravet i artikel 20.5 i IOF på att hänsyn ska tas till att ingen diskriminering av tredjelandsmedborgare får förekomma.

Sverige bör möjliggöra sökningar i CIR enligt artikel 20.1–20.3 i IOF inom ramen för en brottsutredning

Relevanta myndigheter bör alltså få rätt att göra sökningar i CIR enligt artikel 20 inom ramen för en brottsutredning. Frågan uppstår då var detta ska regleras.

I dataskyddslagstiftningen finns regler om hur personuppgifter som tas med stöd av 28 kap. 14 § rättegångsbalken får lagras och användas. Det handlar om vilka register Polismyndigheten får föra, hur lång tid olika uppgifter får sparas, för vilka ändamål uppgifter får användas och om sökningar. För Polismyndighetens del består dataskyddslagstiftningen främst av brottsdatalagen och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag). Svenska myndigheters åtkomst till uppgifter i CIR:s underliggande system i brottsbekämpande syfte regleras dock såvitt avser VIS och Eurodac i lagen och förordningen om internationellt polisiärt samarbete. Nämnda författningar innebär specialreglering i förhållande till polisens brottsdatalag (se 3 § polisens brottsdatalag). I promemoriorna Anpassning av svensk rätt till EU:s nya in- och utresesystem (Ds 2021:9) och Anpassning av svensk rätt till EU:s nya system för reseuppgifter och resetillstånd (Ds 2021:19) föreslås att åtkomst till uppgifter i in- och utresesystemet samt Etias för brottsbekämpande ändamål regleras i samma regelverk. Det bedöms lämpligt att även åtkomst till uppgifter i CIR i enlighet med artikel 20.1–20.3 i IOF regleras där i de fall då det är fråga om sökningar som görs inom ramen för en förundersökning. Det bör därför föreskrivas i lagen om internationellt polisiärt samarbete att sökningar i CIR enligt artikel 20 i IOF får ske i syfte att utreda brott. Det bör även framgå av bestämmelsen att sådana sökningar får genomföras med fotografi eller fingeravtryck som upptagits med stöd av 28 kap. 14 § rättegångsbalken.

Behöriga myndigheter bör utses i förordning

Som redan nämnts ska de medlemsstater som vill utnyttja möjligheten till sökningar enligt artikel 20 peka ut de nationella myndigheter som ska ha rätt att göra sådana sökningar. Det måste alltså framgå av svensk författning vilka nationella myndigheter som

ska ha rätt att söka i CIR med fingeravtryck som upptagits inom ramen för en brottsutredning. Eftersom behöriga myndigheter kan komma att ändras över tid bör utpekandet av dessa göras på förordningsnivå, vilket kan ske med stöd av 8 kap. 7 § regeringsformen.

Polismyndighetens hemställan gäller endast myndighetens eget brottsutredande arbete. Även Säkerhetspolisen får inom ramen för sitt brottsutredande uppdrag ta upp biometri med stöd av 28 kap. 14 § rättegångsbalken (se 23 kap. 3 § rättegångsbalken, jfr med 3 § polislagen). Detsamma gäller Tullverket som i vissa fall (se t.ex. 19 § första stycket lagen [2000:1225]) om straff för smuggling) får fatta beslut om att inleda förundersökning enligt 23 kap. rättegångsbalken. De befogenheter och skyldigheter som en undersökningsledare har enligt rättegångsbalken gäller då Tullverket. När en åklagare leder en förundersökning som avser t.ex. brott mot lagen om straff för smuggling eller vissa narkotikabrott får åklagaren anlita biträde av Tullverket och får också ge en tjänsteman vid Tullverket i uppdrag att vidta en viss åtgärd som hör till förundersökningen, om det är lämpligt med hänsyn till åtgärdens beskaffenhet (19 § tredje stycket lagen om straff för smuggling).

Vad som ovan anförts om Polismyndighetens behov av att snabbt kunna identifiera personer som befinner sig på en brottsplats eller annars är misstänkta för brott gör sig även gällande i Säkerhetspolisens och Tullverkets brottsutredande verksamheter. Det bör därför införas en bestämmelse på förordningsnivå som ger Polismyndigheten, Säkerhetspolisen och Tullverket behörighet att göra sökningar i CIR i syfte att utreda brott.

Polismyndigheten har i sin hemställan anfört att även Kustbevakningen bör ges möjlighet att söka i CIR enligt artikel 20. Det saknas dock stöd i dagens regelverk för att Kustbevakningen ska få behandla biometriska uppgifter inom ramen för sitt brottsbekämpande uppdrag. I förarbetena till lagen om Kustbevakningens behandling av personuppgifter på brottsdatalagens område instämde regeringen i bedömningen att det inte har framkommit något behov för Kustbevakningen att behandla biometriska och genetiska uppgifter för brottsbekämpande syften (se prop. 2017/18:269 s. 193). För att Kustbevakningen ska kunna utföra sökningar enligt artikel 20.1–20.3 i IOF krävs således överväganden om detta ställningstagande bör ändras. Sådana

överväganden skulle komma att avse myndighetens möjlighet att behandla känsliga personuppgifter även i andra situationer än vid sökningar i CIR. Frågan bedöms därför ligga utanför ramarna för detta lagstiftningsarbete. Kustbevakningen bör därför inte i dagsläget ges behörighet att utföra sökningar enligt artikel 20.1–20.3 i IOF i identifieringssyfte.

9.4 Sökningar enligt artikel 20 i IOF vid upprätthållande av allmän ordning och säkerhet

Bedömning: Sökningar i den gemensamma databasen för id-uppgifter kommer att vara tillåtna i identifieringssyfte vid ingripanden enligt polislagen eller skyddslagen om det finns förutsättningar att uppta biometri med stöd av reglerna om förundersökning.

Skälen för bedömningen

Sökningar i CIR vid ingripanden enligt 14 § polislagen

Polismyndigheten anför i sin hemställan att det finns behov av att kunna göra sökningar i CIR enligt artikel 20.1–20.3 i IOF i samband med s.k. polisiering. Med polisiering avses ingripanden som görs med stöd av 14 § polislagen. Enligt den bestämmelsen får en okänd person som anträffas av en polisman omhändertas för identifiering, om han eller hon vägrar att lämna uppgift om sin identitet eller det finns anledning att anta att hans eller hennes uppgift om denna är oriktig. Vidare krävs att det finns särskild anledning att anta att personen är efterspanad eller efterlyst och med stöd av lag ska berövas friheten vid anträffandet. Av 16 § tredje stycket polislagen framgår att åtgärder för att fastställa den omhändertagnes identitet ska vidtas skyndsamt. Den omhändertagne ska omedelbart friges så snart han eller hon har identifierats. Han eller hon får dock inte hållas kvar längre än sex timmar eller, om det är av synnerlig vikt att han eller hon identifieras, tolv timmar.

Enligt Polismyndigheten behöver polisen snabbt och med säkerhet kunna fastställa en omhändertagen persons identitet vid polisiering. Sökningar i CIR skulle innebära att en omhändertagen

person snabbare skulle kunna avfärdas som efterspanad eller efterlyst. Detta skulle enligt myndigheten innebära att personen inte behöver vara omhändertagen längre än nödvändigt.

Som nämns i avsnitt 9.3 måste medlemsstaterna säkerställa att de myndigheter som ska ges rätt att söka i CIR enligt artikel 20.1–20.3 även har rätt att uppta de uppgifter som krävs för att kunna utföra sådana sökningar. 14 § polislagen föreskriver dock inte någon särskild möjlighet att uppta fotografi eller fingeravtryck. Frågan uppstår därför om det bör införas en ny bestämmelse i polislagen som innebär att sådana uppgifter kan upptas i samband med polisiering för att sökningar i CIR ska kunna göras enligt artikel 20.1–20.3 i IOF. Ett sådant övervägande kräver en noggrann analys utifrån enskildas grundlagsskyddade rättigheter och befintliga rättssäkerhetsgarantier.

Det konstateras att polislagen inte heller i övrigt innehåller någon bestämmelse som i sig ger Polismyndigheten rätt att uppta en persons fotografi eller fingeravtryck. Möjligheten att uppta sådana uppgifter skulle alltså kräva principiella överväganden som aktualiserar frågan om denna möjlighet bör införas även i andra situationer som regleras i polislagen. Vidare skulle övervägandena av naturliga skäl också väcka frågan om uppgifterna bör kunna användas för sökningar i andra, t.ex. nationella, register. Det bedöms därför inte lämpligt att inom ramen för detta lagstiftningsarbete överväga ändringar i polislagen som innebär att polisen ges ytterligare tvångsbefogenheter. Som framgår av avsnitt 9.3 föreslås dock att det införs en möjlighet att utföra sökningar i CIR enligt artikel 20.1–20.3 i IOF med fingeravtryck som tas upp inom ramen för en förundersökning. Om rättegångsbalkens regler för upptagning av biometri är uppfyllda kommer således sökningar i CIR att kunna göras även då en person har omhändertagits med stöd av 14 § polislagen.

Sökningar i CIR vid ingripanden enligt 12 § skyddslagen

Polismyndigheten har i sin hemställan pekat på ett behov av att kunna göra sökningar i CIR vid ingripanden enligt skyddslagen. Skyddslagen innehåller bl.a. bestämmelser om vissa åtgärder till förstärkt skydd för byggnader, andra anläggningar, områden och

andra objekt mot bland annat sabotage, terroristbrott, spioneri och grovt rån (l § skyddslagen [2010:305]). För att tillgodose behovet av skydd kan det beslutas att något ska vara skyddsobjekt (3–6 §§ skyddslagen). Ett beslut om skyddsobjekt innebär att obehöriga inte har tillträde till skyddsobjektet (7 § skyddslagen). Den som bevakar ett skyddsobjekt får om det behövs för att kunna fullgöra bevakningsuppgiften avvisa, avlägsna eller, om en sådan åtgärd inte är tillräcklig, tillfälligt omhänderta en person inom eller invid skyddsobjektet, bl.a. om personen vägrar att på begäran lämna uppgift om namn, födelsetid eller hemvist eller lämnar uppgift om detta som skäligen kan antas vara oriktig, eller vägrar att underkasta sig kroppsvisitation (12 § skyddslagen).

Av 9 § skyddslagen framgår att för bevakning av ett skyddsobjekt får polismän, militär personal eller annan särskilt utsedd personal anlitas. Den som bevakar ett skyddsobjekt och som inte är polisman benämns skyddsvakt. Det finns såväl militära skyddsvakter som civila skyddsvakter, de förstnämnda godkänns av Försvarsmakten och de senare av länsstyrelserna (se 6 § skyddsförordningen [2010:523]). Vidare får finsk militär i vissa fall anlitas för bevakning av skyddsobjekt. En skyddsvakt har inom skyddsobjektet och i dess närhet samma befogenhet som en polisman att gripa den som det finns skäl att anhålla för spioneri, sabotage, terroristbrott, grovt rån eller förberedelse till ett sådant brott samt att ta i beslag föremål som personen för med sig. Detta gäller också om den misstänkte är på flykt från skyddsobjektet. I 17 § skyddslagen anges att ett tillfälligt omhändertagande, gripande eller beslag som har gjorts av en skyddsvakt genast ska anmälas till en polisman. Den som tagit emot anmälan ska genast pröva om åtgärden ska bestå. Ett tillfälligt omhändertagande ska upphöra så snart ändamålet med åtgärden har förlorat sin betydelse, dock senast sex timmar efter omhändertagandet. En polisman som tar befattning med tillfälliga omhändertaganden som gjorts med stöd av skyddslagen ska tillämpa bestämmelserna i 15–17 §§ polislagen.

Polismyndigheten anser att det i nationell lagstiftning bör ges möjlighet att ta upp biometriska uppgifter för sökning mot bl.a. CIR i identifieringssyfte vid ingripanden enligt skyddslagen. Enligt Polismyndigheten skulle detta möjliggöra en snabb och säker identifiering, vilket bidrar till att kroppsvisitationer och omhändertaganden av personer som saknar identitetshandlingar

eller vägrar att medverka till identifiering kan undvikas. I likhet med polislagen föreskriver inte skyddslagen någon särskild möjlighet att uppta biometri. Därmed uppstår frågan om sådana befogenheter bör övervägas för att möjliggöra sökningar i CIR i samband med bevakning av skyddsobjekt.

I samband med införandet av den nya skyddslagen ansågs de befogenheter som gällde enligt dåvarande lagstiftning vara väl avpassade för ifrågavarande bevakningsuppgifter (se Skyddslagsutredningens betänkande Skyddet för samhällsviktig verksamhet, SOU 2008:50 s. 157 f.). Skyddslagsutredningen fann därför inte någon anledning att föreslå några principiella ändringar i fråga om regleringen rörande de befogenheter som skyddslagen tillerkänner skyddsvakter. Regeringen, som i huvudsak delade utredningens bedömning, konstaterade att redan då gällande skyddslag ger en skyddsvakt relativt långt gående befogenheter att använda tvångsmedel mot enskilda personer. Samtidigt ansåg regeringen att bestämmelserna är väl avpassade för att i möjligaste mån begränsa intrånget i den enskildes fysiska och privata sfär (se prop. 2009/10:87 s. 60 f.). Regeringen föreslog därför att en skyddsvakt ska ha samma befogenheter som enligt då gällande skyddslag. Det föreslogs inte heller någon ändring av polismans befogenheter.

Som regeringen konstaterade i nämnda proposition medför de regler som finns i skyddslagen bl.a. begränsningar i enskildas fri- och rättigheter. Regeringen anförde vidare att de grundlagsfästa rättigheterna gör att det finns all anledning att vara återhållsam vid övervägandet av vilka befogenheter en skyddsvakt bör ha (se ovan a. prop. s. 60). Införandet av en bestämmelse i skyddslagen om upptagning av biometri skulle innebära en utvidgning av befintliga befogenheter.

Det bedöms inte lämpligt att inom ramen för detta lagstiftningsarbete göra överväganden om att införa bestämmelser om ytterligare befogenheter i skyddslagen. Det konstateras dock att en skyddsvakt har samma befogenheter som polisman att inom skyddsobjektet och i dess närhet gripa den som det finns skäl att anhålla för vissa uppräknade brott (se 13 § skyddslagen). Vid sådana ingripanden kan det i förlängningen bli aktuellt att uppta fotografi eller fingeravtryck med stöd av 28 kap. 14 § rättegångsbalken. Om förutsättningarna för sådan upptagning är uppfyllda kommer

sökningar i CIR att vara möjliga i enlighet med det förslag som görs i avsnitt 9.3.

9.5 Användning av CIR på utlänningsrättens område

9.5.1 Inre utlänningskontroller

Förslag: En polisman eller en tjänsteman vid Kustbevakningen ska vid en inre utlänningskontroll få genomföra en sökning i identifieringssyfte i den gemensamma databasen för id-uppgifter. En utlänning ska vara skyldig att låta en polisman eller en tjänsteman vid Kustbevakningen fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

Skälen för förslaget

Det finns skäl att ge nationella myndigheter rätt att söka i CIR vid inre utlänningskontroller

Artikel 20 i IOF innebär att en polismyndighet kan ges rätt att söka i CIR med en persons biometriska uppgifter som tagits direkt under en identitetskontroll. Det bör övervägas om svenska myndigheter bör ges rätt att utföra sådana sökningar vid inre utlänningskontroller.

En inre utlänningskontroll innebär en kontroll av en utlänning som finns inne i landet, i syfte att kontrollera utlänningens rätt att vistas här. Bestämmelser om inre utlänningskontroller finns i 9 kap. 9 § UtlL. Vid en inre utlänningskontroll är en utlänning som vistas i Sverige skyldig att på begäran av en polisman överlämna pass eller andra handlingar som visar att han eller hon har rätt att uppehålla sig i Sverige. Begreppet polisman omfattar tjänstemän vid både Polismyndigheten och Säkerhetspolisen (se 4 § polislagen och 2 § polisförordningen [2014:1104]).

Utlänningen är också skyldig att efter kallelse av Migrationsverket eller Polismyndigheten inställa sig och lämna uppgifter om

sin vistelse här i landet, och får dessutom hämtas av Polismyndigheten om han eller hon inte inställer sig. Kustbevakningen medverkar också i kontrollverksamheten genom kontroll av och i anslutning till sjötrafiken. Kustbevakningen får även i annat fall biträda Polismyndigheten. En inre utlänningskontroll får endast vidtas om det finns grundad anledning att anta att utlänningen saknar rätt att uppehålla sig här i landet eller om det annars finns särskild anledning till kontroll.

Det finns redan i dag vissa möjligheter att göra sökningar med biometriska uppgifter i exempelvis SIS i samband med en inre utlänningskontroll (se artikel 27 1 b i SIS-II-förordningen). Även efter att det nya SIS-regelverket börjat tillämpas fullt ut kommer det att vara möjligt att göra sådana sökningar i SIS (se artikel 34.1 b i gränsförordningen, artikel 17.1 i återvändandeförordningen och 11 § 2 förordningen [2021:1188] med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem). När in- och utresesystemet har tagits i drift kommer det även att vara möjligt att söka i det systemet med biometriska uppgifter vid inre utlänningskontroller (se artiklarna 26 och 27 i in- och utreseförordningen och prop. 2021/22:81).

De nu nämnda möjligheterna till sökningar är mer begränsade än de möjligheter som följer enligt artikel 20 i IOF (jfr avsnitt 9.1.1). CIR kommer att innehålla uppgifter från in- och utresesystemet men inte från SIS. Databasen kommer dessutom att innehålla uppgifter från flera andra EU-informationssystem, t.ex. VIS och Ecris-TCN. En möjlighet att söka i CIR i identifieringssyfte skulle alltså avsevärt utöka möjligheterna för myndigheterna att samtidigt få tillgång till information i flera olika EU-informationssystem.

För att upprätthålla den reglerade invandringen är det nödvändigt att kunna klarlägga om personer som befinner sig i Sverige har rätt att vistas här. För att det ska vara möjligt behöver personerna kunna identifieras. Inre utlänningskontroller bidrar på ett betydelsefullt sätt till att upprätthålla en hållbar migrationspolitik och ett effektivt återvändandearbete. Att identiteten på utlänningar som befinner sig i Sverige klarläggs är även viktigt ur ett säkerhetsperspektiv och kontrollerna kan tjäna som ett verktyg för att förebygga, motverka och bekämpa terroristhandlingar och annan allvarlig brottslighet. De terroristattentat som har förekommit i Europa under senare år har tydligt visat hur viktigt det är att ha kontroll på vilka som vistas i

landet. Även när det gäller bekämpande av annan gränsöverskridande brottslighet är brottsmisstänktas identitet av stor betydelse. Det är inte ovanligt att det i dessa sammanhang förekommer personer som uppträder under olika identiteter (jfr prop. 2020/21:159 s. 11).

Det är inte alltid det går att identifiera en person vid en inre utlänningskontroll. Enligt artikel 20 kan myndigheter ges rätt att utföra sökningar i CIR i fem angivna situationer som kan aktualiseras vid en inre utlänningskontroll. Det gäller bl.a. om en polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller annan trovärdig handling, om det finns tvivel om de identitetsuppgifter som lämnats eller om en person inte kan eller vägrar att samarbeta (artikel 20.1, se vidare avsnitt 9.1.1).

En sökning i CIR med en persons ansiktsbild eller fingeravtryck skulle i sådana situationer vara ett viktigt verktyg för att kunna identifiera personen i fråga. I många fall skulle en sådan sökning kunna bidra till en snabbare och säkrare identifiering.

En reglering som ger rätt för myndigheter att göra sökningar i CIR skulle innebära personuppgiftsbehandling. En sådan reglering aktualiserar frågor om enskildas grundläggande fri- och rättigheter. I avsnitt 4.2 finns en närmare redogörelse för regler i regeringsformen, Europakonventionen, EU:s rättighetsstadga och barnkonventionen som rör enskildas fri- och rättigheter. Regelverken innebär bl.a. ett skydd för den enskildes personliga integritet. De rättigheter som aktualiseras är dock inte absoluta utan de får inskränkas under vissa förutsättningar.

Vidare innehåller dataskyddsförordningen ett principiellt förbud mot att behandla vissa särskilda kategorier av personuppgifter (artikel 9.1). Förbudet omfattar bl.a. behandling av biometriska uppgifter för att entydigt identifiera en fysisk person. Förbudet kompletteras av ett antal undantag som gör det möjligt att behandla sådana personuppgifter i vissa fall. Ett sådant undantag är om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades rättigheter och intressen (artikel 9.2 g).

IOF har tagits fram med beaktande av dataskyddsförordningen (se t.ex. skäl 73–75 i förordning [EU] 2019/817 och skäl 69–71 i förordning [EU] 2019/818). Dessutom finns i IOF bestämmelser om dataskydd, däribland gällande säkerhet vid behandling av personuppgifter, egenkontroll, sanktioner, och skadestånd (se kapitel VII). Förordningarna innehåller därigenom sådana skyddsåtgärder som krävs enligt ovan nämnda undantag (jfr även skäl 20 i IOF).

Det finns också rättighetsgarantier i artikel 5 i IOF som gäller för behandling av personuppgifter vid tillämpning av IOF.

Vidare innehåller reglerna om sökning i CIR tydliga avgränsningar. I artikel 20 finns ett antal villkor och begränsningar avseende möjligheten att genomföra sökningar. En förutsättning för att få söka med biometriska uppgifter i CIR är att någon av de specifika situationer kopplade till identifieringssvårigheter som räknas upp i förordningarna föreligger. Sökningar får endast göras i identifieringssyfte och förfarandet ska ha inletts i den berörda personens närvaro. De biometriska uppgifterna ska vidare ha tagits direkt under en identitetskontroll. Dessutom tillåts sökningar inte när det gäller barn under 12 år, såvida det inte sker för barnets bästa. Den krets av myndigheter som kan genomföra sökningar begränsas därtill av att det endast kan röra sig om polismyndigheter enligt förordningarnas definition (artikel 20.1 och 20.2).

Sökning med personuppgifter i identifieringssyfte vid en inre utlänningskontroll har till ändamål att tillgodose angelägna samhällsintressen, bl.a. att värna statens säkerhet. Det intrång i den enskildes personliga integritet som det innebär att söka med fotografier och fingeravtryck bedöms uppvägas av de allmänna intressen som åtgärden syftar till. Regler om rätt till sådana sökningar är alltså förenliga med Europakonventionen och EU:s rättighetsstadga. Den föreslagna åtgärden är också förenlig med regeringsformen och barnkonventionen. Vidare bedöms den personuppgiftsbehandling som en sökning med fotografi och fingeravtryck i CIR vid en inre utlänningskontroll innebär, i enlighet med vad som framgår ovan, vara nödvändig av hänsyn till ett viktigt allmänt intresse och att förutsättningarna även i övrigt är uppfyllda för att tillämpa undantaget i artikel 9.2 g i dataskyddsförordningen.

Inre utlänningskontroller bedöms ligga inom ramen för målet att bidra till att förebygga och bekämpa olaglig invandring (se avsnitt 9.1.1 och artikel 2.1 b och 20.5 i IOF).

För att en myndighet ska kunna ges rätt att söka enligt artikel 20 krävs att den ryms inom definitionen av en polismyndighet (se artiklarna 4.19 och 20.5 och avsnitt 9.1.2). Polismyndigheten, Säkerhetspolisen och Kustbevakningen har sådana brottsbekämpande uppgifter som gör att de ska anses vara polismyndigheter enligt förordningarnas definition. Däremot har Migrationsverket inte sådana uppgifter som faller inom definitionen. Migrationsverket kan därmed inte ges rätt att söka i CIR. Det bör också framhållas att de aktuella myndigheterna redan i dag behandlar personuppgifter vid inre utlänningskontroll enligt utlänningslagen.

Mot denna bakgrund talar starka skäl för att det bör införas en rätt för Polismyndigheten, Säkerhetspolisen och Kustbevakningen att söka i CIR i samband med en inre utlänningskontroll.

En förutsättning för att kunna söka i CIR enligt artikel 20.1–20.3 är dock att det finns en möjlighet att ta upp biometriska uppgifter för detta ändamål. Frågan om upptagning av biometriska uppgifter behandlas i följande avsnitt.

Det är ändamålsenligt och proportionerligt att införa regler om upptagande av fingeravtryck och fotografier för sökningar i CIR

Av artikel 20.2 i IOF följer att en polismyndighet får söka i CIR med en persons biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro. I förordningarna anges att det i nationell rätt bör föreskrivas en befogenhet för en anställd vid en behörig myndighet att ta biometriska uppgifter av en person under en identitetskontroll (skäl 30). Däremot innehåller förordningarna inte några bestämmelser om upptagning av biometriska uppgifter (dvs. fingeravtrycksuppgifter eller ansiktsbilder, eller båda, se artikel 4.11). För att kunna utnyttja möjligheten att söka i CIR enligt artikel 20.1–20.3 i samband med inre utlänningskontroller krävs alltså att det enligt nationell rätt finns en möjlighet att ta upp biometriska uppgifter i form av fingeravtryck och ansiktsbilder som får användas för det ändamålet.

Med ansiktsbild avses i IOF digitala bilder av en persons ansikte (artikel 4.10). I utlänningslagen används dock genomgående ”fotografi” eller ”fotografera”. Syftet är att skapa enhetlighet inom

utlänningslagen (se t.ex. prop. 2021/22:81 s. 37). Samma uttryck bör därför användas även i detta sammanhang.

Bestämmelser om myndigheters möjlighet att ta fotografier och fingeravtryck i utlänningsärenden finns i 9 kap. UtlL.

Det finns redan i dag en möjlighet att ta fingeravtryck och fotografi vid en inre utlänningskontroll enligt ett antal olika bestämmelser. Migrationsverket eller Polismyndigheten får fotografera en utlänning och, om utlänningen har fyllt 14 år, ta hans eller hennes fingeravtryck om varken utlänningens identitet eller rätt att vistas i Sverige kan klarläggas vid en inre utlänningskontroll (9 kap. 8 § första stycket 4 UtlL). Vid en sådan kontroll är en utlänning även skyldig att låta en polisman, en särskilt förordnad passkontrollant eller en tjänsteman vid Tullverket, Kustbevakningen eller Migrationsverket fotografera honom eller henne och ta hans eller hennes fingeravtryck för att genom en sökning i SIS identifiera utlänningen om identiteten inte kan fastställas på annat sätt (9 kap. 8 f § första stycket UtlL). Dessutom är den som innehar ett uppehållstillståndskort, ett uppehållskort, ett permanent uppehållskort, ett bevis om uppehållsstatus eller ett bevis för gränsarbetare skyldig att vid en inre utlänningskontroll låta en polisman, en särskilt förordnad passkontrollant eller en tjänsteman vid Tullverket, Kustbevakningen eller Migrationsverket fotografera honom eller henne och ta hans eller hennes fingeravtryck, för kontroll av att dessa motsvarar dem som finns sparade i kortet eller beviset (9 kap. 8 b § första stycket UtlL). Det finns också en skyldighet att låta sig fotograferas och lämna fingeravtryck för en utlänning som ansöker om asyl eller uppehållstillstånd – vilket kan aktualiseras i samband med en inre utlänningskontroll (se exempelvis 9 kap. 8 § första stycket 2). Vidare har regeringen utfärdat en lag med en bestämmelse, 9 kap. 8 h § UtlL, som kommer att träda i kraft i samband med att in- och utresesystemet tas i drift. Enligt bestämmelsen ska en utlänning vid en inre utlänningskontroll vara skyldig att låta en polisman, eller en tjänsteman vid Kustbevakningen eller Migrationsverket, fotografera honom eller henne och ta hans eller hennes fingeravtryck för kontroll i enlighet med artiklarna 26 och 27 i in- och utreseförordningen. Skyldigheten ska inte gälla om utlänningen är under tolv år eller om det är fysiskt omöjligt att lämna fingeravtryck (SFS 2022:242, som träder i kraft den dag som regeringen bestämmer).

En förutsättning för att ett fotografi eller fingeravtryck ska kunna tas med stöd av 9 kap. 8 § första stycket 4 UtlL är att varken utlänningens identitet eller rätt att vistas i Sverige kan klarläggas. Denna förutsättning innebär att det inte skulle gå att ta upp biometriska uppgifter med stöd av denna bestämmelse i alla de situationer där sökningar kan ske enligt artikel 20. Vidare får de uppgifter som tas med stöd av 9 kap. 8 f § UtlL endast användas för sökningar i SIS. Även bestämmelserna i 9 kap. 8 b § och 9 kap. 8 h § innehåller begränsningar av de ändamål för vilka de biometriska uppgifterna får användas, som innebär att de biometriska uppgifter som tas upp med stöd av dessa bestämmelser inte kan användas för sökningar enligt artikel 20. Av motsvarande skäl ger inte heller övriga bestämmelser i 9 kap. tillräckliga möjligheter till fotografering och upptagande av fingeravtryck för sökningar enligt artikel 20. Dessutom är det delvis andra myndigheter som det kan komma i fråga att ge en möjlighet att söka i CIR med fingeravtryck och fotografi än de myndigheter som får ta sådana uppgifter enligt de aktuella bestämmelserna i utlänningslagen.

De befintliga bestämmelserna i utlänningslagen kan alltså inte tillämpas för att ta de fingeravtryck och fotografier som är nödvändiga för att möjliggöra sökningar i CIR. För att möjliggöra sådana sökningar krävs alltså att det införs nya bestämmelser om upptagande av biometriska uppgifter vilket aktualiserar frågor om enskildas grundläggande fri- och rättigheter. I avsnitt 4.2 finns en närmare redogörelse för regler i regeringsformen, Europakonventionen, EU:s rättighetsstadga och barnkonventionen som rör enskildas fri- och rättigheter. Regelverken innebär bl.a. ett skydd för den enskildes kroppsliga och personliga integritet. De rättigheter som aktualiseras är dock inte absoluta utan de får inskränkas under vissa förutsättningar.

Som framgår i föregående avsnitt syftar rätten att söka i CIR i identifieringssyfte vid en inre utlänningskontroll till att tillgodose angelägna samhällsintressen, bl.a. att värna statens säkerhet. En möjlighet att ta fingeravtryck och fotografier skulle ta sikte endast på upptagning i de fall där det finns en rätt att göra sökningar enligt artikel 20.1–20.3. Reglerna om sökning i CIR innehåller som utvecklas i föregående avsnitt tydliga avgränsningar. Det intrång i den enskildes kroppsliga och personliga integritet som det innebär att ta fingeravtryck och fotografier bedöms uppvägas av de allmänna

intressen som åtgärden syftar till. Regler om upptagning av sådana uppgifter är alltså förenliga med Europakonventionen och EU:s rättighetsstadga. Den föreslagna åtgärden är också förenlig med regeringsformen och barnkonventionen.

Sammanfattningsvis är det ändamålsenligt och proportionerligt att införa regler om upptagande av fingeravtryck och fotografier för sökningar i CIR vid inre utlänningskontroll.

Det bör införas bestämmelser om att nationella myndigheter får söka i CIR och ta upp biometriska uppgifter för en sådan sökning i samband med en inre utlänningskontroll

Mot bakgrund av vad som framgår ovan bör det införas bestämmelser om att Polismyndigheten, Säkerhetspolisen och Kustbevakningen får söka i CIR i samband med en inre utlänningskontroll och att en utlänning är skyldig att lämna biometriska uppgifter för en sådan sökning.

Det är fråga om en skyldighet för enskilda att lämna biometriska uppgifter i form av fingeravtryck och fotografier (jfr artikel 4.11 i IOF). En sådan skyldighet måste regleras i lag (jfr avsnitt 4.2).

Enligt artikel 20.1 första stycket får sökningar i CIR utföras endast under vissa angivna förutsättningar när det finns identifieringssvårigheter. Av artikel 20.2 framgår att om någon av dessa förutsättningar uppstår får en polismyndighet söka i CIR i identifieringssyfte med biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro. I artikel 20.3 finns regler om sökningen och åtkomst till uppgifter i CIR.

Medlemsstater som vill utnyttja möjligheten till sökningar enligt artikel 20.2 ska anta nationella lagstiftningsåtgärder (artikel 20.5). Även om det förutsätts nationella lagstiftningsåtgärder för att sökningar enligt artikel 20 ska kunna göras behöver bestämmelsen i sig inte införlivas i svensk rätt för att vara tillämplig. Artikel 20 ska likställas med svensk lag under förutsättning att Sverige genom lagstiftningsåtgärder valt att utnyttja möjligheten till sökningar i identifieringssyfte. Om så har skett bedöms de kriterier för sökningar i CIR i identifieringssyfte som anges i artikel 20.1–20.3 vara direkt tillämpliga och behöver därför inte återges i nationell författning (se även avsnitt 9.3).

Det bör därför komma till uttryck i lagbestämmelsen att sökning i CIR och upptagande av biometriska uppgifter för det ändamålet får ske enligt artikel 20.1–20.3.

Vidare ska i de lagstiftningsåtgärder som avses i artikel 20.5 anges de exakta syftena med identifieringen inom ramen för bl.a. målet att bidra till att förebygga och bekämpa olaglig invandring. Dessutom ska de behöriga polismyndigheterna utses och förfaranden, villkor och kriterier för sådana kontroller fastställas i lagstiftningsåtgärderna. Hänsyn ska vidare tas till att ingen diskriminering av tredjelandsmedborgare får förekomma (artikel 20.5).

Syftet med identifieringen är att kontrollera utlänningens rätt att vistas i landet. Förordningarnas krav på att förfaranden, villkor och kriterier ska fastställas motsvaras för inre utlänningskontroller framför allt av bestämmelser i 9 kap. utlänningslagen, 8 och 10 §§ polislagen, 6 kap. kustbevakningslagen (2019:32) och Rikspolisstyrelsens föreskrifter och allmänna råd om Polisens inre utlänningskontroll (RPSFS 2011:4, FAP 273-1). Det behövs inga ytterligare nationella regler. För svenska myndigheter följer redan ett förbud mot diskriminering av gällande rätt (se t.ex. 1 kap. 9 § RF och 5 § andra stycket förvaltningslagen [2017:900]). Kravet på att hänsyn ska tas till att ingen diskriminering av tredjelandsmedborgare får förekomma bedöms därför vara tillgodosett genom befintligt regelverk.

Sammantaget bör det införas en bestämmelse om att en polisman eller en tjänsteman vid Kustbevakningen får söka enligt artikel 20.1–20.3 i IOF vid en inre utlänningskontroll. Vidare bör gälla att en utlänning är skyldig att låta en polisman eller en tjänsteman vid Kustbevakningen fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning. De nya bestämmelserna bör placeras i 9 kap. UtlL tillsammans med bestämmelserna om att ta fotografier och fingeravtryck.

I IOF finns en bestämmelse som begränsar möjligheten till sökningar i CIR när det gäller barn under tolv år. I artikel 20.1 andra stycket anges nämligen att sökningar i CIR i identifieringssyfte inte ska tillåtas när det gäller minderåriga under tolv år, såvida det inte sker för barnets bästa. Den föreslagna bestämmelsen om en rätt för myndigheterna att söka i CIR enligt artikel 20.1–20.3 och en skyldighet för utlänningar att för det ändamålet låta sig fotograferas

och lämna fingeravtryck innebär att skyldigheten för barn under tolv år att låta sig fotograferas och lämna fingeravtryck samt bli föremål för sökningar i CIR är begränsad till situationer när det är för barnets bästa. Det är därför inte nödvändigt med någon särskild bestämmelse om begränsning av skyldigheten att lämna biometriska uppgifter för barn under tolv år.

9.5.2 Verkställighet av beslut om avvisning och utvisning enligt utlänningslagen

Förslag: En polisman ska i ett ärende om verkställighet av ett beslut om avvisning eller utvisning enligt utlänningslagen få genomföra en sökning i identifieringssyfte i den gemensamma databasen för id-uppgifter. En utlänning ska vara skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

Skälen för förslaget

Det finns skäl att ge nationella myndigheter rätt att söka i CIR i ärenden om verkställighet av beslut om avvisning och utvisning

Artikel 20 i IOF innebär att en polismyndighet kan ges rätt att söka i CIR med en persons biometriska uppgifter som tagits direkt under en identitetskontroll. Det bör övervägas om svenska myndigheter bör ges rätt att utföra sådana sökningar i ärenden om verkställighet av beslut om avvisning och utvisning enligt utlänningslagen.

Verkställighet av beslut om avvisning och utvisning regleras i 12 kap. UtlL. Ett beslut om avvisning eller utvisning ska anses verkställt, om utlänningen har lämnat landet (12 kap. 21 § UtlL). Som utgångspunkt ska ett beslut om avvisning eller utvisning verkställas av Migrationsverket. Från denna huvudregel finns ett antal undantag. Polismyndigheten ska verkställa sina egna beslut om avvisning, en allmän domstols beslut om utvisning på grund av brott och beslut om avvisning eller utvisning som ska verkställas på nytt enligt 23 § första stycket UtlL. Dessutom får Migrationsverket

lämna över ett avvisnings- eller utvisningsärende för verkställighet till Polismyndigheten, om den som ska avvisas eller utvisas håller sig undan och inte kan anträffas utan myndighetens medverkan eller om det kan antas att tvång kommer att behövas för att verkställa beslutet (12 kap. 14 § UtlL).

Utlänningslagen innehåller en särskild bestämmelse om verkställighet av beslut om avvisning eller utvisning i säkerhetsärenden. Säkerhetsärenden är ärenden där Säkerhetspolisen av skäl som rör rikets säkerhet eller som annars har betydelse för allmän säkerhet förordar en viss utgång i ett ärende, t.ex. att en utlänning ska avvisas eller utvisas (1 kap. 7 § UtlL). Det är fråga om sådana säkerhetsärenden på vilka lagen (2022:700) om särskild kontroll av vissa utlänningar inte är tillämplig (se vidare nästa avsnitt). Som huvudregel ska Säkerhetspolisen verkställa beslut om avvisning eller utvisning i säkerhetsärenden. Migrationsverket eller den domstol som avgör ett säkerhetsärende får dock, i beslutet om avvisning eller utvisning, bestämma att en annan myndighet ska ombesörja verkställigheten (12 kap. 14 § andra stycket UtlL).

I betänkandet Ett effektivare regelverk för utlänningsärenden med säkerhetsaspekter (SOU 2020:16) lämnas förslag till ändringar av definitionen av säkerhetsärenden och ansvarsfördelningen mellan myndigheter. Betänkandet har remitterats och förslagen bereds inom Justitiedepartementet. Ett eventuellt genomförande av förslagen bedöms inte påverka de bedömningar som görs i detta avsnitt.

Varken bestämmelserna i 9 kap. UtlL eller de underliggande rättsakterna ger i dag någon sökmöjlighet som motsvarar möjligheten att enligt artikel 20 söka med fingeravtryck och fotografi mot uppgifter från flera olika EU-informationssystem, för att förbereda verkställigheten av ett beslut om avvisning eller utvisning.

För att upprätthålla den reglerade invandringen är det nödvändigt att beslut om avvisning och utvisning kan verkställas. Verkställigheten av sådana beslut är också en förutsättning för en hållbar migrationspolitik och ett effektivt återvändandearbete. Det är även angeläget ur ett säkerhetsperspektiv att personer som inte har rätt att vistas i landet kan avlägsnas härifrån. Det gäller inte minst när det är fråga om säkerhetsärenden, där avlägsnande sker med hänsyn till rikets säkerhet eller upprätthållande av allmän ordning.

För att myndigheterna ska kunna verkställa ett beslut om avvisning eller utvisning krävs i regel att utlänningens identitet kan klarläggas. Identiteten har betydelse för mottagarlandets möjlighet och vilja att ta emot personen och utfärda resehandlingar (jfr prop. 2020/21:159 s. 10). Ett vanligt förekommande problem inom ramen för Polismyndighetens och Säkerhetspolisens arbete med att verkställa ett beslut om avvisning eller utvisning är dock att det råder osäkerhet om utlänningens identitet eller hans eller hennes medborgarskap (jfr prop. 2016/17:191 s. 25, i vilken det inte lämnades några förslag om upptagande av biometriska uppgifter och sökningar med dessa). Polismyndigheten lägger ned omfattande resurser på att utreda identiteter och använda polisiära befogenheter, som spaning eller brukande av tvångsmedel, för att fastställa identiteteten på personer med beslut om avvisning eller utvisning som ska verkställas.

Svenska myndigheter kan ges rätt att utföra sökningar i CIR enligt artikel 20 i fem angivna situationer som kan vara aktuella vid svårigheter att identifiera en person i samband med verkställighet av ett beslut om avvisning eller utvisning (se artikel 20.1 och avsnitt 9.5.1). En sökning i CIR med en persons fingeravtryck eller fotografi skulle i sådana situationer vara ett viktigt verktyg för att kunna identifiera personen i fråga.

I många fall skulle en sådan sökning kunna bidra till en snabbare och säkrare identifiering och samtidigt minska behovet av andra mer ingripande och tidskrävande åtgärder för att klarlägga identiteten. I dag finns vissa möjligheter att besluta om förvar eller omhändertagande av en utlänning i samband med verkställighet av ett beslut om avvisning eller utvisning när det råder oklarhet kring identiteten (se 10 kap. respektive 9 kap. 12 § UtlL). En möjlighet att utreda identiteten genom en sökning i CIR skulle kunna innebära färre frihetsberövanden i syfte att klarlägga identiteten. Det framstår som mindre ingripande för den enskilde, samtidigt som det kan innebära lägre kostnader för samhället för exempelvis förvarsplatser. Det bör också framhållas att verkställande myndigheter redan i dag behandlar personuppgifter i samband med verkställighet av beslut om avvisning och utvisning enligt utlänningslagen.

En reglering som ger rätt för myndigheter att göra sökningar i CIR skulle innebära personuppgiftsbehandling. Av samma skäl som anges i avsnitt 9.5.1 bedöms det vara förenligt med de regler om

grundläggande fri- och rättigheter som anges där och artikel 9 i dataskyddsförordningen att införa en sådan möjlighet.

Verkställighet av beslut om avvisning och utvisning bedöms ligga inom ramen för målet att bidra till att förebygga och bekämpa olaglig invandring (se artiklarna 2.1 b och 20.5 i IOF).

Som framgår i avsnitt 9.5.1 ska bl.a. Polismyndigheten och Säkerhetspolisen anses vara polismyndigheter enligt IOF:s definition och de kan därmed ges rätt att söka i CIR enligt artikel 20. Migrationsverket ryms däremot inte inom definitionen och kan därför inte ges sådan rätt.

Starka skäl talar därför för att det bör införas en rätt för Polismyndigheten och Säkerhetspolisen att söka i CIR i ärenden om verkställighet av beslut om avvisning och utvisning.

En förutsättning för att kunna söka i CIR enligt artikel 20.1–20.3 är dock att det finns en möjlighet att ta upp biometriska uppgifter för detta ändamål. Frågan om upptagning av biometriska uppgifter behandlas i följande avsnitt.

Det är ändamålsenligt och proportionerligt att införa regler om upptagande av fingeravtryck och fotografier för sökningar i CIR

För att kunna utnyttja möjligheten att söka i CIR enligt artikel 20.1–20.3 i IOF i ett ärende om avvisning eller utvisning krävs att det enligt nationell rätt finns en möjlighet att ta upp biometriska uppgifter i form av fingeravtryck och fotografier som får användas för det ändamålet (jfr avsnitt 9.5.1).

I utlänningslagen finns bestämmelser om tvångsåtgärder i samband med verkställigheten av ett beslut om avvisning eller utvisning. En utlänning som har fyllt 18 år får tas i förvar om det är fråga om att förbereda eller genomföra verkställigheten av ett beslut om avvisning eller utvisning om det annars finns en risk att utlänningen bedriver brottslig verksamhet i Sverige, avviker, håller sig undan eller på annat sätt hindrar verkställigheten (10 kap. 1 § andra stycket 3 och tredje stycket UtlL). Vid bedömningen av om det finns risk för att en utlänning avviker får det bl.a. beaktas om utlänningen har uppträtt under någon identitet som var felaktig eller inte har medverkat till att klarlägga sin identitet och därigenom försvårat prövningen av sin ansökan om uppehållstillstånd (1 kap.

15 § UtlL). Under vissa, mer begränsande, förutsättningar får även barn tas i förvar enligt 10 kap. 2 § UtlL.

Migrationsverket eller Polismyndigheten får fotografera en utlänning och, om utlänningen har fyllt 14 år, ta hans eller hennes fingeravtryck om det finns grund för att besluta om förvar (9 kap. 8 § första stycket 3 UtlL). Det finns således viss möjlighet redan i dag att fotografera en utlänning eller ta dennes fingeravtryck i samband med verkställighet av beslut om avvisning eller utvisning. Det finns dock ingen rättslig grund för att ta fingeravtryck eller fotografi av en utlänning i syfte att använda dem för att söka i CIR i ett ärende om verkställighet. Bestämmelsen i 9 kap. 8 § första stycket 3 förutsätter att villkoren för förvar är uppfyllda. Dessutom motsvarar åldersgränsen på 14 år inte förordningarnas åldersgräns för sökningar (jfr artikel 20.1 andra stycket). De myndigheter som får ta upp biometriska uppgifter enligt bestämmelsen motsvarar därtill inte de myndigheter som kan vara aktuella för att ta upp sådana uppgifter för sökningar i CIR.

De befintliga bestämmelserna i utlänningslagen kan alltså inte tillämpas för att ta de fingeravtryck och fotografier som är nödvändiga för att möjliggöra sökningar i CIR. För att möjliggöra sådana sökningar krävs alltså att det införs nya bestämmelser om upptagande av biometriska uppgifter vilket aktualiserar frågor om enskildas grundläggande fri- och rättigheter. Av samma skäl som anges i avsnitt 9.5.1 bedöms det vara förenligt med de regler om grundläggande fri- och rättigheter som redogörs för där, och proportionerligt, att införa sådana bestämmelser.

Sammanfattningsvis är det ändamålsenligt och proportionerligt att införa regler om upptagande av fingeravtryck och fotografier för sökningar i CIR i ärenden om verkställighet av beslut om avvisning och utvisning.

Det bör införas bestämmelser om att nationella myndigheter får söka i CIR och ta upp biometriska uppgifter för en sådan sökning i ett ärende om verkställighet av beslut om avvisning och utvisning

Mot bakgrund av vad som framgår ovan bör det införas bestämmelser om att Polismyndigheten och Säkerhetspolisen får söka i CIR i ett ärende om verkställighet av beslut om avvisning eller utvisning och att en utlänning är skyldig att lämna biometriska

uppgifter för en sådan sökning. I enlighet med vad som anges i avsnitt 9.5.1 bör detta regleras på lagnivå.

I lagbestämmelsen bör det komma till uttryck att sökning i CIR och upptagande av biometriska uppgifter för det ändamålet får ske enligt artikel 20.1–20.3 (jfr avsnitt 9.5.1). Vidare bör uttrycket fotografera användas även här.

Förordningarna ställer upp vissa krav i fråga om medlemsstaternas lagstiftningsåtgärder (se artikel 20.5 och avsnitt 9.5.1). Syftet med identifieringen är att kunna genomföra verkställigheten av ett beslut om avvisning eller utvisning. Förordningarnas krav på att förfaranden, villkor och kriterier ska fastställas motsvaras för kontroller inom ramen för ärenden om verkställighet framför allt av bestämmelser i 12 kap. utlänningslagen, 8 och 10 §§ polislagen och Rikspolisstyrelsens föreskrifter och allmänna råd om verkställighet av beslut om avvisning och utvisning (RPSFS 2014:8, FAP 638-1). Det behövs inga ytterligare nationella regler. För svenska myndigheter följer redan ett förbud mot diskriminering av gällande rätt (se t.ex. 1 kap. 9 § RF och 5 § andra stycket förvaltningslagen). Kravet på att hänsyn ska tas till att ingen diskriminering av tredjelandsmedborgare får förekomma bedöms därför vara tillgodosett genom befintligt regelverk.

Sammantaget bör det införas en bestämmelse om att en polisman i ett ärende om verkställighet av ett beslut om avvisning eller utvisning får genomföra en sökning enligt artikel 20.1–20.3 i IOF. Vidare bör gälla att en utlänning är skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning. De nya bestämmelserna bör placeras i 9 kap. UtlL. Det bedöms, av samma skäl som anges i avsnitt 9.5.1, inte vara nödvändigt med någon särskild bestämmelse om begränsning av skyldigheten att lämna biometriska uppgifter för barn under 12 år.

9.5.3 Verkställighet av beslut om utvisning i kvalificerade säkerhetsärenden

Förslag: En polisman ska i ett ärende om verkställighet av ett beslut om utvisning enligt lagen om särskild kontroll av vissa utlänningar få genomföra en sökning i identifieringssyfte i den gemensamma databasen för id-uppgifter. En utlänning ska vara skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

Skälen för förslaget

Det finns skäl att ge nationella myndigheter rätt att söka i CIR vid verkställighet av beslut om utvisning i kvalificerade säkerhetsärenden

Artikel 20 i IOF innebär att en polismyndighet kan ges rätt att söka i CIR med en persons biometriska uppgifter som tagits direkt under en identitetskontroll. Det bör övervägas om svenska myndigheter bör ges rätt att utföra sådana sökningar vid verkställighet av beslut om utvisning i kvalificerade säkerhetsärenden.

Vid sidan av utlänningslagen finns lagen om särskild kontroll av vissa utlänningar som reglerar de mer kvalificerade säkerhetsärendena. Lagen trädde i kraft den 1 juli 2022 och ersätter lagen (1991:572) om särskild utlänningskontroll.

En utlänning ska enligt lagen få utvisas ur Sverige om utlänningen med hänsyn till vad som är känt om hans eller hennes tidigare verksamhet och övriga omständigheter kan antas komma att begå eller på annat sätt medverka till ett brott enligt terroristbrottslagen (2022:666), eller om utlänningen kan utgöra ett allvarligt hot mot Sveriges säkerhet (2 kap. 1 §). En ansökan om utvisning ska ges in av Säkerhetspolisen till Migrationsverket, som beslutar i frågan (2 kap. 2 § första stycket).

Ett beslut om utvisning ska verkställas av Säkerhetspolisen. Säkerhetspolisen får uppdra åt Polismyndigheten att genomföra verkställigheten, vilket dock inte innebär att Säkerhetspolisens ansvar som verkställande myndighet övergår till Polismyndigheten (2 kap. 11 §). Enligt förarbetena kan uppdraget till Polismyndig-

heten ha olika omfattning, allt från att enbart sköta den rent praktiska delen med att ha hand om resehandlingar och följa med utlänningen på utresan till att ha nödvändiga kontakter med myndigheterna i det land som utlänningen ska utvisas till. Säkerhetspolisen bör inte lämna uppdraget till Polismyndigheten alltför tidigt i verkställighetsprocessen, utan arbetet med verkställigheten bör som regel ha kommit så långt att eventuella verkställighetshinder är utredda och den faktiska verkställigheten är relativt nära förestående (prop. 2021/22:131 s. 89).

Varken bestämmelserna i lagen om särskild kontroll av vissa utlänningar eller de underliggande rättsakterna ger i dag någon sökmöjlighet som motsvarar möjligheten att enligt artikel 20 söka med fingeravtryck och fotografi mot uppgifter från flera olika EU-informationssystem, för att förbereda verkställigheten av ett beslut om utvisning i ett kvalificerat säkerhetsärende.

Det är mycket angeläget att beslut om utvisning i kvalificerade säkerhetsärenden kan verkställas. De skäl som motiverar en effektiv hantering av verkställighet av beslut om avvisning eller utvisning och en möjlighet till sökning i CIR i säkerhetsärenden enligt utlänningslagen gör sig gällande med ännu större styrka när det gäller sådana utlänningar som kan antas komma att begå eller på annat sätt medverka till brott enligt terroristbrottslagen eller utgör ett allvarligt hot mot Sveriges säkerhet.

En reglering som ger rätt för myndigheter att göra sökningar i CIR skulle innebära personuppgiftsbehandling. Av samma skäl som anges i avsnitt 9.5.1 bedöms det vara förenligt med de regler om grundläggande fri- och rättigheter som redogörs för där att införa en sådan möjlighet.

Verkställighet av beslut om utvisning i kvalificerade säkerhetsärenden bedöms ligga inom ramen både för målet att bidra till att förebygga och bekämpa olaglig invandring och att bidra till en hög säkerhetsnivå inom området med frihet säkerhet och rättvisa i unionen, bl.a. att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier (se artiklarna 2.1 b, 2.1 c och 20.5 i IOF).

Det är Säkerhetspolisen och i vissa fall Polismyndigheten som hanterar verkställigheten av utvisningsbeslut enligt lagen om särskild kontroll av vissa utlänningar. Även om Polismyndigheten inte kommer att överta ansvaret för verkställigheten av utvisnings-

beslutet kan det uppstå behov av att kunna söka i CIR i identifieringssyfte när myndigheten har fått i uppdrag av Säkerhetspolisen att genomföra verkställigheten. Som framgår i avsnitt 9.5.1 ska både Polismyndigheten och Säkerhetspolisen anses vara polismyndigheter enligt IOF:s definition och de kan därmed ges rätt att söka i CIR enligt artikel 20.

Starka skäl talar därför för att det bör införas en rätt för Säkerhetspolisen och Polismyndigheten att söka i CIR vid verkställighet av beslut om utvisning som fattats enligt lagen om särskild kontroll av vissa utlänningar.

En förutsättning för att kunna söka i CIR enligt artikel 20.1–20.3 är dock att det finns en möjlighet att ta upp biometriska uppgifter för detta ändamål. Frågan om upptagning av biometriska uppgifter behandlas i följande avsnitt.

Det är ändamålsenligt och proportionerligt att införa regler om upptagande av fingeravtryck och fotografier för sökningar i CIR

För att kunna utnyttja möjligheten att söka i CIR enligt artikel 20.1–20.3 i IOF i ett kvalificerat säkerhetsärende krävs att det enligt nationell rätt finns en möjlighet att ta upp biometriska uppgifter i form av fingeravtryck och fotografier som får användas för det ändamålet (jfr avsnitt 9.5.1).

I lagen om särskild kontroll av vissa utlänningar finns ett antal möjligheter att vidta tvångsåtgärder i samband med verkställigheten av ett beslut om utvisning. En utlänning som har fyllt 18 år får tas i förvar om det finns ett beslut om utvisning och förvar behövs för att förbereda eller genomföra verkställighet av beslutet förutsatt att det finns anledning att anta att utlänningen annars avviker, håller sig undan eller på annat sätt hindrar verkställigheten eller utövar brottslig verksamhet i Sverige, eller att utlänningens identitet är oklar (3 kap. 1 §). Vidare får även personer under 18 år tas i förvar under vissa omständigheter (3 kap. 2 §).

När ett beslut om utvisning enligt lagen ska verkställas får utlänningen omhändertas av Säkerhetspolisen, eller i förekommande fall Polismyndigheten, om det är nödvändigt för att verkställigheten av beslutet ska kunna förberedas eller genomföras (5 kap. 29 § första stycket). Vidare gäller att när en utlänning har omhändertagits enligt 5 kap. 29 § eller har tagits i förvar enligt 3 kap. 1 eller 2 § för att

verkställigheten av ett beslut om utvisning ska kunna förberedas eller genomföras, får Säkerhetspolisen eller Polismyndigheten vidta sådana åtgärder som behövs för att utlänningen ska få nödvändiga handlingar för verkställigheten eller för att utlänningens identitet eller medborgarskap ska kunna klarläggas. Säkerhetspolisen eller Polismyndigheten får också ta fingeravtryck av och fotografera utlänningen i ett sådant syfte (5 kap. 30 §).

Dessutom får Migrationsverket ta fingeravtryck av och fotografera utlänningen när en utlännings rätt att vistas i Sverige handläggs enligt lagen. Om utlänningen inte samarbetar får Migrationsverket begära hjälp av Polismyndigheten eller Säkerhetspolisen med att verkställa beslutet (5 kap. 28 §).

Möjligheten för Säkerhetspolisen och Polismyndigheten att ta upp biometriska uppgifter enligt 5 kap. 30 § är begränsad till situationer där utlänningen är tagen i förvar eller omhändertagen och kan därmed inte tillämpas i alla situationer där sökningar enligt artikel 20 kan aktualiseras. Vidare ger 5 kap. 28 § endast Migrationsverket rätt att ta biometriska uppgifter. Migrationsverket kan dock inte ges rätt att söka i CIR enligt artikel 20 eftersom myndigheten inte kan anses vara en polismyndighet (jfr avsnitt 9.5.1).

Bestämmelserna i lagen om särskild kontroll av vissa utlänningar kan alltså inte tillämpas för att ta de fingeravtryck och fotografier som är nödvändiga för att möjliggöra sökningar i CIR. För att möjliggöra sådana sökningar krävs att det införs nya bestämmelser om upptagande av biometriska uppgifter, vilket aktualiserar frågor om enskildas grundläggande fri- och rättigheter. Av samma skäl som anges i avsnitt 9.5.1 bedöms det vara förenligt med de regler om grundläggande fri- och rättigheter som redogörs för där, och proportionerligt, att införa sådana bestämmelser.

Sammanfattningsvis är det ändamålsenligt och proportionerligt att införa regler om upptagande av fingeravtryck och fotografier för sökningar i CIR vid verkställighet av beslut om utvisning som fattats enligt lagen om särskild kontroll av vissa utlänningar.

Det bör införas bestämmelser om att nationella myndigheter får söka i CIR och ta upp biometriska uppgifter för en sådan sökning vid verkställighet av beslut om utvisning i ett kvalificerat säkerhetsärende

Mot bakgrund av vad som framgår ovan bör det införas bestämmelser om att Säkerhetspolisen och Polismyndigheten får söka i CIR vid verkställighet av beslut om utvisning i ett kvalificerat säkerhetsärende och att en utlänning är skyldig att lämna biometriska uppgifter för en sådan sökning. I enlighet med vad som anges i avsnitt 9.5.1 bör detta regleras på lagnivå.

I lagbestämmelsen bör det komma till uttryck att sökning i CIR och upptagande av biometriska uppgifter för det ändamålet får ske enligt artikel 20.1–20.3 (jfr avsnitt 9.5.1). Vidare bör uttrycket fotografera användas även här.

IOF ställer upp vissa krav i fråga om medlemsstaternas lagstiftningsåtgärder (se artikel 20.5 och avsnitt 9.5.1) Syftet med identifieringen är att kunna genomföra verkställigheten av ett beslut om utvisning. Förordningarnas krav på att förfaranden, villkor och kriterier ska fastställas motsvaras för kontroller inom ramen för ärenden om verkställighet framför allt av bestämmelser i 1 kap. 8 § och 2 kap. lagen om särskild kontroll av vissa utlänningar och 8 och 10 §§ polislagen. Det behövs inga ytterligare nationella regler. För svenska myndigheter följer redan ett förbud mot diskriminering av gällande rätt (se t.ex. 1 kap. 9 § RF och 5 § andra stycket förvaltningslagen). Kravet på att hänsyn ska tas till att ingen diskriminering av tredjelandsmedborgare får förekomma bedöms därför vara tillgodosett genom befintligt regelverk.

En utgångspunkt för lagen om särskild kontroll av vissa utlänningar har varit att så långt det är möjligt undvika hänvisningar till utlänningslagens bestämmelser och i stället samla reglerna i den nya lagen, bl.a. för att göra regleringen mer sammanhållen och tydlig (se prop. 2021/22:131 s. 61 f.). Bestämmelserna bör därför införas i lagen om särskild kontroll av vissa utlänningar.

Sammantaget bör det införas en bestämmelse om att en polisman i ett ärende om verkställighet av ett beslut om utvisning får genomföra en sökning enligt artikel 20.1–20.3 i IOF. Vidare bör gälla att en utlänning är skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning. Bestämmelserna bör placeras i 5 kap. i lagen om

särskild kontroll av vissa utlänningar. Det bedöms, av samma skäl som anges i avsnitt 9.5.1, inte vara nödvändigt med någon särskild bestämmelse om begränsning av skyldigheten att lämna biometriska uppgifter för barn under 12 år.

9.5.4 In- och utresekontroller

Bedömning: Det bör inte införas någon rätt för nationella myndigheter att genomföra sökningar i identifieringssyfte i den gemensamma databasen för id-uppgifter i samband med in- och utresekontroller.

Skälen för bedömningen: Kontroll av personer i samband med in- och utresa regleras i gränskodexen. Det finns bestämmelser som kompletterar gränskodexen i utlänningslagen. I Sverige ansvarar Polismyndigheten för kontroll av personer enligt gränskodexen. Tullverket och Kustbevakningen är skyldiga att hjälpa Polismyndigheten vid en sådan kontroll och Migrationsverket får efter överenskommelse med Polismyndigheten hjälpa till vid kontrollen. Kustbevakningen ska dessutom medverka i Polismyndighetens kontrollverksamhet genom att utöva kontroll av sjötrafiken (9 kap. 1 § UtlL). Frågan är då om det bör införas en rätt för nationella myndigheter att söka i CIR enligt artikel 20.1–20.3 i IOF vid sådana kontroller.

När medlemsstaterna antar nationell lagstiftning för att möjliggöra sökningar i CIR i identifieringssyfte enligt artikel 20.2 ska de ange de exakta syftena med identifieringen inom ramen för de mål som avses i artikel 2.1 b och 2.1 c i IOF (artikel 20.5). Dessa målbestämmelser anger alltså ramen för vilken typ av sökningar i CIR i identifieringssyfte som kan tillåtas i nationell rätt. För att sökningar i CIR i identifieringssyfte ska kunna möjliggöras i samband med in- och utresekontroller krävs därmed att sådana kontroller ryms inom nyss nämnda mål. Enligt bestämmelserna har förordningarna som mål att bidra till att förebygga och bekämpa olaglig invandring (artikel 2.1 b) och att bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i

unionen, bland annat att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier (artikel 2.1 c).

Det går visserligen att argumentera för att sökningar i samband med in- och utresekontroller bidrar till att förebygga och bekämpa olaglig invandring och därmed faller inom ramen för målet i artikel 2.1 b. Något som talar mot detta är dock att in- och utresekontroller omfattas av en annan målbestämmelse, till vilken artikel 20.5 inte hänvisar. Av artikel 2.1 a framgår nämligen att ett av förordningarnas mål är att förbättra ändamålsenligheten och effektiviteten hos in- och utresekontrollerna vid de yttre gränserna. Den omständigheten att artikel 20.5 inte hänvisar till denna bestämmelse talar alltså för tolkningen att artikel 20 inte är avsedd att tillämpas för sökningar i CIR vid in- och utresekontroller.

Det kan dessutom ifrågasättas om det finns något behov av att kunna göra sökningar i CIR i identifieringssyfte i samband med in- och utresekontroller. Det finns nämligen redan enligt befintligt regelverk möjligheter att göra sökningar i flera av de underliggande systemen i samband med in- och utresekontroller, bl.a. de som beskrivs nedan.

Vid in- och utresa ska tredjelandsmedborgare genomgå noggranna kontroller som ska omfatta kontroll av villkoren för inresa enligt gränskodexen och i förekommande fall kontroll av de handlingar som ger tillstånd till vistelse och utövande av yrkesverksamhet. Detta ska bl.a. innefatta verifiering av tredjelandsmedborgarens identitet och nationalitet genom sökning i SIS och andra relevanta databaser. Även in- och utresekontroller av personer med rätt till fri rörlighet ska omfatta sådan verifiering (artikel 8.2, 8.3 a och 8.3 g i gränskodexen). Om tredjelandsmedborgaren innehar visering i enlighet med artikel 6.1 b i gränskodexen, ska inresekontrollen som utgångspunkt även omfatta verifikation av viseringsinnehavarens identitet och av viseringens äkthet, genom sökning i VIS i enlighet med artikel 18 i VIS-förordningen (artikel 8.3 b i gränskodexen).

Gränskodexen har reviderats i samband med antagandet av in- och utreseförordningen. I och med detta införs vissa nya moment i de in- och utresekontroller som ska göras enligt artikel 8 i gränskodexen. Vid gränskontroller av personer som ska registreras i in- och utresesystemet ska det enligt de nya bestämmelserna genomföras en verifiering – vilket förenklat är en slags bekräftande kontroll

– av deras identitet i enlighet med artikel 23.2 i in- och utreseförordningen och, i tillämpliga fall, en identifiering i enlighet med artikel 23.4 i samma förordning (artikel 8.2 b tredje stycket, 8.3 a iii och 8.3 g iii i gränskodexen, som införs genom artikel 1.4 i förordningen om ändring av gränskodexen). Ändringarna ska tillämpas från och med att in- och utresesystemet tas i drift (se prop. 2021/22:81).

Dessutom ska det enligt IOF inrättas en detektor för multipla identiteter som ska syfta till att underlätta identitetskontroller och bekämpa identitetsbedrägerier. I och med detta kommer det att genomföras en spårning av multipla identiteter när en personakt skapas eller uppdateras i exempelvis in- och utresesystemet i samband med en gränskontroll (se artiklarna 25.1 och 27.1 i IOF och artikel 14 i in- och utreseförordningen). Vissa av de uppgifter som registreras, bl.a. biometriska uppgifter och identitetsuppgifter, kommer då att jämföras med de uppgifter som redan finns i CIR och SIS. Beroende på resultatet av genomförd spårning kommer ansvariga myndigheter att kunna få åtkomst till uppgifter i CIR och SIS i syfte att verifiera olika identiteter eller bekämpa identitetsbedrägerier (se artiklarna 21 och 27.2–27.5 i IOF och artikel 34.1 g i gränsförordningen). Spårningen av multipla identiteter beskrivs närmare i avsnitt 10.

Det bedöms att det med hänsyn till de nu redovisade möjligheterna till sökningar och åtkomst till information från olika EU-informationssystemen inte finns något behov för de nationella myndigheterna att kunna söka i CIR enligt artikel 20.1–20.3 i samband med in- eller utresekontroller.

Promemorians bedömning är sammantaget att det inte bör införas någon möjlighet för nationella myndigheter att genomföra sökningar enligt artikel 20.1–20.3 i IOF i samband med in- och utresekontroller.

9.6 Sökningar enligt artikel 20 i IOF vid naturkatastrofer, olyckor och terrordåd

Förslag: Det ska i lagen om internationellt polisiärt samarbete föreskrivas att de myndigheter som regeringen bestämmer ska få genomföra sökningar i den gemensamma databasen för id-uppgifter om det behövs för att fastställa en avlidens identitet i samband med en naturkatastrof, olycka eller terrordåd. Sådana sökningar får genomföras med fotografi eller fingeravtryck som tagits vid en rättsmedicinsk undersökning. Det ska i förordning anges att Polismyndigheten, Säkerhetspolisen och Rättsmedicinalverket ska vara behöriga att göra sådana sökningar.

Skälen för förslaget

Möjligheten att söka i CIR i händelse av en naturkatastrof, en olycka eller ett terrordåd måste föreskrivas i nationell rätt

Polismyndigheten har i sin hemställan anfört det finns ett behov av att få ta upp biometriska uppgifter och göra sökningar i CIR i samtliga de fall där myndigheten idag bedriver verksamhet som direkt eller indirekt innefattar att identifiera okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor i händelse av en naturkatastrof, en olycka eller ett terrordåd.

Som nämnts ovan får enligt artikel 20.4 i IOF en polismyndighet som har bemyndigats genom nationella lagstiftningsåtgärder 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. Vad som avses med begreppen naturkatastrof, olycka och terrordåd framgår inte av IOF. Någon vägledning ges inte heller i de förklarande skälen till förordningarna.

I artikel 20.6 anges vidare att de medlemsstater som vill utnyttja den möjlighet som anges i punkt 4 ska anta nationella lagstiftningsåtgärder som fastställer förfarandena, villkoren och kriterierna. För att sökningar enligt artikel 20.4 ska kunna göras krävs alltså att medlemsstaterna föreskriver detta nationellt.

Den nationella regleringen om identifiering av avlidna vid naturkatastrofer, olyckor och terrordåd

I lagen (2003:778) om skydd mot olyckor finns bestämmelser som syftar till att i hela landet bereda människors liv och hälsa samt egendom och miljö ett med hänsyn till de lokala förhållandena tillfredsställande och likvärdigt skydd mot olyckor (1 kap. 1 §). I lagen behandlas enskildas, kommuners och statens ansvar för att uppnå det syftet. Statens skyldigheter regleras särskilt i 4 kap. där bl.a. fjällräddningstjänsten (1 §), flygräddningstjänsten (2 §) och sjöräddningstjänsten (3 §) räknas upp som statens ansvar. Enligt 4 kap. 4 § lagen om skydd mot olyckor ska också i andra fall än som avses i 1–3 §§ den eller de myndigheter som regeringen bestämmer efterforska personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa. I 4 kap. 11 § förordningen (2003:789) om skydd mot olyckor anges att Polismyndigheten ansvarar för att göra sådana efterforskningar. I det ansvaret ligger bl.a. att upprätta ett program för efterforskningen. Polismyndighetens ansvar enligt nämnda förordning bör skiljas från myndighetens brottsutredande arbete. Spaningsarbete i samband med förundersökning på grund av misstanke om brott ska nämligen inte betraktas som räddningstjänst. Däremot kan det i något fall förekomma att sådan efterforskning som ska utgöra räddningstjänst blir nödvändig även i samband med brott, t.ex. om en misstänkt person befaras ha råkat ut för en olycka som gör det nödvändigt att undsätta honom eller henne. Se prop. 1991/92:70 s. 6 ff.

Enligt 1 § förordningen (1988:530) om expertgruppen för identifiering vid katastroffall ska när en större olyckshändelse eller naturkatastrof har inträffat vid behov en särskild expertgrupp hjälpa till vid identifiering av omkomna (expertgruppen för identifiering vid katastroffall). Vid identifiering i samband med katastroffall utomlands av omkomna svenska medborgare och andra personer med nära anknytning till Sverige får expertgruppen på begäran av myndigheterna på olycksplatsen också hjälpa till vid identifiering av andra personer. Enligt 2 § förordningen om expertgruppen för identifiering vid katastroffall beslutar Polismyndigheten efter samråd med Rättsmedicinalverket om att sända ut expertgruppen och om gruppens sammansättning vid katastroffall inom landet. När

ett katastroffall inträffat utomlands ska Polismyndigheten även samråda med Regeringskansliet. I expertgruppen kan polismän, rättsläkare, rättsodontologer och rättsmedicinska assistenter ingå och, om det behövs, annan lämplig personal. En företrädare för Polismyndigheten ska utses till chef för gruppen.

Vilka åtgärder som får vidtas för att identifiera en avliden i samband med en olycka eller katastrof regleras bl.a. i begravningslagen (1990:1144) och lagen (1995:832) om obduktion m.m. Vid dödsfall i Sverige ska bevis om dödsfallet (dödsbevis) och intyg om dödsorsaken utfärdas utan dröjsmål av läkare (4 kap. 2 § begravningslagen). Enligt 4 kap. 4 § första stycket nämnda lag ska den läkare som fastställt att döden har inträtt eller som i annat fall ska utfärda dödsbeviset snarast möjligt anmäla dödsfallet till Polismyndigheten om förhållandena vid ett dödsfall är sådana att det kan finnas skäl för en rättsmedicinsk undersökning enligt lagen om obduktion m.m. En polisanmälan ska alltid göras om identiteten på den avlidne inte går att fastställa (se 14 § 4 i Socialstyrelsens föreskrifter och allmänna råd om vissa åtgärder i hälso- och sjukvården vid dödsfall HSLF-FS 2015:15).

I 15 § lagen om obduktion m.m. fastslås att en rättsmedicinsk undersökning får göras om det behövs för att fastställa en avlidens identitet. En rättsmedicinsk undersökning av en avliden får enligt 13 § samma lag även göras om undersökningen kan antas vara av betydelse för utredningen av ett dödsfall som inträffat under sådana omständigheter att det inte skäligen kan bortses från möjligheten att dödsfallet har samband med ett brott. Med rättsmedicinsk undersökning avses enligt 12 § rättsmedicinsk obduktion eller rättsmedicinsk likbesiktning. Med obduktion avses att kroppen efter en avliden öppnas och undersöks invändigt (4 § första stycket). Med rättsmedicinsk likbesiktning avses en yttre undersökning av kroppen efter en avliden. Undersökningen kan innefatta blodprovstagning och andra mindre ingrepp. Med andra mindre ingrepp avses i första hand tagande av andra kroppsvätskor, hud- eller nagelbitar m.m. för laboratorie- och andra undersökningar. Undersökningen ska göras i form av rättsmedicinsk obduktion, om inte ändamålet kan tillgodoses genom rättsmedicinsk likbesiktning.

Beslut om rättsmedicinsk undersökning som avses i 13–15 §§ meddelas av Polismyndigheten (18 §) och ska utföras av läkare (20 §). Enligt 2 § 2 förordningen (2007:976) med instruktion för

Rättsmedicinalverket ansvarar den myndigheten för rättsmedicinska obduktioner och andra rättsmedicinska undersökningar.

Närmare om Polismyndighetens och Rättsmedicinalverkets samarbete

När det inträffar en stor olycka eller annan händelse med många omkomna ansvarar polisen för att identifiera de omkomna. På händelseplatsen registrerar polisen uppgifter om de personer som befunnit sig där vid det aktuella tillfället. Polisen jämför inkomna uppgifter gällande efterfrågade och anträffade personer. Detta ligger sedan till grund för det fortsatta identifieringsarbetet.

Polismyndigheten har fyra regionala ID-lag som utför identifieringsarbete inom sina respektive geografiska områden. ID-lagen finns i Umeå, Stockholm, Göteborg och Malmö och består av dels AM-team ("Ante Mortem - före döden") som tar fram uppgifter om befarat drabbade, dels PM-team ("Post Mortem - efter döden") som undersöker de anträffade kropparna. De regionala ID-lagens AM-team kontaktar anhöriga och vårdgivare för att samla in underlag, så kallade ante mortem-uppgifter, som kan hjälpa till att identifiera den omkomne. Det kan vara fingeravtryck, dna, patientjournaler och röntgenbilder från läkare och tandläkare, men även signalement som hårfärg, längd, födelsemärken, ärr och tatueringar. För att få fram ett dna behövs ett dna-prov från en nära anhörig. Provet tas på saliv från munnen med en tops. PM-teamen undersöker kropparna från de omkomna personerna och dokumenterar motsvarande uppgifter. Detta kallas post mortem-uppgifter. Uppgifterna både före och efter dödsfallet registreras i ett datasystem där de jämförs. En särskild expertgrupp gör sedan den slutgiltiga identifieringen av de omkomna personerna och utfärdar intyg när det går att konstatera att en viss kropp är en viss saknad person.

Vid en händelse i Sverige där ID-lagets resurser inte räcker till kan Nationella operativa avdelningen (NOA) vid Polismyndigheten ta över ansvaret och då aktiveras den s.k. ID-kommissionen. Beslutet att aktivera ID-kommissionen fattas av Polismyndigheten i samråd med Rättsmedicinalverket. Då samlas både AM- och PM-uppgifterna in till Nationellt DVI Center vid NOA och matchningsarbetet sker där. DVI står för Disaster Victim

Identification som är en internationell metod framtagen av Interpol och som används över hela världen för att på ett säkert sätt kunna identifiera ett större antal avlidna vid katastrofer och olyckor. Polisen och Rättsmedicinalverket samarbetar i dessa situationer för att säkerställa att arbetet sker med hög kvalitet och på ett likvärdigt sätt. Metoden har i Sverige använts ett flertal gånger, bl.a. vid terrorattentatet i Stockholm 2017 och när ett Herculesplan flög in i Kebnekaise 2012. DVI-metoden användes också vid olyckorna med fallskärmshoppare i Umeå 2019 och Örebro 2021.

Vid en händelse utomlands kan polisen, i samråd med Regeringskansliet och Rättsmedicinalverket, välja att aktivera ID-kommissionen som då ansvarar för identifieringsarbetet. Arbetet leds dock alltid av det drabbade landets myndigheter och kan göras på olika sätt beroende på i vilket land som olyckan har inträffat.

Vid större olyckor och katastrofer kan specialister inom rättsgenetik, rättsmedicin och rättsodontologi (tänder och munhåla) användas i arbetet med att identifiera avlidna. Dna-prov, fingeravtryck och tandidentifiering är de vanligaste metoderna som används. Rättsläkare, rättsodontologer och rättsgenetiker från Rättsmedicinalverket deltog i identifieringsarbetet efter bland annat tsunamin i Thailand, Estoniakatastrofen och diskoteksbranden i Göteborg.

Behovet av sökningar i CIR för att identifiera offer vid naturkatastrofer, olyckor och terrordåd

Polismyndighetens uppfattning är att det är viktigt att i nationell lagstiftning fullt ut ta vara på de möjligheter till identifiering som IOF ger, särskilt i sådana situationer som innebär de största påfrestningarna för både samhället och enskilda. För anhöriga innebär ovissheten kring vad som hänt en närstående i samband med en naturkatastrof, en olycka eller ett terrordåd en synnerligen stor påfrestning. I sådana situationer är det också extra angeläget att samhällets begränsade och då ofta hårt prövade resurser utnyttjas så effektivt som möjligt. Utifrån att IOF endast fastställer ramar för verifiering av personers identitet och för identifiering av personer finns enligt Polismyndigheten ett stort utrymme att tolka begreppen naturkatastrof och olycka på ett sätt som harmonierar med Polismyndighetens ansvar för att identifiera personer och mänskliga

kvarlevor. Polismyndighetens bedömning är sammanfattningsvis att det finns ett behov av att få ta upp biometriska uppgifter och göra sökningar i CIR i samtliga de fall där myndigheten idag bedriver verksamhet som direkt eller indirekt innefattar att identifiera okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor i händelse av en naturkatastrof, en olycka eller ett terrordåd.

Det bör införas en möjlighet för Polismyndigheten, Säkerhetspolisen och Rättsmedicinalverket att söka i CIR enligt artikel 20.4 i IOF

Det saknas skäl att ifrågasätta vad Polismyndigheten har uppgett om behovet av att kunna göra sökningar i CIR för att identifiera en avliden i samband med en olycka, naturkatastrof eller terrordåd. Sådana situationer innebär, som Polismyndigheten anger, en stor påfrestning för anhöriga, särskilt om dessa måste leva i ovisshet om en närstående person har avlidit eller inte. Vidare förutsätter begravningslagen att det vid dödsfall i Sverige ska utfärdas bevis om dödsfallet, för vilket en fastställd identitet är nödvändig. I de fall den avlidne är tredjelandsmedborgare kan det bli svårt att identifiera denna utifrån tillgängliga uppgifter i nationella register. Personen kan vidare i sådana fall sakna anhöriga i landet som kan hjälpa till att identifiera personen. Med hänsyn till att CIR kommer innehålla identitetsuppgifter på i stort sett alla tredjelandsmedborgare som rest in i Schengen kommer denna databas att kunna utgöra ett värdefullt komplement till uppgifter som finns i nationella register vid identifieringen av en avliden tredjelandsmedborgare. Visserligen kommer CIR inte att innehålla samtliga uppgifter som skulle kunna hjälpa myndigheterna i arbetet med att identifiera en avliden person. Till exempel kommer uppgifter om dna eller en persons fysiska kännetecken inte att kunna användas för sökningar i systemet. Som anförts ovan kan dock en fingeravtrycksundersökning som innebär att fingeravtryck jämförs i olika register vara ett viktigt verktyg för att kunna identifiera en avliden. Undersökningsmetoden används också redan av ansvariga myndigheter i arbetet med att identifiera avlidna.

Det finns redan idag ett rättsligt stöd i lagen om obduktion m.m. för att genomföra undersökningar i syfte att identifiera en avliden person. Reglerna får anses infatta en rätt att ta sådana biometriska

uppgifter från avlidna som krävs för att sökningar i CIR ska kunna göras enligt artikel 20.4 i IOF. Eftersom Rättsmedicinalverket är den myndighet som ansvarar för rättsmedicinska undersökningar torde det i första hand ankomma på den myndigheten att uppta nödvändiga uppgifter för identifiering av avlidna. Behandlingen omfattas då av lagen (2020:421) om Rättsmedicinalverkets behandling av personuppgifter. Enligt 1 kap. 7 § nämnda lag gäller den lagen, EU:s dataskyddsförordning, dataskyddslagen, brottsdatalagen och föreskrifter som meddelats i anslutning till dessa lagar i tillämpliga delar även vid behandling av uppgifter om avlidna i Rättsmedicinalverkets verksamhet. Det dataskyddsrättsliga regelverket tillåter sådan behandling under vissa förutsättningar (se 3 kap. 3 § nämnda lag).

Biometriska uppgifter från avlidna kan också ingå i Polismyndighetens och Säkerhetspolisens verksamhet. Som nämnts ovan finns ett nära samarbete mellan Polismyndigheten och Rättsmedicinalverket vid identifieringen av avlidna vid olyckor och katastrofer. Vidare kan rättsmedicinska uppgifter om avlidna förekomma i myndigheternas brottsutredande verksamhet, t.ex. i samband med ett terrordåd. Förekommer uppgifterna hos Polismyndigheten eller Säkerhetspolisen kommer behandlingen att ske utifrån det regelverk som gäller för respektive myndighet.

Det bedöms mot bakgrund av det ovan anförda att förfaranden, villkor och kriterier för upptagandet och behandling av biometri från avlidna i samband med de situationer som avses i artikel 20.4 i IOF framgår av befintligt regelverk. För att uppgifterna ska kunna användas för sökningar i CIR krävs dock att behöriga myndigheter pekas ut i nationell lagstiftning.

Artikel 20.4 i IOF förutsätter att sökningar utförs av en polismyndighet. Som anförts i avsnitt 9.1.2 bör som utgångspunkt begreppet polismyndighet tolkas utifrån dataskyddsdirektivets definition. Myndigheter vars uppdrag innefattar att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten torde således omfattas. Rättsmedicinalverket utför brottsutredande arbetsuppgifter (se 2 § förordningen med instruktion för Rättsmedicinalverket). Myndigheten bör således kunna ges behörighet att söka i CIR enligt artikel 20.4 i IOF.

Sammanfattningsvis bedöms det såväl möjligt som lämpligt att ge Polismyndigheten, Säkerhetspolisen och Rättsmedicinalverket behörighet att göra sökningar enligt artikel 20.4 i IOF om det behövs för att fastställa en avlidens identitet. Sådana sökningar bör få genomföras med uppgifter som tagits i samband med en rättsmedicinsk undersökning. Som förutsättning gäller enligt IOF att sådana sökningar görs i samband med en naturkatastrof, olycka eller terrordåd. Det framgår inte av IOF vad som avses med dessa begrepp. Behöriga myndigheter måste därför i det enskilda fallet bedöma om situationen är en sådan som medger rätt att genomföra sökningar, varvid begreppen får tolkas utifrån EU-rätten. Såvitt avser terrordåd kan de brottsutredande myndigheternas rubricering av eventuell brottsmisstanke vara vägledande.

I enlighet med det resonemang som förs i avsnitt 9.3 bör det i lagen om internationellt polisiärt samarbete föreskrivas en möjlighet för de myndigheter som regeringen bestämmer att utföra sökningar enligt artikel 20.4 i IOF om det behövs för att fastställa en avlidens identitet i samband med en naturkatastrof, olycka eller terrordåd. Sådana sökningar bör få genomföras med fotografi eller fingeravtryck som upptagits vid en rättsmedicinsk undersökning. Utpekandet av behöriga myndigheter bör dock ske på förordningsnivå med stöd av 8 kap. 7 § regeringsformen.

10 Detektorn för multipla identiteter

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om detektorn för multipla identiteter kräver inte några författningsändringar.

Skälen för bedömningen

Åtkomstbehörighet till uppgifter i MID följer direkt av IOF

En av de komponenter som introduceras av IOF är detektorn för multipla identiteter (MID). Enligt artikel 25.2 i IOF ska MID bestå av en central infrastruktur som lagrar länkar och hänvisningar till EU-informationssystem och en säker kommunikationsinfrastruktur som kopplar MID till SIS och ESP:s och CIR:s centrala infrastrukturer. Det är eu-LISA som ska utveckla MID och säkerställa den tekniska förvaltningen.

MID:s syfte är att upptäcka multipla identiteter i underliggande system för att underlätta identitetskontroller och bekämpa identitetsbedrägerier (artikel 25.1 i IOF). En process i MID påbörjas när uppgifter registreras, ändras eller uppdateras i ett av de underliggande systemen. I processen jämförs tillgänglig biometrisk information och andra identitetsuppgifter för att kontrollera om det redan finns uppgifter om personen i ett annat system. Utifrån vissa kriterier skapar systemet länkar i olika färger beroende på vad de indikerar. En *gul länk* innebär att systemet avvaktar en manuell verifiering av uppgifterna (artikel 30 i IOF), en *grön länk* innebär att de länkade uppgifterna avser två olika personer (artikel 31 i IOF), en *röd länk* innebär att de länkade uppgifterna på ett oberättigat sätt avser antingen samma person eller två olika personer (artikel 32 i

IOF) medan en *vit länk* exempelvis kan innebära att de länkade uppgifterna på ett berättigat sätt avser samma person (artikel 33 i IOF). Länkarna sparas i en s.k. akt med identitetsbekräftelse (artikel 34 i IOF). Akterna med identitetsbekräftelse och uppgifterna i dem, inbegripet länkarna, ska enligt artikel 35 i IOF lagras i MID endast under den tid som de länkade uppgifterna lagras i två eller fler EU-informationssystem. De ska raderas automatiskt från MID.

MID kan automatiskt skapa vita och gula länkar medan röda och gröna länkar endast kan skapas efter en manuell verifiering. Vita länkar kräver som regel inte någon åtgärd från medlemsstaternas sida. I de fall då systemet skapar en gul länk kommer medlemsstaternas myndigheter att informeras om länken. Gula länkar skapas när MID får en träff mot uppgifter som redan finns registrerade i de underliggande systemen och de länkade uppgifter inte kan anses vara lika. Som exempel kan nämnas om registreringen av ett fingeravtryck resulterar i en träff mot samma fingeravtryck i ett annat system men då övriga identitetsuppgifter inte överensstämmer. I sådant fall kommer den registrerande myndigheten att få information om länken, varvid en verifiering av de länkade uppgifterna måste göras enligt artikel 29 i IOF. Med ”verifiering” avses förfarandet att jämföra en uppsättning uppgifter med en annan för att fastställa om en påstådd identitet är riktig, s.k. one-to-one-check (se artikel 4.5 i IOF).

Rätten till åtkomst till uppgifter i MID regleras i artikel 26 i IOF. Bestämmelsen reglerar åtkomsträtt till såväl länkade uppgifter som länkarna i sig. I bestämmelsen specificeras vilka myndigheter som ska ha åtkomst till uppgifter i MID i syfte att kunna utföra den manuella verifieringen av gula länkar (artikel 26.1). Vidare finns särskilda regler om åtkomsträttigheter för röda, vita och gröna länkar (artikel 26.2–26.4).

Ovan nämna bestämmelser är direkt tillämpliga och kräver inte några nationella författningsändringar.

Ansvaret för verifieringen av gula länkar följer direkt av IOF

Vilken myndighet som ska utföra den manuella verifieringen regleras i artikel 29 i IOF. Som huvudregel ska verifieringen göras av den myndighet som har gjort den registrering eller uppdatering i de underliggande systemen som föranlett att länken skapats. För vissa länkar till känsliga registreringar i SIS är det dock alltid medlemsstaternas utsedda Sirene-kontor som ska göra kontrollen. Det kan gälla länkar till uppgifter i SIS som hör till registreringar om t.ex. eftersökta personer.

Den ansvariga myndigheten kommer vid den manuella verifieringen att bedöma de länkade uppgifterna. Beroende på utfallet av den bedömningen ska den gula länken ändras till en vit, grön eller röd länk utifrån de kriterier som framgår av förordningarna och kompletterande bestämmelser på EU-nivå. En verifiering behöver ske skyndsamt och om möjligt i personens närvaro. Det kan bli aktuellt för den verifierande myndigheten att be om klargöranden och ytterligare information från personen i fråga. När verifieringsprocessen är avklarad ansvarar myndigheten för att länken uppdateras och sparas i akten med identitetsbekräftelse.

På grund av sina uppdrag förutses Polismyndigheten stå för merparten av arbetet med att verifiera gula länkar i Sverige. Enligt 9 kap. 1 § UtlL ansvarar Polismyndigheten för kontroll av personer enligt gränskodexen. Tullverket och Kustbevakningen är skyldiga att hjälpa Polismyndigheten vid en sådan kontroll och även Migrationsverket får hjälpa till efter överenskommelse med Polismyndigheten. Regeringen har bedömt att det följer av in- och utreseförordningen och nationell rätt att dessa myndigheter är att anse som behöriga myndigheter som kommer att fungera som gränsmyndigheter i enlighet med artikel 9.2 i in- och utreseförordningen (prop. 2021/22:81 s. 22). Dessa myndigheter kommer att ansvara för verifieringen av gula länkar som uppstår när de skapar eller uppdaterar personakter i in- och utresesystemet (jfr artikel 27.1 a och 29.1 a i förordning [EU] 2019/817). Polismyndigheten föreslås utses till Etias nationella enhet i Sverige och kommer därmed att bli ansvarig för verifiering av länkar som uppstår i samband med registreringar enligt Etias-förordningen (se Ds 2021:19 och artikel 29.1 c i förordning [EU] 2019/817). Vidare är Polismyndigheten utsedd till att vara Sirene-kontor och central myndighet för Ecris (se p. 4 a och

i i bilagan till förordningen [2014:1102] med instruktion för Polismyndigheten). Myndigheten kommer därmed att ansvara för den manuella verifieringen vid registrering eller ändring av uppgifter i Ecris-TCN och skapandet eller uppdateringar av registreringar i SIS (artikel 29.1 d i förordning [EU] 2019/817 och artikel 29.1 a och b i förordning [EU] 2019/818). Såvitt avser SIS gäller att Migrationsverket framöver kommer att ansvara för att göra vissa registreringar i SIS (se 4 § andra stycket lagen med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem). Den nya lagen om SIS kommer att träda i kraft den dag regeringen bestämmer, vilket i sin tur är avhängigt den tidpunkt då det nya EU-rättsliga regelverket för SIS ska börja tillämpas fullt ut (se prop. 2020/21:222 s. 71). Av IOF följer att det är medlemsstaternas Sirenekontor som ska verifiera länkar som uppstår i samband med registrering i det systemet. Oaktat Migrationsverkets rätt att registrera uppgifter i systemet kommer det således vara Polismyndigheten i sin egenskap av Sirenekontor som ansvarar för verifieringen av gula länkar som uppstått dels vid skapandet eller uppdateringar av registreringar i SIS, dels till vissa känsliga registreringar i SIS (se artikel 29.2 i IOF).

Såvitt avser verifieringen av gula länkar som uppstår i samband med skapandet eller uppdateringen av en ansökningsakt i VIS kommer ansvaret att falla på svenska viseringsmyndigheter (se artikel 29.1 b i förordning [EU] 2019/817). Med viseringsmyndigheter avses de myndigheter som i varje medlemsstat är ansvariga för att behandla och fatta beslut om viseringsansökningar eller för beslut om huruvida viseringar ska ogiltigförklaras, återkallas eller förlängas, inbegripet de centrala viseringsmyndigheterna och de myndigheter som ansvarar för att utfärda viseringar vid gränsen (artikel 4.3 i VIS-förordningen). Av reglerna i viseringskodexen följer att de beskickningar och konsulat som utfärdar viseringar ska anses vara viseringsmyndigheter enligt nyss nämnda definition (se artiklarna 2.9 och 4.1 i viseringskodexen, jfr även prop. 2021/22:81 s. 25 f.). Polismyndigheten, som är den myndighet som utfärdar viseringar vid yttre gräns, omfattas också av definitionen (se artikel 4.2 i viseringskodexen och 9 kap. 1 § UtlL). Utöver vad som följer av viseringskodexen får beslut om Schengenvisering meddelas av Migrationsverket (3 kap. 5 § första meningen UtlL).

Vissa myndigheter, bl.a. Migrationsverket och Regeringskansliet, får meddela beslut om nationell visering (se 3 kap. 5 § andra meningen UtlL och 3 kap. 12 § utlänningsförordningen [2006:97]). En sådan visering omfattas inte av definitionen av visering enligt artikel 4.1 i VIS-förordningen. Dessa myndigheter är därmed inte att anse som viseringsmyndigheter när de hanterar ansökningar om nationell visering.

Eftersom ansvaret för verifiering av gula länkar följer direkt av IOF och gällande rätt bedöms bestämmelserna om den manuella verifieringen inte kräva några nationella författningsändringar.

Konsekvenserna av en länk regleras inte i IOF

Som ovan nämnts kommer den slutliga färgen på en länk som skapats i MID avgöras av den verifierande myndighetens bedömning av de länkade uppgifterna. Den verifierande myndigheten kan t.ex. dra slutsatsen att en person har använt olika identitetsuppgifter på ett oberättigat sätt. Då skapas en röd länk som kommer att synliggöras för de myndigheter som har åtkomst till åtminstone ett av de underliggande systemen. I vilka fall en sådan avvikelse ska anses oberättigad framgår inte av IOF.

En person vars uppgifter i olika system länkas genom en vit eller röd länk har enligt huvudregeln i artiklarna 32.4 och 33.4 i IOF rätt att underrättas om länken. Denna underrättelseskyldighet har dock vissa undantag, t.ex. om en sådan underrättelse kan äventyra en pågående utredning på nationell nivå. Vilka konsekvenser som en länk kan få för den enskilde följer i övrigt inte av IOF. Enligt artikel 32.2 i IOF ska röda länkar inte i sig få några rättsliga konsekvenser för den berörda personen. En röd länk ska enligt IOF följas upp enligt EU-rätten och nationell rätt. På vilket sätt detta ska följas upp specificeras inte i IOF. I skäl 63 till förordning (EU) 2019/817 förtydligas dock att gränskontrolltjänstemän bör beakta de identitetsuppgifter eller resehandlingsuppgifter som har lett till att en länk i MID klassificerades som en röd länk när de bedömer huruvida en person uppfyller de inresevillkor som anges i förordning (EU) 2016/399. Förekomsten av en röd länk bör dock inte i sig utgöra ett skäl för nekad inresa, och de befintliga skäl för nekad inresa som anges i förordning (EU) 2016/399 bör därför inte ändras.

Det skulle kunna uppstå fall då en länk skapas pga. att en person har använt sig av felaktiga eller falska personuppgifter eller resehandlingar. Ett sådant beteende kan få rättsverkningar för den enskilda i olika avseenden. Det kan t.ex. påverka en persons rätt att resa in i och vistas i Sverige. Vidare kan det aktualisera straffrättsligt ansvar för t.ex. urkundsförfalskning eller brukande av falsk urkund. Det är i sådant fall inte länken i MID i sig som får rättsverkningar för den enskilde utan det bakomliggande beteendet. Det går dock inte att göra en uttömmande redogörelse för i vilka situationer som svenska myndigheter ska vidta ytterligare åtgärder i samband med skapandet eller upptäckten av en röd länk. Det får anses vara upp till berörda myndigheter att i det enskilda fallet förhålla sig till informationen om en röd länk och bedöma vilka åtgärder som ska vidtas utifrån de regler som styr myndighetens verksamhet.

Kravet på registerföring av loggar följer av förordningarna

Av artikel 36.1 i IOF framgår att eu-LISA ska föra loggar över all uppgiftsbehandling i MID. Av bestämmelsen framgår även vad loggarna ska omfatta. Vidare ska varje medlemsstat föra loggar över sökningar som utförs av dess myndigheter och den personal vid dessa myndigheter som är vederbörligen bemyndigad att använda MID (artikel 36.2).

Bestämmelserna i artikel 36 är direkt tillämpliga och kräver inte några nationella författningsåtgärder.

11 Åtgärder till stöd för interoperabilitet

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om åtgärder till stöd för förmågan för underliggande system och den gemensamma databasen för id-uppgifter att utbyta uppgifter och dela information med varandra kräver inte några författningsändringar.

Skälen för bedömningen: I kapitel VI i IOF finns bestämmelser om tekniska åtgärder som ska vidtas för att stödja förmågan för underliggande system och EU:s databas för identitetsuppgifter att utbyta uppgifter och dela information med varandra. Bland annat fastslås att eu-LISA ska inrätta automatiska mekanismer och förfaranden för kontroll av kvaliteten på de uppgifter som lagras där (artikel 37). Vidare ska det inrättas en standard för ett universellt meddelandeformat (UMF). Genom UMF definieras standarder för vissa innehållselement i det gränsöverskridande informationsutbytet mellan informationssystem, myndigheter eller organisationer på området rättsliga och inrikes frågor (artikel 38).

I artikel 39 fastslås att det ska inrättas en central databas för rapporter och statistik (CRRS) för att stödja målen för in- och utresesystemet, VIS, Etias och SIS, i enlighet med de respektive rättsliga instrument som reglerar de systemen, och för att tillhandahålla systemöverskridande statistiska uppgifter och analysrapporter för politiska och operativa syften samt för uppgiftskvaliteten. Uppgifterna i CRRS ska inte möjliggöra identifiering av enskilda personer. Syftet med CRRS är att generera systemöverskridande statistiska uppgifter och analytisk rapportering för verksamhetsstyrande och operativa syften samt för uppgiftskvalitet i enlighet med tillämpliga rättsliga instrument (skäl 52). Den ska innehålla

anonymiserade statistiska uppgifter från underliggande system, CIR, MID och sBMS.

Bestämmelserna i artiklarna 37–39 är direkt tillämpliga och kräver inte författningsåtgärder på nationell nivå.

12 Dataskydd och personuppgiftsansvar

12.1 IOF:s förhållande till allmän dataskyddsreglering

Förslag: EU:s förordningar om interoperabilitet ska undantas från tillämpningsområdet för polisens brottsdatalag och utlänningsdatalagen.

Skälen för förslaget

Det allmänna dataskyddsrättsliga regelverket

Dataskyddsförordningen utgör den generella regleringen för behandling av personuppgifter inom EU. Dataskyddsförordningen kompletteras på generell nivå av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Dataskyddsförordningen är dock inte tillämplig på den behandling av personuppgifter som myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder (artikel 2.2 d). För personuppgiftsbehandling inom detta område gäller i stället dataskyddsdirektivet, som har genomförts i svensk rätt genom brottsdatalagen.

Brottsdatalagen gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet (1 kap. 2 §).

IOF:s förhållande till de allmänna dataskyddsreglerna

I IOF anges att dataskyddsförordningen är tillämplig på de nationella myndigheternas behandling av personuppgifter i interoperabilitetssyfte inom ramen för förordningarna, förutom om behandlingen görs av medlemsstaternas utsedda myndigheter eller centrala kontaktpunkter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. I dessa fall är i stället dataskyddsdirektivet – som alltså har genomförts i svensk rätt genom brottsdatalagen – tillämpligt för de nationella myndigheterna (skäl 53 och 54 i IOF).

Behandling av personuppgifter enligt IOF kan alltså omfattas antingen av dataskyddsförordningens eller av brottsdatalagens tillämpningsområde. Ett första krav för att brottsdatalagen ska vara tillämplig är att behandlingen av personuppgifter utförs av en myndighet som fullgör uppgifter inom brottsdatalagens tillämpningsområde eller annars anförtrotts myndighetsutövning i samma syften (1 kap. 2 och 6 §§ brottsdatalagen). Därutöver krävs att behandlingen av personuppgifter i det enskilda fallet sker antingen i ett brottsbekämpande syfte eller i syfte att upprätta allmän ordning och säkerhet (1 kap. 2 § och 6 §§ brottsdatalagen). Det är alltså syftet med behandlingen av personuppgiften i det enskilda fallet som är avgörande för vilken rättsakt som är tillämplig. För en mer utförlig redogörelse kring vilka principer som ska tillämpas för att bedöma om brottsdatalagen är tillämplig eller inte hänvisas till propositionen Brottsdatalag (prop. 2017/18:232 s. 111–113).

Dataskyddsförordningen är direkt tillämplig vid de nationella myndigheternas behandling av personuppgifter enligt IOF, i den mån behandlingen inte sker i syfte att förebygga, förhindra, upptäcka och utreda brott (jfr skäl 53 och 54). Dataskyddslagen innehåller bestämmelser som kompletterar dataskyddsförordningen på nationell nivå. Det bedöms inte krävas några ändringar i nationell rätt för att dataskyddslagen ska vara tillämplig även vid behandling av personuppgifter enligt IOF.

Medlemsstaterna ska enligt IOF se till att de nationella lagar, föreskrifter och administrativa bestämmelser som antas i enlighet med dataskyddsdirektivet vid behov är tillämpliga också på polismyndigheters och utsedda myndigheters åtkomst till IO-komponenterna, även med avseende på rättigheter för de personer

vars uppgifter åtkomsten gäller (artikel 51.2). Även brottsdatalagen är tillämplig vid behandling av personuppgifter enligt IOF, om behandlingen sker i syfte att förebygga, förhindra, upptäcka och utreda brott. Något behov av författningsändringar finns alltså inte i det avseendet.

IOF:s förhållande till utlänningsdatalagen och polisens brottsdatalag

Utöver dataskyddslagen finns sektorspecifika registerlagar som också utgör kompletterande regleringar till dataskyddsförordningen. Utlänningsdatalagen (2016:27) är en sådan sektorsspecifik registerlag som gäller vid behandling av personuppgifter i Migrationsverkets, Polismyndighetens och utlandsmyndigheternas verksamhet enligt utlännings- och medborgarskapslagstiftningen (1 § utlänningsdatalagen). Bestämmelserna i utlänningsdatalagen har sin grund i de särskilda behov som dessa myndigheter har av att behandla personuppgifter för sin verksamhet. Bestämmelserna innehåller specifika krav för uppgiftsbehandlingen som säkerställer en laglig och rättvis behandling av personuppgifter inom tillämpningsområdet (prop. 2017/18:254 s. 16 f.).

För den brottsbekämpande verksamheten finns ett antal registerförfattningar som kompletterar brottsdatalagen. Polisens brottsdatalag, är en sådan författning. Lagen gäller utöver brottsdatalagen vid behandling av personuppgifter i brottsbekämpande verksamhet vid bl.a. Polismyndigheten (1 kap. 1 § polisens brottsdatalag).

Personuppgiftsbehandling som sker i enlighet med IOF faller under det generella tillämpningsområdet för både polisens brottsdatalag och utlänningsdatalagen. Det kommer alltså att finnas särskilda regler om personuppgiftsbehandling i IOF, i utlänningsdatalagen och i polisens brottsdatalag.

För att undvika dubbelreglering och för att säkerställa att det inte införs en reglering som står i strid med andra regelverk har det i liknande situationer gjorts undantag från tillämpningsområdet i utlänningsdatalagen för behandling av personuppgifter som sker med stöd av andra lagar och EU-förordningar (se bl.a. 5 § utlänningsdatalagen och prop. 2017/18:254 s. 25). Vidare har det inte ansetts möjligt att reglera all Polismyndighetens personuppgifts-

behandling i polisens brottsdatalag (prop. 2017/18:269 s. 147 f). I 1 kap. 2 § polisens brottsdatalag undantas därför ett antal lagar från lagens tillämpningsområde. Av samma skäl bör sådan personuppgiftsbehandling som sker med stöd av IOF undantas från tillämpningsområdena för utlänningsdatalagen och polisens brottsdatalag. Bestämmelser med denna innebörd bör därför införas i utlänningsdatalagen och polisens brottsdatalag.

12.2 Personuppgiftsansvar

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om ansvar för personuppgiftsbehandling kräver inte några författningsändringar.

Skälen för bedömningen: I dataskyddsförordningen definieras ”personuppgiftsansvarig” som bl.a. en fysisk eller juridisk person, eller en offentlig myndighet som ensam eller tillsammans med andra bestämmer ändamålen för och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige eller de särskilda kriterierna för hur denna ska utses kan också föreskrivas i medlemsstaternas nationella rätt, om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt (artikel 4.7). I brottsdatalagen definieras ”personuppgiftsansvarig” som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (1 kap. 6 §).

I IOF finns bestämmelser om vilka myndigheter som är personuppgiftsansvariga enligt artikel 4.7 i dataskyddsförordningen eller artikel 3.8 i dataskyddsdirektivet för personuppgiftsbehandling enligt förordningarna.

För personuppgiftsbehandling i den gemensamma biometriska matchningstjänsten ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för in- och utresesystemet, VIS, Eurodac, SIS respektive Ecris-TCN vara personuppgiftsansvariga i enlighet med dataskyddsförordningen eller dataskyddsdirektivet avseende de biometriska mallar som erhållits från de uppgifter som avses i artikel 13 i förordningarna och som de för in i de underliggande systemen

och de ska ansvara för behandlingen av de biometriska mallarna i den gemensamma biometriska matchningstjänsten (artikel 40.1 i IOF).

För personuppgiftsbehandling i CIR ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för in- och utresesystemet, VIS, Etias, Eurodac respektive Ecris-TCN vara personuppgiftsansvariga avseende de uppgifter som avses i artikel 18 i förordningarna och som de för in i de underliggande systemen och de ska ansvara för behandlingen av de personuppgifterna i CIR (artikel 40.2 i IOF).

När det gäller behandling av uppgifter i MID ska Europeiska gräns- och kustbevakningsbyrån vara personuppgiftsansvarig för den behandling av personuppgifter som utförs av Etias centralenhet. Vidare ska de av medlemsstaternas myndigheter som lägger till eller ändrar uppgifter i akten med identitetsbekräftelse vara personuppgiftsansvariga och ska ansvara för behandlingen av personuppgifter i MID (artikel 40.3 i IOF).

De personuppgiftsansvariga som avses i artikel 40 ska vidta nödvändiga åtgärder för att övervaka efterlevnaden av IOF, inklusive genom frekventa kontroller av de loggar som avses i artiklarna 10, 16, 24 och 36, och vid behov samarbeta med tillsynsmyndigheterna och Europeiska datatillsynsmannen (artikel 44 andra stycket i IOF). För övervakningen av dataskyddet, inbegripet kontroll av om en sökning är tillåten och om uppgifter har behandlats på ett lagligt sätt, ska de personuppgiftsansvariga ha åtkomst till nyss nämnda loggar för egenkontroll enligt vad som avses i artikel 44 (artikel 40.4 i IOF).

När det gäller personuppgiftsbehandling i den gemensamma biometriska matchningstjänsten, CIR och MID ska eu-LISA vara personuppgiftsbiträde (artikel 41 i IOF).

När det gäller CRRS anges i delegerade akter till IOF att för anonymisering av personuppgifter enligt artikel 5 i dessa rättsakter ska eu-LISA vara personuppgiftsbiträde (artikel 7 i kommissionens delegerade förordning [EU] 2021/2222 av den 30 september 2021 om komplettering av Europaparlamentets och rådets förordning [EU] 2019/818 med detaljerade bestämmelser om driften av den centrala databasen för rapporter och statistik och artikel 7 i kommissionens delegerade förordning [EU] 2021/2223 av den 30 september 2021 om komplettering av Europaparlamentets och rådets förordning [EU] 2019/817 med detaljerade bestämmelser om driften av den centrala databasen för rapporter och statistik).

I det följande redogörs för myndighetsansvaret för personuppgiftsbehandling enligt IOF och de underliggande EU-rättsakterna och det nationella regelverket.

Migrationsverket har personuppgiftsansvar när det gäller VIS (11 § 3 förordningen [2019:502] med instruktion för Migrationsverket).

Såvitt avser personuppgiftsansvar för behandling av personuppgifter i SIS är Polismyndigheten personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför (1 § andra stycket lagen om Schengens informationssystem). När det nya SIS-regelverket har börjat tillämpas fullt ut kommer både Polismyndigheten och Migrationsverket att kunna registrera uppgifter i SIS. Respektive myndighet ska då vara personuppgiftsansvarig för den behandling av personuppgifter i systemet som myndigheten utför (5 § lagen med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem, som träder i kraft den dag regeringen bestämmer).

För Ecris-TCN ska varje centralmyndighet fungera som personuppgiftsansvarig med avseende på personuppgiftsbehandling som centralmyndighetens medlemsstat utför enligt EU:s förordning om Ecris-TCN (artikel 23 i den förordningen). Polismyndigheten kommer i egenskap av centralmyndighet att bli personuppgiftsansvarig för den nationella behandlingen av uppgifter i Ecris-TCN när systemet sätts i drift (se artikel 3.5 i EU:s förordning om Ecris-TCN, 16 § och bilagan till förordningen [2014:1102] med instruktion för Polismyndigheten och prop. 2021/22:172 s. 68).

Vidare har Polismyndigheten föreslagits bli personuppgiftsansvarig för in- och utresesystemet när detta system sätts i drift (Ds 2021:9, s. 132 f.).

När det gäller en medlemsstats behandling av personuppgifter i Etias centrala system ska den nationella Etias-enheten vara personuppgiftsansvarig (artikel 57.2 i Etias-förordningen). Polismyndigheten har föreslagits bli nationell Etias-enhet när Etias sätts i drift (Ds 2021:19 s. 49 f.).

För Eurodac har ingen myndighet pekats ut som personuppgiftsansvarig, utan det följer av det allmänna dataskyddsrättsliga regelverket vilken myndighet som är personuppgiftsansvarig.

IOF:s bestämmelser om personuppgiftsansvar är direkt tillämpliga. Därutöver finns det regler om vilka myndigheter som är person-

uppgiftsansvariga och vilken innebörd detta ansvar har, i det allmänna dataskyddsrättsliga regelverket, de underliggande rättsakterna och nationell kompletterande reglering. Sammantaget kräver bestämmelserna om personuppgiftsansvar i IOF inte några författningsändringar.

12.3 Säkerhetsfrågor, egenkontroll och överföring av uppgifter till tredjeland

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om säkerhetsfrågor, egenkontroll och överföring av uppgifter till tredjeländer kräver inte några författningsändringar.

Skälen för bedömningen: I artikel 42 i IOF regleras säkerhet vid personuppgiftsbehandling. Eu-LISA, Etias centralenhet, Europol och medlemsstaternas myndigheter ska säkerställa säkerheten vid den behandling av personuppgifter som äger rum enligt IOF. Vidare ska dessa aktörer samarbeta kring säkerhetsrelaterade uppgifter (artikel 42.1 i IOF). Eu-LISA ska vidta nödvändiga åtgärder för att säkerställa IO-komponenternas och den relaterade kommunikationsinfrastrukturens säkerhet (artikel 42.2). I synnerhet ska eu-LISA vidta nödvändiga åtgärder, inbegripet en säkerhetsplan, en kontinuitetsplan och en katastrofplan, i syfte att bl.a. fysiskt skydda uppgifter och hindra obehörig behandling av uppgifter (artikel 42.3). Medlemsstaterna, Europol och Etias centralenhet ska vidta åtgärder som är likvärdiga med de som avses i punkt 3 vad gäller säkerheten vid behandling av personuppgifter som utförs av de myndigheter som har rätt till åtkomst till någon av IO-komponenterna (artikel 42.4).

Artikel 42.1 riktar sig till medlemsstaternas myndigheter och är direkt tillämplig för de personuppgiftsansvariga myndigheterna. Den kräver inga kompletterande nationella bestämmelser. När det gäller de övriga bestämmelserna i artikel 42 om medlemsstaternas skyldigheter i fråga om behandling av uppgifter kommer behandlingen av personuppgifter enligt IOF, som anges i avsnitt 12.1, att omfattas av antingen dataskyddsförordningens eller brottsdata-

lagens tillämpningsområde. I dessa finns preciserade krav på åtgärder för att säkerställa en säker och lagenlig uppgiftsbehandling. Här kan bl.a. nämnas bestämmelser om den personuppgiftsansvariges skyldigheter att vidta tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter är författningsenlig och att den enskildes rättigheter skyddas samt att se till att nödvändiga skyddsåtgärder integreras i behandlingen (artiklarna 24, 25 och 32 i dataskyddsförordningen och 3 kap. 2–4 §§ brottsdatalagen). Dessa regler gäller för de myndigheter som är personuppgiftsansvariga enligt IOF. Därigenom bedöms kraven i artikel 42 vara uppfyllda. Bestämmelserna om säkerhet vid personuppgiftsbehandling kräver därför inte några kompletterande nationella bestämmelser.

Artikel 43 innehåller bestämmelser om säkerhetstillbud, dvs. alla händelser som har eller kan ha inverkan på IO-komponenternas säkerhet och som kan orsaka skada på eller förlust av uppgifter lagrade i dem. Enligt artikeln gäller bl.a. att medlemsstaterna utan dröjsmål ska underrätta kommissionen, eu-LISA, de behöriga tillsynsmyndigheterna och Europeiska datatillsynsmannen om alla säkerhetstillbud (artikel 43.3). De berörda medlemsstaterna, Etias centralenhet, Europol och eu-LISA ska samarbeta om ett säkerhetstillbud inträffar. Kommissionen ska fastställa specifikationer för detta samarbete genom genomförandeakter (artikel 43.5).

Vidare finns bestämmelser om egenkontroll i artikel 44. Medlemsstaterna och de relevanta unionsbyråerna ska se till att varje myndighet som har åtkomsträtt till IO-komponenterna vidtar nödvändiga åtgärder för att övervaka efterlevnaden av IOF och vid behov samarbetar med tillsynsmyndigheterna (artikel 44 första stycket).

I artikel 50 föreskrivs att personuppgifter som lagras eller behandlas i IO-komponenterna eller till vilka dessa fått åtkomst inte ska få överföras eller göras tillgängliga för tredjeländer, internationella organisationer eller privata parter. Förbudet ska dock inte påverka viss angiven reglering i relaterade frågor i bl.a. underliggande rättsakter.

Bestämmelserna om säkerhetsfrågor, egenkontroll och förbud mot överföring till tredjeländer är direkt tillämpliga och bedöms inte kräva några författningsåtgärder.

12.4 De registrerades rättigheter

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om enskildas rätt till information och rätt till tillgång till samt rättelse, komplettering och radering av uppgifter i MID kräver inte några författningsändringar. Inte heller bestämmelserna om begränsning av behandlingen av personuppgifter i MID kräver några författningsändringar.

Skälen för bedömningen

Rätt till information

I artikel 47 finns bestämmelser om rätt till information. Den myndighet som samlar in de personuppgifter som ska lagras i den gemensamma biometriska matchningstjänsten, CIR eller MID ska tillhandahålla de personer vars uppgifter samlas in den information som krävs enligt vissa angivna bestämmelser i dataskyddsförordningen, dataskyddsdirektivet och i förordning (EU) 2018/1725. Myndigheten ska tillhandahålla informationen vid den tidpunkt då uppgifterna samlas in (artikel 47.1). Vidare ställs vissa språkliga krav när det gäller hur informationen ska göras tillgänglig (artikel 47.2). De personer vars uppgifter registrerats i in- och utresesystemet, VIS eller Etias ska underrättas om behandlingen av personuppgifter enligt punkt 1 när en person- eller ansökningsakt skapas eller uppdateras i något av dessa system (artikel 47.3 i förordning [EU] 2019/817). När det gäller personuppgifter som har registrerats i Ecris-TCN och som behandlas i enlighet med förordning (EU) 2019/818 ska bestämmelserna om rätten till information i unionens tillämpliga dataskyddsregler tillämpas (artikel 47.3 i förordning [EU] 2019/818).

Bestämmelserna i artikel 47 är direkt tillämpliga och något behov av kompletterande bestämmelser finns inte.

Enskildas rätt till tillgång till samt rättelse, komplettering och radering av uppgifter, och begränsning av behandlingen av personuppgifter i MID

I artikel 48 regleras vissa ytterligare rättigheter kopplade till personuppgiftsbehandlingen i MID. För att utöva sina rättigheter enligt vissa bestämmelser i dataskyddsförordningen, dataskyddsdirektivet och förordning 2018/1725 ska varje person ha rätt att vända sig till den behöriga myndigheten i vilken medlemsstat som helst, som ska pröva och besvara begäran (artikel 48.1). De angivna bestämmelserna gäller rätt till tillgång till samt rättelse, komplettering och radering av uppgifter. De gäller även begränsning av behandling av personuppgifter. I artikeln anges närmare detaljer kring när en medlemsstat ska svara på en sådan begäran. Vidare anges att medlemsstaterna får besluta att svaren ska lämnas av centralenheter (artikel 48.2).

I artikel 48.3 och 48.4 regleras förfarandet för det fall att begäran om rättelse eller radering av personuppgifter ställs till en annan medlemsstat än den medlemsstat som ansvarar för den manuella verifieringen, respektive om en sådan begäran ställs till en medlemsstat där Etias centralenhet ansvarade för den manuella verifieringen. Den medlemsstat som ansvarade för den manuella verifieringen eller – om det inte fanns någon ansvarig medlemsstat eller om Etias centralenhet var ansvarig – den medlemsstat som begäran ställts till, ska rätta eller radera uppgifter som lagrats i MID om det efter en prövning visar att sig att uppgifterna är oriktiga eller har registrerats på ett olagligt sätt. Den berörda personen ska informeras skriftligen om detta (artikel 48.5). I artikel 48.6 regleras vilka åtgärder en medlemsstat ska vidta om den ändrar uppgifter som lagras i MID under lagringsperioden.

Om den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts inte instämmer i att uppgifter som lagras i MID är oriktiga eller har registrerats på ett olagligt sätt, ska den medlemsstaten utan dröjsmål anta ett administrativt beslut med en skriftlig förklaring till den berörda personen om varför den inte är beredd att rätta eller radera uppgifter som rör honom eller henne (artikel 48.7). Beslutet ska även ge information om möjligheten att invända mot beslutet och, i tillämpliga fall, information om hur talan

kan väckas vid eller klagomål inges till behöriga myndigheter eller domstolar samt möjligheterna till bistånd, även från tillsynsmyndigheterna (artikel 48.8).

I artikel 48.9 regleras vilken information som en begäran från en enskild om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter ska innehålla och hur den informationen ska hanteras. I artikel 48.10 regleras en skyldighet för medlemsstaterna att spara skriftlig dokumentation om en sådan begäran och hanteringen av denna samt att tillhandahålla informationen till tillsynsmyndigheterna. Artikel 48 ska inte påverka begränsningar och inskränkningar av de rättigheter som anges i artikeln i enlighet med dataskyddsförordningen och dataskyddsdirektivet (artikel 48.11).

Med behörig myndighet enligt artikel 48 får, när en begäran enligt artikeln ges in till en myndighet i Sverige avseende en länk som har verifierats här, förstås den myndighet som är personuppgiftsansvarig för de aktuella uppgifterna.

Artikel 48 innebär att vissa uppgifter ska utföras av svenska myndigheter även om den manuella verifieringen inte gjordes av svenska myndigheter. Som anges ovan föreskriver IOF en rätt för enskilda att vända sig till den behöriga myndigheten i vilken medlemsstat som helst, som ska pröva och besvara begäran (artikel 48.1). Med behörig myndighet får i detta sammanhang – alltså när begäran ges in till en medlemsstat som inte verifierade länken – förstås en myndighet som har behörig åtkomst till MID.

Artikel 48 är direkt tillämplig. Ges en ansökan om rättelse, radering eller begränsning av behandlingen av personuppgifter som lagras i MID in till en svensk behörig myndighet måste denna förhålla sig till och tillämpa de regler som gäller enligt artikel 48 i IOF. Det krävs därför inga kompletterande nationella regler till artikel 48.

Som anges ovan har medlemsstaterna enligt artikel 48.2 i IOF möjlighet att utse en centralenhet som ska lämna svar på en begäran till den enskilde. Det görs dock bedömningen att det inte finns behov av att utse någon nationell centralenhet för ärenden enligt artikel 48 i IOF.

För att underlätta utövandet av rätten till åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter ska det inrättas en webbportal som bl.a. ska innehålla information om de

rättigheter och förfaranden som avses i artiklarna 47 och 48 (artikel 49.1 och 49.2). Genom webbportalen ska en person vars uppgifter behandlas i MID kunna få kontaktuppgifter till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen enligt ett förfarande som regleras i artikel 49.3. Medlemsstaterna ska ge eu-LISA kontaktuppgifter till alla myndigheter som är behöriga att pröva och besvara varje sådan begäran som avses i artiklarna 47 och 48 och ska regelbundet se över huruvida dessa kontaktuppgifter är aktuella (artikel 49.4). Eu-LISA ska utveckla webbportalen och säkerställa dess tekniska förvaltning (artikel 49.5). Bestämmelserna om webbportalen är direkt tillämpliga och kräver inte några författningsändringar. Närmare bestämmelser om webbportalen finns i två delegerade förordningar (Kommissionens delegerade förordning [EU] 2021/2103 av den 19 augusti 2021 om fastställande av närmare bestämmelser för driften av webbportalen i enlighet med artikel 49.6 i Europaparlamentets och rådets förordning [EU] 2019/818 och kommissionens delegerade förordning [EU] 2021/2104 av den 19 augusti 2021 om fastställande av närmare bestämmelser för driften av webbportalen i enlighet med artikel 49.6 i Europaparlamentets och rådets förordning [EU] 2019/817).

12.5 Tillsyn

Förslag: I förordningen med instruktion för Integritetsskyddsmyndigheten ska det anges att myndigheten är nationell tillsynsmyndighet för behandling av personuppgifter enligt EU:s förordningar om interoperabilitet.

Bedömning: Bestämmelserna om tillsyn kräver i övrigt inte några författningsändringar.

Skälen för förslaget och bedömningen: I artiklarna 51 och 53 finns bestämmelser om tillsyn respektive tillsynsmyndigheternas samarbete med Europeiska datatillsynsmannen. Av bestämmelserna framgår bl.a. att varje medlemsstat ska se till att tillsynsmyndigheterna på ett oberoende sätt övervakar lagligheten i den berörda medlemsstatens behandling av personuppgifter enligt IOF

inklusive överföringen av dem till och från IO-komponenterna (artikel 51.1). Vidare ska medlemsstaterna se till att deras tillsynsmyndigheter har de resurser och den expertis som krävs för att fullgöra de uppgifter som de åläggs enligt IOF (artikel 51.4). Bland dessa uppgifter kan följande nämnas:

- Tillsynsmyndigheten ska säkerställa att en revision av den personuppgiftsbehandling som utförs av de nationella myndigheterna enligt IOF genomförs i enlighet med relevanta internationella revisionsstandarder minst vart fjärde år. Myndigheten ska offentliggöra vissa uppgifter om ansökningar om rättelse, radering och begränsning av behandling av uppgifter (artikel 51.3).
- Tillsynsmyndigheterna och Europeiska datatillsynsmannen ska aktivt samarbeta inom ramen för sina respektive ansvarsområden och säkerställa en samordnad tillsyn av användningen av IO-komponenterna och tillämpningen av övriga bestämmelser i IOF (artikel 53.1).

Vidare ska medlemsstaterna tillhandahålla all information som begärs av den tillsynsmyndighet som avses i artikel 51.1 i dataskyddsförordningen och ska i synnerhet förse den med information om verksamhet som bedrivs enligt IOF. Medlemsstaterna ska bevilja tillsynsmyndigheten åtkomst till de loggar som avses i artiklarna 10, 16, 24 och 36 och till de motiveringar som avses i artikel 22.2 och när som helst bereda den tillträde till alla sina lokaler som används för interoperabilitetsändamål (artikel 51.5).

Med tillsynsmyndighet syftas i IOF på den tillsynsmyndighet som avses i artikel 51.1 i dataskyddsförordningen och i artikel 41.1 i dataskyddsdirektivet (artikel 4.4 i IOF). I Sverige är Integritetsskyddsmyndigheten tillsynsmyndighet för personuppgiftsbehandling enligt dataskyddsförordningen och dataskyddsdirektivet (2 a § första stycket förordningen [2007:975] med instruktion för Integritetsskyddsmyndigheten). Det krävs därför inte några författningsändringar för att tillsyn ska kunna utövas i enlighet med kraven i dataskyddsförordningen och dataskyddsdirektivet. Däremot bör det klargöras att Integritetsskyddsmyndigheten är tillsynsmyndighet för person-

uppgiftsbehandling enligt IOF. En bestämmelse med denna innebörd bör därför införas i förordningen.

Bestämmelserna om tillsyn kräver i övrigt inte några författningsåtgärder.

12.6 Efterföljande behandling av biometriska uppgifter som tagits upp vid verkställighet av ett beslut om avvisning eller utvisning enligt utlänningslagen

Bedömning: Det krävs inte några författningsändringar i fråga om den efterföljande behandlingen av de biometriska uppgifter som tagits vid verkställighet av ett beslut om avvisning eller utvisning enligt utlänningslagen.

Skälen för bedömningen

Biometriska uppgifter kommer att tas för ett nytt ändamål

I avsnitt 9.5.2 föreslås en bestämmelse om skyldighet för en utlänning att i ett ärende om verkställighet av ett beslut om avvisning eller utvisning enligt utlänningslagen lämna biometriska uppgifter för en sökning i CIR. Uppgifter som har samlats in för att en sökning ska kunna genomföras finns, när sökningen är klar, fortfarande kvar. Det finns inga bestämmelser i IOF om hur de biometriska uppgifter som tas för att genomföra en sökning i CIR ska hanteras efter det att sökningen har genomförts. Frågan är om den föreslagna bestämmelsen bör kompletteras med en bestämmelse om efterföljande behandling av de biometriska uppgifter som har tagits upp för sökningar enligt den föreslagna bestämmelsen, dvs. om hur sådana uppgifter ska behandlas efter sökningen.

De allmänna dataskyddsrättsliga bestämmelserna

Bestämmelser om behandling av personuppgifter – såsom fotografier och fingeravtryck – finns i dataskyddsförordningen, som gäller vid bl.a. verkställighet av beslut om avvisning och utvisning och utlänningskontroll, i den mån verksamheten inte bedrivs i brottsbekämpande syfte eller i syfte att verkställa straffrättsliga påföljder. Dataskyddsförordningen innehåller allmänna bestämmelser som gäller för all personuppgiftsbehandling som faller inom tillämpningsområdet. Bestämmelserna innebär bl.a. att personuppgifter inte får behandlas på ett sätt som är oförenligt med de ändamål för vilka de samlades in och inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (artikel 5.1 b och 5.1 e). Biometriska uppgifter räknas som känsliga personuppgifter om de behandlas i syfte att entydigt identifiera en person och de omgärdas därför av särskilda, mer restriktiva bestämmelser för behandlingen (artiklarna 4.14 och 9.1).

I svensk rätt kompletteras dataskyddsförordningen av bl.a. utlänningsdatalagen, som är en sektorspecifik registerlag. Den gäller inom bl.a. Polismyndighetens och Migrationsverkets verksamhet som rör utlänningskontroll och verkställighet av beslut om avvisning och utvisning, i den mån verksamheten inte bedrivs i brottsbekämpande syfte eller i syfte att verkställa en straffrättslig påföljd (2, 3 och 4 c §§ utlänningsdatalagen, prop. 2015/16:65 s. 41, prop. 2017/18:232 s. 113 och prop. 2017/18:254 s. 23 f.).

I 14 § utlänningsdatalagen finns särskilda bestämmelser som rör behandling av sådana känsliga personuppgifter som avses i artikel 9.1 i dataskyddsförordningen. Sådana uppgifter får behandlas endast för de ändamål som anges i 11 och 13 §§ utlänningsdatalagen, dvs. om det behövs för bl.a. handläggning av ärenden inom lagens tillämpningsområde, och endast om uppgifterna är absolut nödvändiga för syftet med behandlingen (14 §). I 15 § utlänningsdatalagen finns också särskilda bestämmelser som rör Migrationsverkets möjlighet att föra separata register över de fingeravtryck och fotografier som tas med stöd av 9 kap. 8 § UtlL. I och med anpassningarna till in- och utresesystemet har en ny möjlighet att ta upp fingeravtryck och fotografi för kontroll enligt in- och utreseförordningen förts in i en ny paragraf, 9 kap. 8 h § i utlänningslagen. Samtidigt har 15 § första

stycket utlänningsdatalagen ändrats så att även uppgifter som tas med stöd av 9 kap. 8 h § UtlL ska få lagras i registret. Ändringarna träder i kraft den dag som regeringen bestämmer (se prop. 2021/22:81).

För personuppgiftsbehandling i brottsbekämpande syfte eller i syfte att verkställa straffrättsliga påföljder gäller reglerna i brottsdatalagen. Den är bl.a. tillämplig på Polismyndighetens personuppgiftsbehandling vid verkställighet av ett beslut om utvisning på grund av brott (prop. 2017/18:254 s. 24). Enligt brottsdatalagen får personuppgifter inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (2 kap. 17 § första stycket). Vidare får känsliga personuppgifter i form av biometriska uppgifter behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 12 §).

Brottsdatalagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen (1 kap. 4 § första stycket). För sådan personuppgiftsbehandling gäller i stället lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Lagen är tillämplig på Säkerhetspolisens personuppgiftsbehandling vid verkställighet av ett beslut om utvisning i ett säkerhetsärende enligt utlänningslagen (jfr 2 kap. 1 § 3 c) och prop. 2018/19:163 s. 218). Enligt lagen gäller bl.a. att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål de ursprungligen behandlades för och att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (2 kap. 3 § och 4 kap. 1 §). Det finns även ytterligare begränsningar kring längsta tillåtna behandling som gäller vid automatiserad behandling (se bl.a. 4 kap. 1, 2, 6 och 7 §§). Vidare får Säkerhetspolisen behandla biometriska uppgifter om det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 10 §).

Det behövs inga kompletterande bestämmelser för efterföljande behandling av uppgifter som tas vid verkställighet av beslut om avvisning och utvisning enligt utlänningslagen

För de biometriska uppgifter som tas i ett ärende om verkställighet av beslut om avvisning eller utvisning finns det, som framgår ovan, ett befintligt dataskyddsrättsligt regelverk som skulle reglera hur dessa uppgifter får behandlas efter genomförda sökningar, om det inte införs några särskilda bestämmelser. Det befintliga regelverk som det skulle handla om är, utom i fråga om säkerhetsärenden, antingen reglerna i dataskyddsförordningen och utlänningsdatalagen, eller reglerna i brottsdatalagen. Utrymmet för att lagra biometriska uppgifter i enlighet med dessa regler får bedömas som begränsat. I många fall innebär regelverket alltså att uppgifterna måste förstöras efter att sökningen har genomförts.

Den begränsade möjlighet till fortsatt behandling som det dataskyddsrättsliga regelverket i vissa fall kan ge utrymme för – om det är absolut nödvändigt för syftet med behandlingen och för särskilt angivna ändamål – bedöms vara proportionell i förhållande till det behov av fortsatt behandling som kan finnas och skyddet för den personliga integriteten. Frågan är då om det finns något annat skäl för att införa kompletterande nationella regler.

Med hänsyn till att en person som har ett verkställbart avlägsnandebeslut som utgångspunkt ska lämna landet bedöms det inte vara ändamålsenligt och proportionerligt att införa en särskild möjlighet att spara de biometriska uppgifter som tas i ett ärende om avvisning eller utvisning (jfr t.ex. 9 kap. 8 § andra stycket UtlL). Någon kompletterande reglering om efterföljande behandling för uppgifterna är alltså inte motiverad för ett sådant syfte.

Ett skäl för att införa kompletterande bestämmelser kan vara vikten av enhetlighet eller överskådlighet i regelverket (se t.ex. prop. 2021/22:81 s. 27). Det finns flera bestämmelser i 9 kap. UtlL om efterföljande behandling som anger att biometriska uppgifter ska förstöras omedelbart efter genomförd kontroll (se t.ex. 9 kap. 8 b, 8 c och 8 f §§).

I fråga om regleringen av efterföljande behandling inom dataskyddsförordningens tillämpningsområde är det visserligen tillåtet att återge bestämmelser i EU-förordningar om det är nödvändigt för att den nationella regleringen ska bli begriplig och

sammanhållen. Under senare tid har det antagits allt fler unionsrättsliga rättsakter som direkt eller indirekt innebär att enskilda behöver lämna biometriska uppgifter i olika sammanhang. Detta är en utveckling som kan antas fortsätta, bl.a. med hänsyn till de möjligheter som utvecklingen av ny teknik innebär. När det tillkommer bestämmelser om upptagning av biometriska uppgifter kan det också medföra att nya bestämmelser om förstörande av uppgifter införs. Att även fortsättningsvis reglera den efterföljande behandlingen i svensk rätt, trots att det redan finns reglering på EU-nivå, kan på sikt riskera att leda till ett komplext och svåröverskådligt regelverk snarare än att skapa enhetlighet och tydlighet. I den utsträckning de unionsrättsliga bestämmelserna är tydliga kan det därför finnas skäl att undvika reglering även på nationell nivå. Huvudregeln är dessutom att bestämmelser i EU-förordningar inte ska återges i nationell rätt. De bestämmelser i utlänningslagen som uttryckligen reglerar att uppgifter ska förstöras efter att en kontroll har genomförts har dessutom i huvudsak genomförts i tiden innan dataskyddsförordningen började tillämpas. Även när det gäller den personuppgiftsbehandling som omfattas av brottsdatalagens tillämpningsområde riskerar regelverket att bli svåröverskådligt om bestämmelser om efterföljande behandling införs i frågor som redan regleras i den lagen. Det finns mot denna bakgrund inte skäl att regelmässigt införa bestämmelser om efterföljande behandling när nya bestämmelser om upptagning av biometriska uppgifter införs.

I linje med dessa överväganden infördes i lagstiftningsärendet om anpassningar till in- och utresesystemet bestämmelser om upptagning av biometriska uppgifter i 9 kap. 8 d § första stycket och 9 kap. 8 i § UtlL, utan någon särskild reglering om efterföljande behandling (se även prop. 2021/22:81 s. 45 ff.).

Mot denna bakgrund finns det inte skäl att införa någon särskild reglering av efterföljande behandling av biometriska uppgifter som tas upp vid verkställighet av beslut om avvisning eller utvisning, för de situationer då bestämmelserna i antingen dataskyddsförordningen och utlänningsdatalagen eller brottsdatalagen är tillämpliga.

För behandlingen av biometriska uppgifter som tas upp vid verkställighet av ett beslut om avvisning eller utvisning i ett säkerhetsärende enligt utlänningslagen gäller bestämmelserna i lagen om Säkerhetspolisens behandling av personuppgifter. Det bedöms

inte finnas något behov av att särskilt reglera den efterföljande behandlingen av dessa uppgifter.

Sammantaget bör det inte införas särskilda bestämmelser om den efterföljande behandlingen av de biometriska uppgifter som tagits i ärenden om verkställighet av beslut om avvisning och utvisning enligt utlänningslagen.

12.7 Efterföljande behandling av biometriska uppgifter som tagits upp vid en inre utlänningskontroll

Förslag: Det fotografi och de fingeravtryck som har tagits vid en inre utlänningskontroll för sökning i den gemensamma databasen för id-uppgifter ska omedelbart förstöras när kontrollen har genomförts om det framkommer att utlänningen har rätt att vistas i Sverige. De biometriska uppgifter som tagits för detta syfte och som inte ska förstöras ska få lagras i Migrationsverkets register över fotografier och fingeravtryck.

Skälen för förslaget

Biometriska uppgifter som tas vid en inre utlänningskontroll bör omedelbart förstöras om utlänningen har rätt att vistas i Sverige

I avsnitt 9.5.1 föreslås en bestämmelse om skyldighet för en utlänning att vid en inre utlänningskontroll lämna biometriska uppgifter för en sökning i CIR. Det finns inga bestämmelser i IOF om hur de biometriska uppgifter som tas för att genomföra en sökning i CIR ska hanteras efter det att sökningen har genomförts. Som redovisas i avsnitt 12.6 finns det dock ett allmänt dataskyddsrättsligt regelverk som gäller för sådan efterföljande behandling. Utöver det regelverk som redogjorts för i det avsnittet aktualiseras även kustbevakningsdatalagen (2019:429) vid behandlingen av uppgifter som tas vid inre utlänningskontroller. Enligt lagen, som kompletterar dataskyddsförordningen, gäller bl.a.

att om uppgifter om en person behandlas får de kompletteras med sådana känsliga personuppgifter som avses i artikel 9.1 i dataskyddsförordningen när det är absolut nödvändigt för syftet med behandlingen (3 och 12 §§). Frågan är om bestämmelsen som föreslås i avsnitt 9.5.1 ändå bör kompletteras med en bestämmelse om efterföljande behandling av de biometriska uppgifterna.

Om det vid kontrollen framkommer att utlänningen har rätt att vistas i Sverige, saknas det skäl att spara de biometriska uppgifter som har tagits. I sådana fall bör uppgifterna inte få sparas utan i stället förstöras, inte minst med hänsyn till integritetsaspekter. Samtidigt bedöms det, som utvecklas nedan, vara motiverat att spara uppgifterna om det visar sig att personen inte har rätt att vistas i Sverige. En sådan ordning kan inte åstadkommas genom att falla tillbaka på den allmänna dataskyddsrättsliga regleringen, eftersom den inte innehåller någon sådan regel. Detta talar för att det i fråga om inre utlänningskontroll är motiverat med en särskild regel om förstörande.

Vidare har i utlänningslagen nyligen införts två olika bestämmelser om skyldighet för en utlänning att lämna fingeravtryck och låta sig fotograferas vid en inre utlänningskontroll. I båda bestämmelserna anges att det fotografi och de fingeravtryck som har tagits omedelbart ska förstöras om det framkommer att utlänningen har rätt att vistas i Sverige (9 kap. 8 och 8 h §§ UtlL, varav den senare träder i kraft den dag som regeringen bestämmer). Det bör undvikas att det i två paragrafer om inre utlänningskontroll finns bestämmelser om efterföljande behandling av personuppgifter medan sådana bestämmelser saknas i en annan paragraf om inre utlänningskontroll (jfr prop. 2021/22:81 s. 51).

En bestämmelse som anger att de biometriska uppgifter som har tagits i nu aktuell situation omedelbart ska förstöras om det framkommer att utlänningen har rätt att vistas i Sverige bör därför införas. Bestämmelsen bör placeras i anslutning till den nya bestämmelsen om skyldighet att lämna biometriska uppgifter vid en inre utlänningskontroll i 9 kap. UtlL.

Biometriska uppgifter som inte ska förstöras bör få lagras i Migrationsverkets register

Om det vid en inre utlänningskontroll i stället framkommer att utlänningen saknar rätt att vistas i landet är situationen annorlunda. Möjligheten att spara och jämföra sådana biometriska uppgifter är ett viktigt verktyg för att motverka att personer som inte har rätt att vistas i Sverige ändå fortsätter att uppehålla sig här, vilket är angeläget för upprätthållandet av den inre säkerheten. Det ligger också i linje med IOF:s syften. Jämförelser av biometriska uppgifter är även avgörande för att kunna upptäcka personer som uppträder under olika identiteter.

Enligt gällande ordning har Migrationsverket rätt att föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 § UtlL (15 § utlänningsdatalagen). Detta kommer även att gälla biometriska uppgifter som tagits med stöd av 9 kap. 8 h § UtlL, när in- och utresesystemet sätts i drift (se avsnitt 12.6). Förutom fingeravtryck och fotografier får registren innehålla uppgift om bl.a. namn och andra identifieringsuppgifter (2 § utlänningsdataförordningen [2016:30]).

Enligt 15 § första stycket får dock endast fotografier och fingeravtryck som tas med stöd av 9 kap. 8 § UtlL och – när regeringen beslutat att sätta regleringen med anpassningar till in- och utreseförordningen i kraft – 9 kap. 8 h § UtlL föras in i registren.

För att det ska vara möjligt att spara de biometriska uppgifter som tas vid en inre utlänningskontroll, i de fall utlänningen saknar rätt att vistas i Sverige, behöver uppgifterna i dessa fall kunna föras in i Migrationsverkets register över fotografier och fingeravtryck. Regeringen har i andra lagstiftningsärenden konstaterat att den rättsliga grunden för den personuppgiftsbehandling som får utföras enligt utlänningsdatalagen är fastställd i den nationella rätten på ett sådant sätt som krävs enligt dataskyddsförordningen (se prop. 2017/18:254 s. 15 f. och prop. 2021/22:81 s. 52). Biometriska uppgifter räknas som känsliga personuppgifter om de behandlas i syfte att entydigt identifiera en person och de omgärdas därför av särskilda, mer restriktiva bestämmelser för behandlingen (artiklarna 4.14 och 9.1 i dataskyddsförordningen). I andra lagstiftningsärenden har regeringen gjort bedömningen att personuppgiftsbehandlingen enligt 15 § utlänningsdatalagen är nödvändig av hänsyn till ett viktigt

allmänt intresse och att förutsättningarna även i övrigt för att tillämpa undantaget i artikel 9.2 g är uppfyllda (se om den bedömningen prop. 2017/18:254 s. 35 och prop. 2021/22:81 s. 52; jfr även prop. 2020/21:159 s. 22). I promemorian görs samma bedömning avseende den nu aktuella personuppgiftsbehandlingen.

Det bör därför göras ett tillägg i 15 § första stycket utlänningsdatalagen med den innebörden att Migrationsverket får föra separata register över de fingeravtryck och fotografier som tas vid en inre utlänningskontroll för att genomföra en sökning i CIR, och som inte ska förstöras omedelbart efter kontrollen.

I utlänningsdataförordningen finns bestämmelser om gallring av uppgifter i registret. Som huvudregel gäller att en uppgift ska gallras när den registrerade blir svensk medborgare eller, i andra fall, senast tio år efter att uppgiften registrerades (3 §). Motsvarande bör gälla för gallring av de nu aktuella uppgifterna. Det krävs ingen författningsändring för att de aktuella uppgifterna ska omfattas av huvudregeln i 3 § utlänningsdataförordningen.

12.8 Efterföljande behandling av biometriska uppgifter som tagits upp vid verkställighet av ett beslut om utvisning i ett kvalificerat säkerhetsärende

Bedömning: Det krävs inte några författningsändringar i fråga om den efterföljande behandlingen av de biometriska uppgifter som tagits vid verkställighet av ett beslut om utvisning enligt lagen om särskild kontroll av vissa utlänningar.

Skälen för bedömningen: I avsnitt 9.5.3 föreslås en bestämmelse om skyldighet för en utlänning att lämna biometriska uppgifter för en sökning i CIR vid verkställighet av ett beslut om utvisning i ett kvalificerat säkerhetsärende enligt lagen om särskild kontroll av vissa utlänningar. Det finns inga bestämmelser i IOF om hur de biometriska uppgifter som tas för att genomföra en sökning i CIR ska hanteras efter det att sökningen har genomförts. Frågan är om bestämmelsen som föreslås i avsnitt 9.5.3 bör kompletteras med en

bestämmelse om efterföljande behandling av de biometriska uppgifterna.

För behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet gäller lagen om Säkerhetspolisens behandling av personuppgifter. Den gäller även vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen, vilket innebär att det som sägs i lagen om Säkerhetspolisen då i stället gäller Polismyndigheten (1 kap. 2 § och prop. 2018/19:163 s. 211). Lagen är bl.a. tillämplig på personuppgiftsbehandling vid verkställighet av nu aktuell typ av utvisningsbeslut (jfr 2 kap. 1 § 3 c) och prop. 2018/19:163 s. 218 f.). Enligt lagen gäller bl.a. att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål de ursprungligen behandlades för och att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (2 kap. 3 § och 4 kap. 1 §). Det finns även ytterligare begränsningar kring längsta tillåtna behandling som gäller vid automatiserad behandling (se bl.a. 4 kap. 1, 2, 6 och 7 §§) Vidare får Säkerhetspolisen behandla biometriska uppgifter om det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 10 §).

Mot bakgrund av bestämmelserna i det befintliga regelverket bedöms det inte finnas något behov av att särskilt reglera den efterföljande behandlingen av uppgifterna. När det gäller övriga bestämmelser om upptagning av fingeravtryck och fotografi i lagen om särskild kontroll av vissa utlänningar innehåller inte heller dessa någon reglering av den efterföljande behandlingen av uppgifterna (se t.ex. 5 kap. 28 och 30 §§). Det finns alltså inte heller anledning att införa någon sådan reglering med hänvisning till enhetligheten i regelverket.

Sammantaget bör det inte införas särskilda bestämmelser om den efterföljande behandlingen av de biometriska uppgifter som tagits vid verkställighet av ett beslut om utvisning enligt lagen om särskild kontroll av utlänningar i vissa fall.

13 Sekretess

Bedömning: EU:s förordningar om interoperabilitet kräver inte några författningsändringar i fråga om sekretess.

Skälen för bedömningen

IOF innebär att svenska myndigheter får en utökad åtkomstbehörighet till uppgifter i EU-gemensamma it-system

Som nämnts i avsnitt 8.1 är det inte tänkt att IOF ska påverka medlemsstaternas myndigheters åtkomstbehörighet till uppgifter i underliggande system (se artiklarna 9.6 och 18.3 i IOF). Inrättandet av IO-komponenterna innebär inte heller, med undantag för uppgifter i akterna med identitetsbekräftelse och CRRS, att fler uppgifter kommer att lagras i systemen. De ändringar som införs genom IOF handlar främst om tekniska lösningar för lagring och åtkomst till uppgifterna. Artiklarna 20–22 i IOF innehåller dock bestämmelser som i viss mån utvidgar medlemsstaternas myndigheters åtkomstbehörighet till uppgifter i underliggande system. Om en myndighet ges behörighet att göra sökningar enligt artikel 20 i IOF kan myndigheten komma att få åtkomst till uppgifter som annars inte hade varit sökbara för myndigheten. Även artikel 22 i IOF utvidgar de brottsbekämpande myndigheternas behörighet till åtkomst till uppgifter i underliggande system även om bestämmelsen begränsar sig till information om att en person finns i ett visst system. Syftet med artikel 22 i IOF är dock inte att utvidga myndigheternas behörighet till uppgifter i underliggande system utan att ge dem snabbare information om i vilket system uppgifter om en viss person finns (se avsnitt 8.2).

Vidare förutsätter inrättandet av MID att de myndigheter som ansvarar för den manuella verifieringen av länkar också har åtkomst till de uppgifter som krävs för verifieringen (se artiklarna 21.1 och 26.1 i IOF). Detta kan innebära att den verifierande myndigheten får åtkomst till uppgifter som den annars inte hade haft behörighet till. IOF innebär även att medlemsstaternas myndigheter får åtkomst till uppgifter om de länkar som skapas i MID och som lagras i akten med identitetsbekräftelse. För att få åtkomst till uppgift om en vit eller grön länk krävs att myndigheten har åtkomst till de två EU-informationssystem som innehåller uppgifter mellan vilka den länken skapats (artikel 26.3 och 26.4 i IOF). Såvitt avser åtkomst till röda länkar räcker det med att myndigheten har behörighet till ett av de underliggande systemen (artikel 26.2 i IOF). Myndigheten ska då ges åtkomst till den röda länken och hänvisningen till de EU-informationssystem i vilka de länkade uppgifterna finns. Om en sökning i CIR ger upphov till en röd länk, ska myndigheterna enbart i syfte att bekämpa identitetsbedrägerier ha åtkomst till de personuppgifter som lagrats i CIR och som är kopplade genom en röd länk (artikel 21.2 i IOF). Detta innebär en utvidgad åtkomstbehörighet för de myndigheter som inte har behörighet till samtliga system.

Avslutningsvis innebär skapandet av CRRS att svenska myndigheter kommer att få åtkomst till vissa avidentifierade uppgifter som behandlas för statistiska ändamål (se avsnitt 11).

En utökad åtkomstbehörighet innebär inte i sig att fler uppgifter kommer att förvaras hos svenska myndigheter

Som ovan konstaterats innebär IOF att svenska myndigheter kommer att få en utökad åtkomstbehörighet till uppgifter i underliggande system. Detta kan i sin tur leda till att myndigheterna kommer att befatta sig med fler uppgifter än vad de gör idag. Aktuella uppgifter kan vara känsliga och behöva skyddas med sekretess. Enligt IOF har medlemsstaterna en skyldighet att vidta åtgärder för att skydda personuppgifter som behandlas enligt förordningarna (artikel 42 i IOF). Medlemsstaterna ska bl.a. förhindra obehörig läsning, kopiering, ändring eller obehörigt avlägsnande av datamedier. Någon särskild bestämmelse om sekretess för uppgifter som lagras i IO-komponenterna föreskrivs inte i IOF. Det får dock

anses underförstått att medlemsstaterna också ska säkerställa att känslig information inte lämnas ut på begäran från allmänheten om detta skulle skada ett allmänt eller enskilt intresse. Det behöver således göras en bedömning av om det finns ett adekvat sekretesskydd för uppgifterna som kommer att behandlas enligt IOF.

För att bedöma behovet av sekretesskydd måste det först konstateras att aktuella uppgifter omfattas av handlingsoffentlighet, dvs. rätten att ta del av allmänna handlingar. Som handlingar anses inte bara fysiska dokument utan också upptagningar som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniska hjälpmedel (se 2 kap. 3 § TF). En speciell sorts upptagning är upptagning för automatiserad behandling. Med det avses uppgift som är fixerad på någon form av datamedium och som antingen finns i eller kan matas in i en dator (se Bohlin, Offentlighetsprincipen, 2015, s. 40). En upptagning för automatiserad behandling kan bestå av allt från enstaka uppgifter till mycket stora informationssamlingar. Varje konstellation av sakligt och logiskt sammanhängande uppgifter ses som en upptagning för sig (prop. 1975/76:160 s. 90). Det är alltså, när det gäller upptagningar, informationsinnehållet som betraktas som en handling (se prop. 1990/91:60 s. 22).

En grundläggande förutsättning för att allmänheten ska ha rätt att hos en svensk myndighet ta del av handlingar är att handlingarna förvaras hos myndigheten och är att anse som inkomna till eller upprättade hos denna (se 2 kap. 4 § TF). Allmänna handlingar som finns hos en myndighet och som en annan myndighet genom direktåtkomst får tillgång till, utgör allmänna handlingar även hos denna myndighet (prop. 2002/03:135 s. 90). Motsvarande bedömning har gjorts såvitt avser svenska myndigheters direktåtkomst till uppgifter i utländska register (se prop. 2011/12:157 s. 8). En viktig faktor vid bedömningen av om en uppgift är tillgänglig och således förvaras hos en myndighet, är om myndigheten på egen hand kan söka efter information i registret (jfr HFD 2015 ref. 61). Däremot har ändamålsbegränsningar eller villkorade sökbegränsningar inte ansetts kunna tillmätas någon betydelse för den bedömningen (se a. prop. s. 8).

IOF:s bestämmelser om åtkomst till uppgifter innebär inte nödvändigtvis att fler uppgifter kommer att omfattas av den svenska handlingsoffentligheten än idag. Avgörande för bedömningen av om

en uppgift som behandlas enligt IOF kan begäras ut är om uppgiften ska anses förvarad hos myndigheten enligt 2 kap. 4 § TF. Den bedömningen får göras i det enskilda fallet.

Tillämpliga sekretessbestämmelser

IO-komponenterna kommer främst att innehålla uppgifter som rör tredjelandsmedborgare. Bestämmelser om sekretess avseende utlänningar finns i 21 kap. 5 § och 37 kap. offentlighets- och sekretesslagen (2009:400, OSL). Sekretess gäller t.ex. för en uppgift som rör en utlänning, om det kan antas att röjande av uppgiften skulle medföra fara för att någon utsätts för övergrepp eller lider annat allvarligt men som föranleds av förhållandet mellan utlänningen och en utländsk stat eller myndighet eller organisation av utlänningar (21 kap. 5 §). Sekretess gäller dessutom i verksamhet för kontroll över utlänningar för en uppgift om en enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men (37 kap. 1 § första stycket). Med verksamhet för kontroll över utlänningar avses inte bara förvaltningsärenden om t.ex. visering, uppehållstillstånd, arbetstillstånd, avvisning eller utvisning utan också kontrollåtgärder eller annan löpande tillsyn (se prop. 1979/80:2 Del A s. 210). Sådan sekretess gäller också hos en myndighet som lämnar biträde i verksamhet för kontroll över utlänningar (37 kap. 1 § fjärde stycket).

I 18 kap. OSL finns det bestämmelser till skydd för intresset av att förebygga eller beivra brott. Enligt 1 § gäller sekretess bl.a. för en uppgift som hänför sig till förundersökning i brottmål om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Sekretess gäller, under motsvarande förutsättningar bl.a. för en uppgift som hänför sig till annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen. Utöver bestämmelserna i 18 kap. OSL finns det bestämmelser i 35 kap. OSL om sekretess till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott m.m. Enligt 35 kap. 1 § OSL gäller sekretess för en

uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men bl.a. då uppgiften förekommer i en utredning enligt bestämmelserna om förundersökning i brottmål.

För uppgifter som förekommer i Schengens informationssystem finns särskilda sekretessbestämmelser i 18 kap. 17 § och 37 kap. 6 § OSL. Sekretessen tar sikte på vissa typer av registreringar i SIS och gäller hos de myndigheter som räknas upp i bestämmelserna. SIS består av ett centralt system samt nationella register som i Sverige förs av Polismyndigheten. Eftersom vissa andra myndigheter kan få direktåtkomst till registret, aktualiseras även bestämmelserna om överföring av sekretess i 11 kap. 4 § OSL. Med anledning av EU:s nya förordningar om SIS har vissa ändringar gjorts i 18 kap. 17 § och 37 kap. 6 § OSL. Ändringarna innebär att sekretessbestämmelserna omfattar fler registreringskategorier och ska vara direkt tillämpliga hos fler myndigheter än idag (se prop. 2020/21:222 s. 71 ff.). Ändringarna ska träda i kraft den dag regeringen bestämmer.

Vidare finns det tillämpliga bestämmelser om sekretess bl.a. i 15 kap. OSL. Enligt 15 kap. 1 § OSL gäller s.k. utrikessekretess för en uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. I 15 kap. 1 b § OSL anges vidare att sekretess gäller för en uppgift som en myndighet har elektronisk tillgång till i en upptagning för automatiserad behandling hos en annan stat eller mellanfolklig organisation, om myndigheten inte får behandla uppgiften enligt en bindande EU-rättsakt. Syftet med bestämmelsen är att en myndighet, som på grund av ändamålsbegränsningar eller villkorade sökbegränsningar inte får behandla uppgifter i en utländsk databas, inte ska behöva söka fram sådana uppgifter som inte omfattas av överenskommelsen om informationsutbyte för att kunna avgöra sekretessfrågan om uppgifterna begärs ut (se prop. 2011/12:157 s. 17). Sekretessen enligt den sistnämnda bestämmelsen är absolut. Om uppgifter som omfattas av bestämmelsen begärs ut ska de alltså hemlighållas utan att någon skadeprövning görs.

I avsnitt 9.6 behandlas möjligheten för svenska myndigheter att göra sökningar enligt artikel 20.4 i IOF i samband med en naturkatastrof, olycka eller terrordåd. Sådana sökningar föreslås kunna göras med fotografi eller fingeravtryck som tagits vid en rättsmedicinsk undersökning. Enligt 25 kap. 1 § OSL gäller sekretess inom hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Detsamma gäller i annan medicinsk verksamhet, exempelvis rättsmedicinsk och rättspsykiatrisk undersökning.

Det behövs inga författningsändringar om sekretess

Som nämnts ovan medför möjligheten till sökningar i CIR i identifieringssyfte enligt artikel 20 i IOF en utvidgad åtkomstbehörighet. Det kan antas att de svenska myndigheter som ges behörighet, inklusive Polismyndigheten, kommer att göra sådana sökningar i samband med brottsutredningar, inre utlänningskontroller och verkställighet av beslut om avvisning och utvisning. Vidare kommer myndigheter som bedriver gränskontroll, brottsbekämpning och utlänningskontroll inom ramen för sina respektive uppdrag att få åtkomst till röda länkar och därtill hörande uppgifter. Sådana myndigheter kommer även att få en utökad åtkomstbehörighet vid verifieringen av gula länkar. Som framgår av avsnitt 10 förutses Polismyndigheten stå för merparten av arbetet med att verifiera gula länkar i Sverige.

Vid inrättandet av underliggande system har det i svenska lagstiftningsarbeten gjorts överväganden om sekretesskydd för den information som lagras eller kommer att lagras i systemen (se bl.a. Ds 2021:9 s. 144 f. och Ds 2021:19 s. 95 ff.). Bedömningen av sekretesskyddet för uppgifter i underliggande system bör som utgångspunkt gälla även nu. Av föregående avsnitt framgår att det finns en förhållandevis omfattande befintlig sekretessreglering som kan tillämpas på sådana uppgifter som blir aktuella att behandla med anledning av IOF. Flera av de redovisade sekretessbestämmelserna är tillämpliga i Polismyndighetens verksamhet och hos andra myndigheter som bedriver gränskontroll, brottsbekämpning och utlänningskontroll. Uppgifter som kommer att behandlas enligt

IOF i gränskontrollerande eller brottsbekämpande syfte eller i samband med inre utlänningskontroller och verkställighet av beslut om avvisning och utvisning bedöms därför ha ett adekvat sekretesskydd.

Såvitt avser verifieringen av gula länkar som uppstår i samband med skapandet eller uppdateringen av en ansökningsakt i VIS kommer ansvaret att falla på svenska viseringsmyndigheter. Vilka myndigheter som omfattas av definitionen av en viseringsmyndighet utvecklas i avsnitt 10. I och med ansvaret för verifieringen av gula länkar kommer dessa myndigheter att få en utökad åtkomstbehörighet till vissa uppgifter i underliggande system. Vidare kommer myndigheterna att få kännedom om röda länkar i enlighet med vad som beskrivs ovan.

I likhet med vad som ovan anförts om sekretess för uppgifter hos myndigheter som bedriver gränskontroll, brottsbekämpning och utlänningskontroll är flera av de ovan redovisade sekretessbestämmelserna tillämpliga även hos viseringsmyndigheterna. Även de uppgifter som viseringsmyndigheterna kommer att behandla enligt IOF bedöms därför ha adekvat sekretesskydd.

Sammanfattningsvis bedöms IOF inte föranleda något behov av författningsändringar i fråga om sekretess.

14 Sanktioner och skadestånd

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om sanktioner och skadestånd kräver inte några författningsändringar.

Skälen för bedömningen

Gällande nationell rätt bedöms uppfylla IOF:s krav på sanktioner

I artikel 45 i IOF anges att medlemsstaterna ska se till att missbruk av uppgifter eller behandling eller utbyte av uppgifter i strid med förordningarna är belagt med sanktioner i enlighet med nationell rätt. Sanktionerna ska vara effektiva, proportionella och avskräckande. Artikeln är placerad i förordningarnas kapitel om dataskydd och bör tolkas så att de sanktioner som avses ska gälla överträdelser av IOF:s bestämmelser om just dataskydd.

Som anges i avsnitt 12.1. är dataskyddsförordningen tillämplig på myndigheternas behandling av personuppgifter enligt IOF, så länge brottsdatalagen inte är tillämplig. Därmed är också dataskyddsförordningens bestämmelser om administrativa sanktionsavgifter tillämpliga. I Sverige har det införts bestämmelser som innebär att tillsynsmyndigheten får ta ut en sanktionsavgift av en myndighet vid sådana överträdelser som avses i artikel 83.4–83.6 i dataskyddsförordningen (6 kap. 2 § dataskyddslagen). Eftersom dataskyddslagen gäller vid personuppgiftsbehandling enligt IOF så länge brottsdatalagen inte är tillämplig (se avsnitt 12.1), krävs det inte någon särskild reglering för att dataskyddslagens bestämmelser om sanktionsavgifter för myndigheter ska bli tillämpliga. Det innebär att de myndigheter som ska ha åtkomst till IO-komponenterna, och som

därmed kommer att behandla personuppgifter enligt IOF, kan påföras administrativa sanktionsavgifter i enlighet med 6 kap. 2 § dataskyddslagen.

Enligt dataskyddsförordningen ska medlemsstaterna även fastställa regler om andra sanktioner för överträdelser av den förordningen (artikel 84). Sådana sanktioner ska särskilt fastställas för överträdelser som inte är föremål för administrativa sanktionsavgifter. I dataskyddslagen finns det bestämmelser som kompletterar dataskyddsförordningens bestämmelser om sanktionsavgifter. Tillsynsmyndigheten får enligt de bestämmelserna ta ut en sanktionsavgift även vid överträdelse av förordningens bestämmelser om behandling av personuppgifter som rör lagöverträdelser (6 kap. 3 § dataskyddslagen). Även denna reglering kommer att vara tillämplig vid behandling av personuppgifter enligt IOF.

Om personuppgiftsbehandling sker i strid med IOF kan det dessutom i vissa fall bli aktuellt med straffansvar enligt svenska bestämmelser. Exempelvis kan en person som olovligen bereder sig tillgång till uppgifter i IO-komponenterna dömas för dataintrång i enlighet med 4 kap. 9 c § brottsbalken (BrB). Beroende på omständigheterna kan även ansvar för tjänstefel eller brott mot tystnadsplikt aktualiseras (20 kap. 1 och 3 §§ BrB). Därtill kan det bli aktuellt med disciplinansvar i form av varning och löneavdrag enligt lagen (1994:260) om offentlig anställning. Ytterst kan avskedande eller uppsägning komma i fråga.

När det gäller administrativa sanktioner inom dataskyddsdirektivets tillämpningsområde görs följande bedömning. Artikel 22 i IOF innehåller särskilda bestämmelser om förfarande och villkor för åtkomst till uppgifter i systemet i brottsbekämpande syfte. Vidare föreslås i avsnitt 9.3 att Polismyndigheten, Säkerhetspolisen och Tullverket ges behörighet att söka i CIR i identifieringssyfte i samband med brottsutredningar. I avsnitt 9.5.2 föreslås även en möjlighet för en polisman att söka i CIR i samband med bl.a. verkställighet av ett beslut om utvisning på grund av brott. Behandling av personuppgifter enligt IOF i brottsbekämpande syfte omfattas av brottsdatalagens tillämpningsområde. I 2 kap. brottsdatalagen finns det bestämmelser om grundläggande krav på behandling av uppgifter som kommer att vara tillämpliga vid behandling av personuppgifter enligt IOF för brottsbekämpande ändamål. Kraven gäller även generellt för brottsbekämpande

myndigheters behandling av uppgifterna i ett senare skede. Skulle behandling av personuppgifter ske i strid med dessa bestämmelser kan sanktioner komma i fråga enligt 6 kap. brottsdatalagen.

Sammanfattningsvis bedöms det finnas sanktioner i svensk rätt som motsvarar kraven i IOF. Det är upp till Integritetsskyddsmyndigheten och rättsvårdande myndigheter att se till att dessa tillämpas. Det behövs därför inte några kompletterande bestämmelser med anledning av artikel 45 i IOF.

IOF:s bestämmelser om skadestånd är direkt tillämpliga

Enligt 46.1 första stycket i IOF ska varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en otillåten behandling av personuppgifter eller av någon annan åtgärd från en medlemsstats sida som är oförenlig med förordningarna ha rätt till ersättning från den berörda medlemsstaten. Vidare ska varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en åtgärd från Europols, Europeiska gräns- och kustbevakningsbyråns eller eu-LISA:s sida som är oförenlig med förordningarna ha rätt till ersättning från byrån i fråga. Den berörda medlemsstaten, Europol, Europeiska gräns- och kustbevakningsbyrån eller eu-LISA ska helt eller delvis undantas från sitt skadeståndsansvar enligt första stycket om de bevisar att de inte är ansvariga för den händelse som orsakade skadan. Bestämmelsen påverkar inte rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet, eller dessas skadeståndsansvar i enlighet med dataskyddsförordningen, dataskyddsdirektivet och förordning (EU) 2018/1725.

I artikel 46.2 anges att om en medlemsstats underlåtenhet att fullgöra sina skyldigheter i enlighet med förordningarna skadar IO-komponenterna, ska den medlemsstaten vara ansvarig för denna skada, såvida inte och i den mån eu-LISA eller en annan medlemsstat som är bunden av IOF har underlåtit att vidta rimliga åtgärder för att hindra skadan från att uppstå eller för att begränsa dess verkningar.

Skadeståndsanspråk mot en medlemsstat för sådan skada som avses i artikel 46.1 och 46.2 i IOF ska regleras av den svarande medlemsstatens nationella rätt (artikel 46.3 i IOF). Skadestånds-

anspråk mot den personuppgiftsansvarige eller eu-LISA för sådan skada som avses i punkterna 1 och 2 ska omfattas av de villkor som fastställs i fördragen.

Det framgår direkt av artikel 46.1 och 46.2 i IOF vilka skador som omfattas av medlemsstaternas och EU-organens skadeståndsansvar enligt förordningarna. Bestämmelserna är direkt tillämpliga. Ett anspråk på skadestånd mot en medlemsstat ska dock enligt artikel 46.3 första meningen regleras av den medlemsstatens nationella rätt. Det ska därför finnas processuella bestämmelser i den nationella rätten som möjliggör och reglerar en sådan talan. Det får även anses finnas utrymme för kompletterande materiella bestämmelser på nationell nivå.

Rättegången i tvistemål i Sverige regleras i rättegångsbalken. Denna innehåller bl.a. bestämmelser om väckande av talan och om bevisning. Av 10 kap. 2 § framgår att en talan mot staten får väckas där den myndighet som ska föra statens talan i målet har sitt säte. Om ett anspråk på ersättning från staten grundas på ett påstående om överträdelse av unionsrätten handläggs det som regel av Justitiekanslern (3 § andra stycket förordningen [1995:1301] om handläggning av skadeståndsanspråk mot staten). Justitiekanslern för då också statens talan inför domstol. Justitiekanslern har även möjlighet att förhandla med den som kräver ersättning och besluta om skadestånd för statens räkning (6 §). Det finns alltså bestämmelser i svensk rätt som möjliggör och reglerar förfarandet för en talan om skadestånd enligt artikel 46 i IOF. Något behov av utfyllande processuella regler finns inte.

Allmänna materiella bestämmelser om skadestånd finns i skadeståndslagen (1972:207). Den lagen är tillämplig om inte något annat är föreskrivet (1 §). Om en ersättningsfråga inte regleras i IOF, och inte annat följer av EU-rätten i övrigt, tillämpas alltså de allmänna bestämmelserna i skadeståndslagen. Så kan vara fallet t.ex. i fråga om hur ersättningen för en skada ska beräknas. Även frågan om huruvida det föreligger kausalitet mellan en skada och den påstådda skadeorsaken får bedömas med utgångspunkt i nationell rätt.

Det finns liknande bestämmelser om skadestånd i de EU-rättsakter som reglerar underliggande system (jfr artikel 63 i Etias-förordningen och artikel 45 i in- och utreseförordningen). I samband med anpassningen av nationell rätt till den EU-rättsliga regleringen

av in- och utresesystemet samt Etias bedömdes skadeståndsbestämmelserna inte kräva några nationella författningsändringar (se Ds 2021:9 s. 147 ff. och 2021:19 s. 119). Någon annan bedömning görs inte i fråga om IOF:s skadeståndsbestämmelser.

15 IOF:s avslutande bestämmelser

15.1 Ansvarsområden

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om ansvarsområden kräver inte några författningsändringar.

Skälen för bedömningen: I kapitel VIII i IOF finns ett antal bestämmelser om ansvarsområden under såväl utvecklingen av IO-komponenterna som när dessa är i drift. Bestämmelserna reglerar eu-LISA:s ansvarsområden under utformnings- och utvecklingsfasen (artikel 54 i IOF) respektive före och efter idrifttagandet (artikel 55 i IOF). Vidare regleras Europols ansvarsområden (artikel 57 i förordning [EU] 2019/818) samt Etias centralenhets ansvarsområden (artikel 57 i förordning [EU] 2019/817 och artikel 58 i förordning [EU] 2019/818). Bestämmelserna om eu-LISA:s, Europols och Etias centralenhets ansvarsområden riktar sig inte till medlemsstaterna. De kräver därför inte några författningsändringar.

Medlemsstaternas ansvar regleras i artikel 56 i IOF. Varje medlemsstat ska enligt artikel 56.1 ha ansvar för

- Anslutning till ESP:s och CIR:s kommunikationsinfrastruktur.
- Integration av de befintliga nationella systemen och infrastrukturerna med ESP, CIR och MID.
- Organisation, förvaltning, drift och underhåll av den befintliga nationella infrastrukturen och dess anslutning till IO-komponenterna.
- Förvaltning av och föreskrifter för åtkomst för vederbörligen bemyndigad personal vid de behöriga nationella myndigheterna till ESP, CIR och MID i enlighet med denna förordning och

upprättande och regelbunden uppdatering av en förteckning över denna personal och deras profiler.

- Antagande av de lagstiftningsåtgärder som avses i artikel 20.5 och 20.6 för att få åtkomst till CIR i identifieringssyfte.
- Den manuella verifiering av olika identiteter som avses i artikel 29.
- Efterlevnad av de krav på uppgiftskvalitet som fastställs i unionsrätten.
- Efterlevnad av reglerna i varje EU-informationssystem beträffande personuppgifternas säkerhet och integritet.
- Avhjälpande av eventuella brister som konstaterats i kommissionens utvärderingsrapport om uppgifternas kvalitet som avses i artikel 37.5.

Vidare ska medlemsstaterna enligt artikel 56.2 i IOF ansluta sina utsedda myndigheter till CIR.

Vissa av de uppräknade ansvarsområdena behandlas i andra avsnitt i promemorian (om antagande av de lagstiftningsåtgärder som avses i artikel 20.5 och 20.6 för att få åtkomst till CIR i identifieringssyfte, se avsnitten 9.3, 9.5 och 9.6 och om den manuella verifieringen av olika identiteter som avses i artikel 29, se avsnitt 10). Ansvarsområdena omfattar i övriga delar organisationsfrågor och praktiska åtgärder bl.a. att upprätta och regelbundet uppdatera en förteckning över vederbörligen bemyndigad personal vid de behöriga myndigheterna med åtkomst till ESP, CIR och MID i enlighet med IOF. Bestämmelserna är direkt tillämpliga och kräver inte några författningsändringar.

15.2 Ändringar av andra EU-rättsakter

Bedömning: Bestämmelserna i EU:s förordningar om interoperabilitet om ändringar i andra EU-rättsakter kräver inte några författningsändringar.

Skälen för bedömningen

IOF:s ändringar i underliggande EU-förordningar är direkt tillämpliga

I kapitel IX i IOF finns bestämmelser som innebär att vissa ändringar görs i EU-rättsakter som reglerar underliggande system. Beroende på rättsområde regleras ändringarna antingen av förordning (EU) 2019/817 (artiklarna 58–65) eller förordning (EU) 2019/818 (artiklarna 59–61). IOF föreskriver ändringar i EU:s nya förordningar om Schengens informationssystem (gränsförordningen och polisförordningen), i EU:s förordning om Ecris-TCN, förordningen om eu-LISA (förordning [EU] 2018/1726), VIS-förordningen, in- och utreseförordningen, Etias-förordningen samt i gränskodexen.

Ändringarna i EU:s förordning om eu-LISA berör i första hand eu-LISA:s verksamhet och bedöms inte medföra något behov av anpassning av nationell rätt. Övriga ändringar utgör anpassningar till IOF och inrättandet av de nya IO-komponenterna. Det gäller t.ex. underliggande systems tekniska uppbyggnad, vilka uppgifter som ska ingå i CIR, användningen av ESP samt ansvaret för den manuella verifieringen av länkar. Vidare utvidgas vissa rättsakters syften i den utsträckning detta behövs för tillämpningen av artiklarna 20 och 21 i IOF.

De ovan berörda förordningarna i lydelse enligt IOF är direkt tillämpliga. Det krävs inga författningsändringar med anledning av de nya lydelserna.

Ändringarna i rådsbesluten om VIS påverkar inte tillämpningen av det nationella regelverket

Ändringarna i rådets beslut 2004/512/EG om inrättandet av VIS respektive VIS-rådsbeslutet utgör anpassningar till IOF och inrättandet av IO-komponenterna. Till skillnad från en EU-förordning är rådsbesluten inte direkt tillämpliga i medlemsstaterna utan kräver som regel nationell implementering för att kunna tillämpas. Rådets beslut 2004/512/EG om inrättandet av VIS utgör en rättslig ram för inrättandet av systemet. Den huvudsakliga

regleringen av VIS finns emellertid i den direkt tillämpliga VIS-förordningen. Beslutet om inrättandet av VIS har inte föranlett några författningsändringar i Sverige och någon annan bedömning görs inte nu med anledning av de ändringar som föreskrivs i IOF.

Genom artikel 65 i förordning (EU) 2019/817 kompletteras artiklarna 5 och 7 i VIS-rådsbeslutet med nya bestämmelser som förs in i en ny punkt 1a i respektive artikel. Artiklarna 5 och 7 i VIS-rådsbeslutet reglerar villkoren för medlemsstaternas respektive Europols åtkomst till uppgifter i systemet för brottsbekämpande ändamål. I tidigare lagstiftningsarbete har bedömningen gjorts att artikel 7 inte kräver några nationella lagstiftningsåtgärder (se Ds 2011:27 s. 117 f.). Någon annan bedömning görs inte nu med anledning av ändringen av den artikeln. Artikel 5 har däremot genomförts i svensk rätt genom 9 kap. 1 § lagen om internationellt polisiärt samarbete (se prop. 2014/15:82 s. 31 ff.). Enligt första stycket nämnda paragraf får den centrala åtkomstpunkten på begäran av behöriga myndigheter genom direktåtkomst söka uppgifter i VIS, om det i enskilda fall finns skäl att anta att uppgifter i systemet väsentligen kan komma att bidra till att utreda ett sådant terroristbrott eller annat grovt brott som omfattas av definitionerna i artikel 2.1 i VIS-rådsbeslutet. Detsamma gäller enligt andra stycket nämnda paragraf om det i enskilda fall finns skäl att anta att uppgifter i systemet väsentligen kan komma att bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i första stycket.

Enligt den nya punkten i artikel 5 får åtkomst till sökningar i VIS även ges om sökningar enligt artikel 22.2 i IOF visar att det finns uppgifter i det systemet, och villkoren i artikel 5 är uppfyllda. Tillägget kan visserligen uppfattas som en ny grund för åtkomst till uppgifter i VIS. Den förutsätter dock att en prövning av övriga villkor i artikel 5 görs innan åtkomst ges. Bestämmelsen innebär därför inte någon ändring av villkoren för åtkomst till VIS för brottsbekämpande ändamål.

Som angetts i avsnitt 8.2 är artikel 22 i IOF direkt tillämplig för medlemsstaternas utsedda myndigheter. Om det vid en sådan sökning framkommer att uppgifter om en viss person finns i VIS får den sökande myndigheten begära åtkomst till dessa. Enligt artikel 22.2 tredje stycket i IOF förutsätts även att en sådan begäran görs. Prövningen av om sökande myndighet kan beviljas åtkomst till

uppgifterna i VIS görs dock utifrån villkoren i VIS-rådsbeslutet (se artikel 22.3 i IOF). Ändringen av artikel 5 i VIS-rådsbeslutet bör mot den bakgrunden ses som ett förtydligande av att en begäran om åtkomst till uppgifter i VIS för brottsbekämpande ändamål även kan ske efter sökningar enligt artikel 22 i IOF. Någon ändring av kriterierna för sådan åtkomst verkar däremot inte avsedd. De nationella bestämmelserna som genomför artikel 5 i VIS-rådsbeslutet bedöms därför inte behöva ändras.

15.3 Slutbestämmelser

Bedömning: Slutbestämmelserna i EU:s förordningar om interoperabilitet kräver inte några författningsändringar.

Skälen för bedömningen: I kapitel X i IOF finns det ett antal slutbestämmelser. Kapitlet innehåller bl.a. bestämmelser om övergångsperioder för

- användningen av ESP (artikel 67 i förordning [EU] 2019/817 och artikel 63 i förordning [EU] 2019/818),
- åtkomst till CIR i brottsbekämpande syfte (artikel 68 i förordning [EU] 2019/817 och artikel 64 i förordning [EU] 2019/818), samt
- spårning av multipla identiteter (artikel 69 i förordning [EU] 2019/817 och artikel 65 i förordning [EU] 2019/818).

I kapitlet regleras också bl.a. användning av uppgifter för rapportering och statistik (artikel 66 i förordning [EU] 2019/817 och artikel 62 i förordning [EU] 2019/818), hantering av kostnader (artikel 70 i förordning [EU] 2019/817 och artikel 66 i förordning [EU] 2019/818) och driftstart (artikel 72 i förordning [EU] 2019/817 och artikel 68 i förordning [EU] 2019/818). Dessa bestämmelser föranleder inte några författningsändringar.

I artikel 76 i förordning (EU) 2019/817 och artikel 72 i förordning (EU) 2019/818 finns bestämmelser om eu-LISA:s och medlemsstaternas skyldigheter att tillhandahålla utbildning. Enligt

andra stycket nämnda artikel ska medlemsstaternas myndigheter tillhandahålla ett lämpligt utbildningsprogram för sin personal om datasäkerhet, uppgifters kvalitet, dataskydd, de förfaranden som är tillämpliga på uppgiftsbehandlingen samt skyldigheter att informera enskilda om länkar i MID. Bestämmelsen vänder sig till relevanta myndigheter och är direkt tillämplig. Något behov av att ytterligare reglera detta i nationell författning saknas därmed.

I kapitlet finns det också bestämmelser om att medlemsstaterna ska underrätta eu-LISA om de myndigheter som avses i artiklarna 7, 20, 21 och 26 och som får använda eller ha åtkomst till ESP, CIR respektive MID (artikel 71 i förordning [EU] 2019/817 och artikel 67 i förordning [EU] 2019/818). Bestämmelserna om underrättelseskyldighet kräver inte några författningsändringar.

Kapitlet innehåller slutligen bestämmelser om övervakning och utvärdering (artikel 78 i förordning [EU] 2019/817 och artikel 74 i förordning [EU] 2019/818). Bestämmelserna riktar sig i första hand till eu-LISA och kommissionen. Medlemsstaterna ska dock 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. Rapporterna ska innehålla viss fastställd information och statistik. Medlemsstaterna ska också förse eu-LISA och kommissionen med den information som de behöver för att utarbeta sina rapporter. Som nämns i avsnitt 3.3 har regeringen gett Polismyndigheten i uppdrag att leda samordningen av berörda myndigheters arbete med genomförandet av IOF. Polismyndigheten kommer därmed att ha mycket god kännedom om IO-komponenternas uppbyggnad och funktion samt en god överblick över användningen av dessa inom svensk statsförvaltning. Det kan vidare antas att myndigheten kommer att kunna få tillgång till den information som ska ingå i de årliga rapporterna. Polismyndigheten bör därför ansvara för att utarbeta dessa tillsammans med övriga berörda myndigheter. Samma sak gäller för den information som ska överlämnas till eu-LISA och kommissionen. Det finns inget behov av att reglera dessa uppgifter i nationell rätt.

16 Ikraftträdande- och övergångsbestämmelser

Förslag: Lagändringarna ska träda i kraft den dag som regeringen bestämmer. Övriga författningsförslag ska träda i kraft den dag som EU:s förordningar om interoperabilitet ska börja tillämpas fullt ut.

Bedömning: Det krävs inte några övergångsbestämmelser.

Skälen för förslaget och bedömningen: IOF trädde i kraft den 11 juni 2019. Vissa bestämmelser i IOF tillämpas från och med detta datum, bl.a. regler om inrättande och teknisk utformning av IO-komponenterna, kommissionens antagande av delegerade akter och genomförandeakter samt de olika aktörernas ansvarsområden innan IO-komponenterna tas i drift. Bestämmelserna i IOF om ESP, sBMS, CIR, MID och CRRS i övrigt ska börja tillämpas när de olika komponenterna tas i drift, vilket ska ske det datum som kommissionen bestämmer. Detsamma gäller bestämmelser som rör de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma uppgiftskvalitetsindikatorerna samt minimikvalitetsstandarderna för uppgifter. Kommissionen ska fastställa dagen för driftsättning när vissa villkor är uppfyllda. Det krävs bl.a. att tester av komponenterna i samarbete med medlemsstaterna har slutförts med ett tillfredställande resultat (artiklarna 72.1–72.6 och 79 i förordning [EU] 2019/817 och artiklarna 68.1–68.6 och 75 i förordning [EU] 2019/818). Enligt den nuvarande tidsplanen ska samtliga komponenter ha tagits i drift före utgången av juni 2024.

En stor del av förordningarnas tillämplighet är alltså beroende av kommissionens beslut. Eftersom det ännu är okänt vilken tidpunkt för driftsättning som kommissionen kommer att välja, bör det över-

lämnas åt regeringen att bestämma tidpunkten för ikraftträdande av de föreslagna lagändringarna. Övriga författningsförslag bör träda i kraft den dag IOF ska börja tillämpas fullt ut.

I IOF finns det vissa övergångsbestämmelser. Enligt artikel 67 i förordning (EU) 2019/817 och artikel 63 i förordning (EU) 2019/818) ska ESP under en övergångsperiod om två år från driftstarten vara frivilligt att använda för medlemsstaterna. Kommissionen får besluta om att förlänga övergångsperioden med ytterligare ett år. Vidare framgår av artikel 68 i förordning (EU) 2019/817 och artikel 64 i förordning (EU) 2019/818 bl.a. att artikel 22 i IOF ska tillämpas från den dag CIR tas i drift. Slutligen finns särskilda övergångsbestämmelser om spårning av multipla identiteter i artikel 69 i förordning (EU) 2019/817 och artikel 65 i förordning (EU) 2019/818. Det föreskrivs att Etias centralenhet, dvs. den enhet som ska inrättas vid den Europeiska gräns- och kustbevakningsbyrån (Frontex) enligt Etias-förordningen, under en ettårsperiod efter slutförandet av testerna av MID ska ansvara för att utföra spårning av multipla identiteter. Spårningarna av multipla identiteter ska då utföras med hjälp av enbart biometriska uppgifter. Verifieringen av vissa länkar till registreringar i SIS ska utföras av medlemsstaternas Sirenekontor som i sådana fall ska beviljas åtkomst till nödvändiga uppgifter i underliggande system.

Övergångsbestämmelserna i IOF är direkt tillämpliga och kräver inte några nationella författningsåtgärder. Inte heller vid sidan av den övergångsreglering som finns i IOF finns det något behov av övergångsbestämmelser.

17 Konsekvenser

Bedömning: Den nya regleringen förväntas leda till en effektivare gräns- och utlänningskontroll samt en mer effektiv brottsbekämpning.

Medlemsstaternas kostnader för genomförandet av EU:s förordningar om interoperabilitet ska finansieras av EU-medel. Kostnader som ändå kan antas uppkomma för myndigheterna ska rymmas inom befintliga ramar.

Skälen för bedömningen

Konsekvenser för gräns- och utlänningskontrollen samt för brottsbekämpningen

IOF och de kompletterande nationella bestämmelser som föreslås i den här promemorian medför en utökad reglering som får konsekvenser för såväl det allmänna som för enskilda. Det är dock främst innehållet i de direkt tillämpliga EU-förordningarna och inte i de förslag som lämnas i promemorian som innebär att dessa konsekvenser uppkommer.

Syftet med IOF är att förbättra ändamålsenligheten och effektiviteten hos in- och utresekontrollerna vid de yttre gränserna och bidra till att förebygga och bekämpa olaglig invandring. Vidare ska förordningarna bl.a. bidra till en hög säkerhetsnivå i unionen och bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott. Genom att länkar skapas mellan uppgifter i olika system kommer gränskontrollerande och brottsbekämpande myndigheter att uppmärksammas på misstänkta identitetsbedrä-

gerier. Att svenska myndigheter uppmärksammas på att personer som vill ta sig in i eller vistas i landet använder sig av olika identitetsuppgifter kan antas bidra till en förbättrad gräns- och utlänningskontroll. Detta kommer i sin tur att leda till positiva effekter för bl.a. den inre säkerheten i Sverige och övriga medlemsstater.

Möjligheten för svenska myndigheter att göra sökningar i identifieringssyfte enligt artikel 20 i IOF kommer att bidra till förbättrad kännedom om vilka utlänningar som befinner sig i landet olovligen. Dessutom förväntas sökmöjligheten leda till ett effektivare arbete med verkställighet av beslut av avvisning och utvisning. Att antalet personer som inte har rätt att vistas i landet minskar kan antas få positiva effekter bl.a. för den inre säkerheten. Vidare bedöms sökmöjligheten kunna leda till att personer lättare kan identifieras inom ramen för en brottsutredning. Detta kan resultera i att brott uppklaras snabbare och att fler gärningsmän lagförs. Artikel 22 i IOF förväntas bidra till en effektivare bekämpning av allvarlig brottslighet genom att brottsbekämpande myndigheter snabbare kan få uppgift om en misstänkt person förekommer i något av de underliggande systemen.

Ekonomiska konsekvenser

Enligt de förslag som lämnas i promemorian kommer utpekade myndigheter att få göra sökningar enligt artikel 20 i IOF i identifieringssyfte. Denna sökmöjlighet innebär dock inte någon utvidgning av myndigheternas uppdrag. Möjligheten till sådana sökningar ska i stället ses som ett verktyg som kan användas i det arbete som redan idag bedrivs hos svenska myndigheter. För att kunna utföra sökningar enligt artikeln kommer myndigheterna att behöva utveckla nödvändig teknik, t.ex. för direktscanning av fingeravtryck, vilket initialt kan innebära kostnader. Sökmöjligheten kommer dock i förlängningen att effektivisera myndigheternas arbete och därmed spara resurser.

Ansvaret för medlemsstaterna att verifiera gula länkar innebär nya arbetsuppgifter för svenska myndigheter. Det kommer att leda till vissa merkostnader för berörda myndigheter, särskilt för Polismyndigheten som förväntas stå för merparten av sådana

ärenden. Det är svårt att på förhand uppskatta hur stora resurser arbetet med att verifiera länkar kommer att ta i anspråk. Det ska dock beaktas att processen med att skapa länkar till stor del är automatiserad och att de personuppgifter som ska jämföras vid verifieringen redan finns i systemen. Vidare har den information om vita och röda länkar som enligt artikel 32.4 och 33.4 i IOF ska lämnas till den enskilde till stor del på förhand fastställts genom beslut av kommissionen. Den administrativa bördan i det enskilda fallet bedöms därför inte bli särskilt betungande för myndigheterna.

Enligt artikel 70 i förordning (EU) 2019/817 och artikel 66 i förordning (EU) 2019/818 ska kostnaderna i samband med inrättandet och driften av ESP, sBMS, CIR och MID belasta unionens allmänna budget. Detsamma gäller kostnaderna i samband med integreringen av befintliga nationella infrastrukturer och deras anslutning till de enhetliga nationella gränssnitten samt i samband med förvaltandet av de enhetliga nationella gränssnitten. Medlemsstaterna ska dock bekosta nationella projektledningskontor, hysning och drift av nationella it-system samt utveckling och drift m.m. av nationella kommunikationsnätverk. Vidare ska medlemsstaterna stå för kostnaderna för de utsedda myndigheterna och deras anslutning till CIR.

Många av de kostnader som uppkommer för svenska myndigheter bedöms kunna täckas av EU-medel. Den nya regleringen kan alltså inte antas medföra någon omfattande kostnadsökning för svenska myndigheter. Den nya regleringen förväntas också leda till en mer effektiv gränskontroll och brottsbekämpning vilket på sikt kan antas medföra kostnadsbesparingar för myndigheterna. De kostnadsökningar som ändå uppkommer bedöms inte vara större än att de ryms inom myndigheternas befintliga anslag.

Förslagen bedöms i övrigt inte ha några ekonomiska konsekvenser för det allmänna eller enskilda.

Konsekvenser för den personliga integriteten och barnets rättigheter

Genom IOF inrättas ett antal nya tekniska komponenter. Komponenterna innebär inte, med undantag för uppgifter i akten för identitetsbekräftelse och CRRS, att fler personuppgifter kommer att lagras i underliggande system. Regleringen i IOF och vissa förslag

till kompletterande nationella bestämmelser innebär dock att personuppgifter kommer att behandlas, även barns personuppgifter. Vidare kommer fotografier och fingeravtryck att tas i fler fall – eller i vart fall för fler syften – än i dag. Regleringen innebär ett visst intrång i den personliga integriteten för de enskilda som berörs.

Det kan dock konstateras att det är noga reglerat i IOF på vilket sätt och hur länge personuppgifterna får behandlas i IO-komponenterna. I artikel 5 i IOF fastslås att behandling av personuppgifter enligt förordningarna inte får leda till diskriminering av personer på någon grund, såsom kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till en nationell minoritet, förmögenhet, börd, funktionsnedsättning, ålder eller sexuell läggning. Den ska ske med fullständig respekt för mänsklig värdighet och integritet samt grundläggande rättigheter, inbegripet rätten till respekt för privatlivet och skydd av personuppgifter. Särskild hänsyn ska tas till barn, äldre, personer med funktionsnedsättning och personer i behov av internationellt skydd. Barnets bästa ska komma i främsta rummet.

Förordningarna innehåller även andra bestämmelser om skydd av personuppgifter. Vidare omfattas personuppgiftsbehandlingen av det allmänna EU-rättsliga och nationella regelverket på området. Till detta kommer de specifika dataskyddsrättsliga bestämmelser som gäller för behandling av uppgifter i respektive underliggande system.

EU vilar på respekt för människans värdighet, frihet, demokrati, jämlikhet, rättsstaten och respekt för de mänskliga rättigheterna, inbegripet rättigheter för personer som tillhör minoriteter. Som ett led i detta ska EU och medlemsstaterna respektera EU:s rättighetsstadga vid tillämpningen av unionsrätten. I skäl 40 i IOF konstateras att förordningarna föreskriver ny uppgiftsbehandling som syftar till att korrekt identifiera de berörda personerna. Vidare konstateras att detta utgör ett ingrepp i deras grundläggande rättigheter som skyddas genom artiklarna 7 och 8 i EU:s rättighetsstadga. Eftersom EU-informationssystemen är beroende av att de berörda personerna identifieras korrekt för att fungera effektivt är detta ingrepp motiverat av samma syften som lett till att vart och ett av dessa system har inrättats, nämligen en effektiv förvaltning av unionens gränser, den inre säkerheten i unionen och ett effektivt genomförande av unionens asyl- och viseringspolitik.

Enligt skälen till IOF bedöms förordningarna vara förenliga med de grundläggande rättigheter och principer som erkänns i stadgan (se skäl 83 i förordning [EU] 2019/817 och skäl 79 i förordning [EU] 2019/818). Även de bestämmelser som föreslås komplettera förordningarna står i överensstämmelse med stadgan.

Även förslagen om en skyldighet att låta sig fotograferas och lämna fingeravtryck är omgärdade av bestämmelser som syftar till att skydda den enskildes integritet. Det kan i sammanhanget konstateras att det är noga reglerat när fotografier och fingeravtryck får tas. Reglerna om förfarandet vid fotografering och fingeravtryckstagning bygger på bestämmelserna i IOF, som ska vara förenliga med EU:s rättighetsstadga. De bedöms också vara förenliga med de rättigheter och principer som fastställs i regeringsformen, Europakonventionen och barnkonventionen. Principen om barnets bästa är central vid alla åtgärder som rör barn och åtgärderna ska genomföras på ett barnvänligt och barnanpassat sätt. Den föreslagna regleringen innebär även i detta avseende sammanfattningsvis inte mer långtgående inskränkningar i den kroppsliga eller personliga integriteten än vad som är nödvändigt och godtagbart med hänsyn till ändamålen.

Övriga konsekvenser

Förslagen bedöms inte ha några konsekvenser för den kommunala självstyrelsen eller för sysselsättning eller offentlig service i olika delar av landet. De bedöms inte heller ha betydelse för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags. Förslagen bedöms slutligen inte ha någon betydelse för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

18 Författningskommentar

18.1 Förslaget till lag om ändring i utlänningslagen (2005:716)

1 kap.

Förordning (EU) 2019/817 och förordning (EU) 2019/818

4 f § *Med förordning (EU) 2019/817 avses i denna lag Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF.*

Med förordning (EU) 2019/818 avses i denna lag Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816.

Paragrafen, som är ny, anger vad som i lagen avses med förordning (EU) 2019/817 och förordning (EU) 2019/818. Hänvisningarna till förordningarna är dynamiska, dvs. avser förordningarna i den vid varje tidpunkt gällande lydelsen.

9 kap.

8 j § *En polisman eller en tjänsteman vid Kustbevakningen får vid en kontroll enligt 9 § genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och artikel 20.1–20.3 i förordning (EU) 2019/818. En utlänning är skyldig att låta en polisman eller en tjänsteman vid Kustbevakningen*

fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

När en sökning enligt första stycket har genomförts ska det fotografi och de fingeravtryck som har tagits för sökningen omedelbart förstöras om det framkommer att utlänningen har rätt att vistas i Sverige.

Paragrafen, som är ny, reglerar möjligheten att vid inre utlänningskontroll söka i EU:s gemensamma databas för identitetsuppgifter (CIR) och fotografering och fingeravtryckstagning i samband med det. Paragrafen innehåller även en bestämmelse om förstörande av uppgifter. Övervägandena finns i avsnitt 9.5.1 och 12.7.

Av *första stycket första meningen* framgår att en polisman eller en tjänsteman vid Kustbevakningen vid en inre utlänningskontroll får genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och förordning (EU) 2019/818.

Enligt artikel 20 i respektive förordning får sökningar utföras i CIR i identifieringssyfte. Sådana sökningar får genomföras vid en inre utlänningskontroll i enlighet med vad som anges i artikel 20.1–20.3.

Hänvisningen till bestämmelserna i förordning (EU) 2019/817 och förordning (EU) 2019/818 innebär att för att en sökning ska få genomföras måste det vara fråga om någon av följande fem situationer som räknas upp i artikel 20.1 första stycket i förordningarna:

- En person kan inte identifieras på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet.
- Det finns tvivel om de identitetsuppgifter som lämnats av en person.
- Det finns tvivel om äktheten i den resehandling eller annan trovärdig handling som har lämnats av en person.
- Det finns tvivel om identiteten på innehavaren av en resehandling eller en annan trovärdig handling.
- En person kan inte eller vägrar att samarbeta.

Sökningar enligt paragrafen är inte tillåtna när det gäller minderåriga under 12 år, om det inte sker för barnets bästa (artikel 20.1 andra stycket).

Vidare förutsätter en sökning att kraven i artikel 20.2 är uppfyllda. Av artikeln framgår att sökningar får göras endast i syfte att identifiera en person, med den personens biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro.

Om personens biometriska uppgifter inte kan användas eller om sökningen med dessa uppgifter misslyckas, ska sökningen utföras med identitetsuppgifter i kombination med resehandlingsuppgifter eller med de identitetsuppgifter som tillhandahållits av personen (artikel 20.3 andra stycket).

Vad som avses med förordning (EU) 2019/817 respektive förordning (EU) 2019/818 framgår av 1 kap. 4 f §.

Av *första stycket andra meningen* framgår en skyldighet för en utlänning att låta en polisman eller en tjänsteman vid Kustbevakningen fotografera honom eller henne och ta hans eller hennes fingeravtryck. Bestämmelsen innebär att skyldigheten att låta sig fotograferas och lämna fingeravtryck endast gäller om förutsättningarna är uppfyllda för att genomföra en sökning enligt första meningen. Skyldigheten gäller alltså endast när sökningar kan ske enligt artikel 20.1–20.3.

I *andra stycket* anges att när en sökning enligt första stycket har genomförts, ska det fotografi och de fingeravtryck som har tagits för sökningen omedelbart förstöras. Det gäller dock endast om det framkommer att utlänningen har rätt att vistas i Sverige. Om den utlänning vars uppgifter har tagits upp vid kontrollen däremot inte har rätt att vistas i Sverige behöver uppgifterna inte förstöras. Migrationsverket får föra separata register över de uppgifter som tas upp med stöd av denna paragraf (15 § första stycket utlänningsdatalagen [2016:27]).

Hänvisningarna till förordning (EU) 2019/817 och förordning (EU) 2019/818 är dynamiska, dvs. avser förordningarna i den vid varje tidpunkt gällande lydelsen.

13 a § *En polisman får i ett ärende om verkställighet av ett beslut om avvisning eller utvisning genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och artikel 20.1–20.3 i förordning (EU) 2019/818. En*

utlänning är skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

Paragrafen, som är ny, reglerar möjligheten att vid verkställighet av beslut om avvisning eller utvisning söka i CIR och fotografering och fingeravtryckstagning i samband med det. Övervägandena finns i avsnitt 9.5.2 och 12.6.

Av *första meningen* framgår att en polisman i ett ärende om verkställighet av ett beslut om avvisning eller utvisning får genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och förordning (EU) 2019/818. Enligt artikel 20 får sökningar utföras i CIR i identifieringssyfte. Sådana sökningar får genomföras vid verkställighet av ett beslut om avvisning eller utvisning i enlighet med vad som anges i artikel 20.1–20.3. Se om artikel 20.1–20.3 kommentaren till 8 j §. Vad som avses med förordning (EU) 2019/817 respektive förordning (EU) 2019/818 framgår av 1 kap. 4 f §.

Av *andra meningen* framgår en skyldighet för en utlänning att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck. Bestämmelsen innebär att skyldigheten att låta sig fotograferas och lämna fingeravtryck endast gäller om förutsättningarna är uppfyllda för att genomföra en sökning enligt första meningen. Skyldigheten gäller alltså endast när sökningar kan ske enligt artikel 20.1–20.3.

Hänvisningarna till förordning (EU) 2019/817 och förordning (EU) 2019/818 är dynamiska, dvs. avser förordningarna i den vid varje tidpunkt gällande lydelsen.

18.2 Förslaget till lag om ändring i utlänningsdatalagen (2016:27)

5 § Denna lag gäller inte när personuppgifter behandlas med stöd av

1. lagen (2006:444) om passagerarregister,

2. Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex),

3. Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva

en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning),

4. Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna,

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

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

7. lagen (2021:1187) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem och föreskrifter som har meddelats i anslutning till den lagen,

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

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

10. Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och

migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816.

I paragrafen anges att lagen inte gäller vid behandling av personuppgifter enligt vissa uppräknade författningar. Övervägandena finns i avsnitt 12.1. I *punkterna 9 och 10*, som är nya, hänvisas till förordning (EU) 2019/817 och förordning (EU) 2019/818. Ändringen innebär att förordningarna undantas från tillämpningsområdet för lagen.

Hänvisningarna till förordning (EU) 2019/817 och förordning (EU) 2019/818 är dynamiska, dvs. avser förordningarna i den vid varje tidpunkt gällande lydelsen.

15 § Migrationsverket får föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8, 8 h *och 8 j* §§ utlänningslagen (2005:716).

Med begränsning av de ändamål som annars gäller enligt 11 och 13 §§ får uppgifter om fingeravtryck eller fotografier i registren användas endast

1. vid prövning av ansökningar om uppehållstillstånd där skäl som anges i 4 kap. 1–2 a §§ utlänningslagen åberopas,
2. i ärenden om avvisning och utvisning,
3. i testverksamhet,
4. om det behövs för att kontrollera identiteten av en person på ett fotografi som kommit in till Migrationsverket,
5. om det behövs för att Migrationsverket ska kunna kontrollera ett fingeravtryck mot fingeravtrycks- och signalementsregister som Polismyndigheten för enligt 5 kap. 11 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, eller
6. vid kontroll av utlänningar under vistelsen i Sverige.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om vilka uppgifter som får behandlas i registren över fingeravtryck och fotografier, och
2. föreskrifter om gallring.

Paragrafen innehåller bestämmelser om Migrationsverkets behandling av fingeravtryck och fotografier. Övervägandena finns i avsnitt 12.7.

Paragrafens *första stycke* ändras på så sätt att bestämmelsen om att Migrationsverket får föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 och 8 h §§ utlänningslagen kompletteras med en hänvisning till 9 kap. 8 j § utlänningslagen. Det

innebär att även fingeravtryck och fotografier som tas vid en inre utlänningskontroll för att genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och förordning (EU) 2019/818 får föras in i de separata registren. Detta gäller inte det fotografi och de fingeravtryck som enligt 9 kap. 8 j § utlänningslagen omedelbart ska förstöras om det framkommer att utlänningen har rätt att vistas i Sverige.

18.3 Förslaget till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

1 kap.

2 § Lagen innehåller bestämmelser om operativt samarbete (2–5 kap.) och uppgiftsutbyte (6–*11* kap.).

I paragrafen anges lagens innehåll och struktur.

Ändringen innebär en upplysning om att det nya kapitel 11 handlar om uppgiftsutbyte.

3 § I lagen avses med

– *Schengenkonventionen*: konventionen om tillämpning av Schengenavtalet av den 14 juni 1985,

– *avtalet med Danmark*: avtalet av den 6 oktober 1999 mellan Konungariket Sveriges regering och Konungariket Danmarks regering om polisiärt samarbete i Öresundsregionen,

– *Öresundsförbindelsen*: den fasta förbindelsen över Öresund som den definieras i artikel 2 i avtalet med Danmark,

– *Prümrådsbeslutet*: rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet,

– *Atlasrådsbeslutet*: rådets beslut 2008/617/RIF av den 23 juni 2008 om förbättrat samarbete i krissituationer mellan Europeiska unionens medlemsstaters särskilda insatsgrupper,

– *avtalet med Norge*: avtalet av den 4 september 2018 mellan Sveriges regering och Norges regering om ömsesidigt bistånd mellan polisens särskilda insatsgrupper i krissituationer,

– *referensuppgifter*: registeruppgifter som inte röjer identiteten på en person, antingen i form av en sifferbeteckning och ett fingeravtryck eller en sifferbeteckning och en dna-profil från den ickekodifierande delen av personens dna,

– *CBE-direktivet*: Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott, i den ursprungliga lydelsen,

– *VIS-rådsbeslutet*: rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott,

– *avtalet med USA*: avtalet av den 16 december 2011 mellan Konungariket Sveriges regering och Amerikas förenta staters regering om ett förstärkt samarbete för att förebygga och bekämpa brottslighet,

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

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

I paragrafen anges vad som avses med vissa uttryck som används i lagen. Övervägandena finns i avsnitt 9.3.

Ändringen innebär att det i paragrafen anges vad som avses med förordning (EU) 2019/817 och förordning (EU) 2019/818. Hänvisningarna till förordningarna är dynamiska, dvs. avser förordningarna i den vid varje tidpunkt gällande lydelsen.

11 kap. Uppgiftsutbyte enligt förordning (EU) 2019/817 och förordning (EU) 2019/818

Sökningar i EU:s gemensamma databas för identitetsuppgifter (CIR)

1 § Den myndighet som regeringen bestämmer får genomföra sökningar enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och artikel 20.1–20.3 i förordning (EU) 2019/818 i syfte att utreda brott. Sådana sökningar får genomföras med fotografi eller fingeravtryck som har tagits med stöd av 28 kap. 14 § rättegångsbalken.

Paragrafen, som är ny, reglerar möjligheten för svenska myndigheter att i samband med brottsutredningar genomföra sökningar i EU:s gemensamma databas för identitetsuppgifter (CIR). Övervägandena finns i avsnitt 9.3.

I *första meningen* anges att den myndighet som regeringen bestämmer får genomföra sökningar enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och förordning (EU) 2019/818 i syfte att utreda brott. Sådana sökningar får endast göras om medlemsstaterna har vidtagit nationella lagstiftningsåtgärder. Paragrafen innebär att en sådan åtgärd har vidtagits. Enligt artikel 20.1–3 i förordning (EU) 2019/817 och förordning (EU) 2019/818 får medlemsstaternas polismyndigheter under vissa förutsättningar genomföra sökningar i CIR i identifieringssyfte vid identitetskontroller (se vidare kommentaren till nya 9 kap. 8 j § UtlL).

Sökning får göras i enskilda fall i syfte att utreda brott. Det innebär att sökningen måste ha en koppling till en viss brottsutredning. I *andra meningen* anges att sökningar får genomföras med fotografi eller fingeravtryck som tagits med stöd av 28 kap. 14 § rättegångsbalken. Där anges att fotografi och fingeravtryck får tas bl.a. av den som är anhållen eller häktad. Kompletterande bestämmelser finns i förordningen (1992:824) om fingeravtryck m.m. Där anges att det är obligatoriskt att ta fotografi och fingeravtryck av den som har häktats och i vissa fall även av den som har anhållits. Om det behövs för att utreda brott på vilket fängelse kan följa får fingeravtryck och fotografi tas även av andra, t.ex. av misstänkta som inte är frihetsberövade. Samma åtgärder får vidtas mot andra personer, om det behövs för att utreda brott på vilket fängelse kan följa.

I artikel 20.3 i förordning (EU) 2019/817 och förordning (EU) 2019/818 anges att om personens biometriska uppgifter inte kan användas eller om sökningen med dessa uppgifter misslyckas, ska sökningen utföras med identitetsuppgifter i kombination med resehandlingsuppgifter eller med de identitetsuppgifter som tillhandahållits av personen. Med identitetsuppgifter avses enligt IOF t.ex. för- och efternamn, födelseort, födelsedatum och medborgarskap (se artikel 4.8 i förordning (EU) 2019/817 och förordning (EU) 2019/818). Med resehandlingsuppgifter avses resehandlingens typ, nummer och utfärdandeland samt sista giltig-

hetsdag och koden på tre bokstäver för det land som utfärdat resehandlingen (se artikel 4.14 i förordning (EU) 2019/817 och förordning (EU) 2019/818). Möjligheten att söka med dessa uppgifter följer direkt av förordningarna.

Regeringen meddelar föreskrifter om vilka myndigheter som ska vara behöriga att utföra sökningar med stöd av bestämmelsen.

2 § *Den myndighet som regeringen bestämmer får genomföra sökningar enligt artikel 20.4 i förordning (EU) 2019/817 och artikel 20.4 i förordning (EU) 2019/818 om det behövs för att fastställa en avlidens identitet i samband med en naturkatastrof, olycka eller terrordåd. Sådana sökningar får genomföras med fotografi eller fingeravtryck som tagits vid en rättsmedicinsk undersökning.*

Paragrafen, som är ny, reglerar möjligheten för svenska myndigheter att genomföra sökningar i EU:s gemensamma databas för identitetsuppgifter (CIR) om det behövs för att fastställa en avlidens identitet i samband med en naturkatastrof, olycka eller terrordåd. Övervägandena finns i avsnitt 9.6.

I *första meningen* anges att den myndighet som regeringen bestämmer får genomföra sökningar enligt artikel 20.4 i förordning (EU) 2019/817 och förordning (EU) 2019/818 om det behövs för att fastställa en avlidens identitet i samband med en naturkatastrof, olycka eller terrordåd. Bestämmelsen införs på grund av krav i den EU-rättsliga regleringen om att sådana sökningar endast får göras om medlemsstaterna har vidtagit nationella lagstiftningsåtgärder.

Sökningar enligt bestämmelsen kan till exempel komma i fråga i samband med utfärdandet av bevis om dödsfall och när den avlidnes identitet inte kan fastställas på annat sätt. Av artikel 20.4 i förordning (EU) 2019/817 och förordning (EU) 2019/818 framgår att sökningar endast får ske i samband med en naturkatastrof, olycka eller terrordåd. Dessa begrepp definieras inte i förordning (EU) 2019/817 eller förordning (EU) 2019/818. Behöriga myndigheter måste därför i det enskilda fallet bedöma om situationen är sådan att en sökning kan genomföras. Mot bakgrund av det angelägna syftet att i utsatta situationer identifiera okända människor eller mänskliga kvarlevor bör begreppen inte tolkas alltför snävt. När det gäller begreppet terrordåd kan de brottsutredande myndigheternas rubricering av eventuell brottsmisstanke vara vägledande.

I *andra meningen* anges att sökningar får genomföras med fotografi eller fingeravtryck som tagits vid en rättsmedicinsk undersökning. Regler för att ta upp och behandla sådana uppgifter finns bl.a. i lagen (1995:832) om obduktion m.m. och lagen (2020:421) om Rättsmedicinalverkets behandling av personuppgifter.

Regeringen meddelar föreskrifter om vilka myndigheter som ska vara behöriga att utgöra sökningar med stöd av bestämmelsen.

Föreskrifter

***3 §** Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om uppgiftsutbyte enligt förordning (EU) 2019/817 och förordning (EU) 2019/818.*

Paragrafen, som är ny, innehåller en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om uppgiftsutbyte enligt förordning (EU) 2019/817 och förordning (EU) 2019/818.

18.4 Förslaget till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

1 kap.

Lagens tillämpningsområde

2 § Denna lag gäller inte vid behandling av personuppgifter enligt

1. vapenlagen (1996:67),
2. lagen (1998:620) om belastningsregister,
3. lagen (1998:621) om misstankeregister,
4. lagen (2006:444) om passagerarregister,
5. lagen (2014:400) om Polismyndighetens elimineringsdatabas,
6. Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna,

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

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

9. lagen (2021:1187) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem och föreskrifter som har meddelats i anslutning till den lagen,

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

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

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

I paragrafen anges att lagen inte gäller vid behandling av personuppgifter enligt vissa uppräknade författningar. Övervägandena finns i avsnitt 12.1.

I punkterna *11 och 12*, som är nya, hänvisas till förordning (EU) 2019/817 och förordning (EU) 2019/818. Ändringen innebär att dessa förordningar undantas från tillämpningsområdet för polisens brottsdatalag.

Hänvisningarna till förordning (EU) 2019/817 och förordning (EU) 2019/818 är dynamiska, dvs. avser förordningarna i den vid varje tidpunkt gällande lydelsen.

18.5 Förslaget till lag om ändring i lagen (2022:700) om särskild kontroll av vissa utlänningar

5 kap.

31 § En polisman får i ett ärende om verkställighet av ett beslut om utvisning genomföra en sökning enligt artikel 20.1–20.3 i Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF och artikel 20.1–20.3 i Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816. En utlänning är skyldig att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck för en sådan sökning.

Paragrafen, som är ny, reglerar möjligheten att vid verkställighet av beslut om utvisning söka i CIR och fotografering och fingeravtryckstagning i samband med det. Övervägandena finns i avsnitt 9.5.3 och 12.8.

Av *första meningen* framgår att en polisman i ett ärende om verkställighet av ett beslut om utvisning får genomföra en sökning enligt artikel 20.1–20.3 i förordning (EU) 2019/817 och förordning (EU) 2019/818. Enligt artikel 20 får sökningar utföras i CIR i identifieringssyfte. Sådana sökningar får genomföras vid verkställighet av ett beslut om utvisning i enlighet med vad som anges i artikel 20.1–20.3. Se om artikel 20.1–20.3 kommentaren till 9 kap. 8 j § utlänningslagen.

Av *andra meningen* framgår en skyldighet för en utlänning att låta en polisman fotografera honom eller henne och ta hans eller hennes fingeravtryck. Bestämmelsen innebär att skyldigheten att låta sig fotograferas och lämna fingeravtryck endast gäller om

förutsättningarna är uppfyllda för att genomföra en sökning enligt första meningen. Skyldigheten gäller alltså endast när sökningar kan ske enligt artikel 20.1–20.3.

Hänvisningarna till förordning (EU) 2019/817 och förordning (EU) 2019/818 är dynamiska, dvs. avser förordningarna i den vid varje tidpunkt gällande lydelsen.

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/817

av den 20 maj 2019

om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 16.2, 74 och 77.2 a, b, d och e,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande [1],

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet [2], och

av följande skäl:

(1) Kommissionen underströk i sitt meddelande av den 6 april 2016 med titeln *Starkare och smartare informationssystem för gränser och säkerhet* behovet av att förbättra unionens uppgiftshanteringsstruktur för gränsförvaltning och säkerhet. Meddelandet inledde arbetet för att uppnå interoperabilitet mellan EU-informationssystem för säkerhet, gränser och migrationshantering, i syfte att komma till rätta med de strukturella brister i systemen som hindrar de nationella myndigheternas arbete och att säkerställa att gränskontrolltjänstemän, tullmyndigheter, poliser och rättsliga myndigheter har tillgång till den information de behöver.

(2) Rådet identifierade i sin Färdplan för förbättring av informationsutbytet och informationshanteringen, inbegripet interoperabilitetslösningar på området för rättsliga och inrikes frågor av den 6 juni 2016 olika rättsliga, tekniska och operativa utmaningar när det gäller interoperabilitet mellan EU-informationssystem och efterlyste en strävan efter lösningar.

(3) I sin resolution av den 6 juli 2016 om de strategiska prioriteringarna för kommissionens arbetsprogram 2017 [3] efterlyste Europaparlamentet förslag för att förbättra och utveckla befintliga EU-informationssystem, åtgärda luckor i informationen och gå i riktning mot interoperabilitet samt förslag om obligatoriskt informationsutbyte på EU-nivå åtföljda av de bestämmelser om dataskydd som krävs.

(4) I sina slutsatser av den 15 december 2016 uppmanade Europeiska rådet till ansträngningar för att fortsatt tillhandhålla resultat i fråga om interoperabilitet mellan EU:s informationssystem och databaser.

(5) Expertgruppen för informationssystem och interoperabilitet konstaterade i sin slutrapport av den 11 maj 2017 att det var nödvändigt och tekniskt genomförbart att eftersträva praktiska lösningar för interoperabilitet, och att interoperabilitet i princip både kan ge operativa vinster och erhållas i överensstämmelse med dataskyddskraven.

[1] EUT C 283, 10.8.2018, s. 48.
[2] Europaparlamentets ståndpunkt av den 16 april 2019 (ännu ej offentliggjord i EUT) och rådets beslut av den 14 maj 2019.
[3] EUT C 101, 16.3.2018, s. 116.

(6) Kommissionen presenterade i sitt meddelande av den 16 maj 2017 med titeln *Sjunde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*, i enlighet med sitt meddelande av den 6 april 2016 och resultaten och rekommendationerna från expertgruppen för informationssystem och interoperabilitet, en ny strategi för uppgiftshantering när det gäller gränser, säkerhet och migration där alla EU-informationssystem för säkerhet, gränsförvaltning och migrationshantering kommer att vara interoperabla på ett sätt som fullt ut respekterar de grundläggande rättigheterna.

(7) I sina slutsatser av den 9 juni 2017 om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabiliteten mellan EU-informationssystem uppmanade rådet kommissionen att i sitt arbete följa de lösningar för interoperabilitet som expertgruppen föreslagit.

(8) I sina slutsatser av den 23 juni 2017 underströk Europeiska rådet behovet av att förbättra interoperabiliteten mellan databaser och uppmanade kommissionen att så snart som möjligt utarbeta förslag till lagstiftning på grundval förslagen från expertgruppen för informationssystem och interoperabilitet.

(9) I syfte att förbättra ändamålsenligheten och effektiviteten i kontrollerna vid de yttre gränserna, bidra till att förebygga och bekämpa olaglig invandring och främja en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen – bland annat att upprätthålla den allmänna säkerheten och allmänna ordningen och trygga säkerheten inom medlemsstaternas territorier – förbättra genomförandet av den gemensamma viseringspolitiken, bistå vid prövningen av ansökningar om internationellt skydd, bidra till att förebygga, förhindra, upptäcka och utreda av terroristbrott och andra grova brott, underlätta identifieringen av okända personer vid en naturkatastrof, en olycka eller ett terrordåd, i syfte att upprätthålla allmänhetens förtroende för unionens migrations- och asylsystem, unionens säkerhetsåtgärder och unionens förmåga att förvalta de yttre gränserna, bör interoperabilitet inrättas mellan EU-informationssystemen, dvs. in- och utresesystemet, Informationssystemet för viseringar (VIS), EU-systemet för reseuppgifter och resetillstånd (Etias), Eurodac, Schengens informationssystem (SIS) och det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN), så att dessa EU-informationssystem och de uppgifter som de innehåller kompletterar varandra, med respekt för den enskildes grundläggande rättigheter, i synnerhet rätten till skydd av personuppgifter. För att uppnå detta bör en europeisk sökportal (ESP), en gemensam biometrisk matchningstjänst, en gemensam databas för identitetsuppgifter (CIR) och en detektor för multipla identiteter (MID) inrättas som interoperabilitetskomponenter.

(10) Interoperabiliteten mellan EU-informationssystem bör göra det möjligt för dessa system att komplettera varandra för att underlätta korrekt identifiering av personer, däribland okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor, bidra till att bekämpa identitetsbedrägeri, förbättra och harmonisera kvalitetskraven på uppgifterna i respektive EU-informationssystem, underlätta medlemsstaternas tekniska implementering och operativa drift av EU-informationssystem, stärka de skyddsåtgärder för datasäkerhet och dataskydd som reglerar respektive EU-informationssystem, rationalisera åtkomst till in- och utresesystemet, VIS, Etias och Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, samt stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

(11) Interoperabilitetskomponenterna bör omfatta in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. De bör också omfatta Europoluppgifter, men endast i den mån som krävs för att Europoluppgifter ska kunna sökas samtidigt med dessa EU-informationssystem.

(12) Interoperabilitetskomponenterna bör behandla personuppgifterna för personer vars personuppgifter behandlas i de underliggande EU-informationssystemen och av Europol.

(13) ESP bör inrättas för att tekniskt underlätta medlemsstaternas myndigheters och unionsbyråernas snabba, smidiga, effektiva, systematiska och kontrollerade åtkomst till EU-informationssystem, Europoluppgifter och Internationella kriminalpolisorganisationens (Interpol) databaser i den mån som krävs för att de ska kunna utföra sina uppgifter, i enlighet med deras åtkomsträttigheter. ESP bör även inrättas för att stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS, Ecris-TCN och Europoluppgifter. Genom att göra det möjligt att utföra parallella

sökningar i alla relevanta EU-informationssystem, Europoluppgifter och Interpols databaser bör ESP fungera som en gemensam kontaktpunkt eller *meddelandehanterare* för att söka i de olika centrala systemen och smidigt hämta den nödvändiga informationen, med full respekt för de underliggande systemens åtkomstkontroll och dataskyddskrav.

(14) Utformningen av ESP bör, vid en sökning i Interpols databaser, säkerställa att de uppgifter som används av en ESP-användare för att inleda en sökning inte delas med ägarna av Interpols uppgifter. Utformningen av ESP bör även säkerställa att sökningar i Interpols databaser enbart sker i enlighet med tillämplig unionsrätt och nationell rätt.

(15) Interpols databas över stulna och förkomna resehandlingar (SLTD-databasen) gör det möjligt för bemyndigade enheter med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i medlemsstaterna, inklusive immigrations- och gränskontrollmyndigheter, att fastställa om en resehandling är giltig. Etias gör sökningar i databasen över stulna och förkomna resehandlingar och Interpols databas för resehandlingar som är föremål för ett meddelande (TDAWN-databasen) i samband med en bedömning av sannolikheten för att en person som ansöker om resetillstånd t.ex. kommer att migrera irreguljärt eller utgöra en säkerhetsrisk. ESP bör möjliggöra en sökning i SLTD och TDAWN med en persons identitetsuppgifter eller resehandlingsuppgifter. Om personuppgifter överförs från unionen till Interpol genom ESP bör bestämmelserna om internationella överföringar i kapitel V i Europaparlamentets och rådets förordning (EU) 2016/679 ([4]) eller de nationella bestämmelser som införlivar kapitel V i Europaparlamentets och rådets direktiv (EU) 2016/680 ([5]) tillämpas. Detta bör inte påverka tillämpningen av de särskilda regler som fastställs i rådets gemensamma ståndpunkt 2005/69/RIF ([6]) och rådets beslut 2007/533/RIF ([7]).

(16) ESP bör utvecklas och konfigureras så att det endast går att göra sådana sökningar med uppgifter som rör personer eller resehandlingar som finns i ett EU-informationssystem, i Europoluppgifter eller i Interpols databaser.

(17) För att säkerställa systematisk användning av de relevanta EU-informationssystemen bör ESP användas för att söka i CIR, in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN. En nationell uppkoppling till de olika EU-informationssystemen bör dock behållas som en teknisk reserv. ESP bör också användas av unionens byråer för att göra sökningar i centrala SIS i enlighet med deras åtkomsträttigheter och för att de ska kunna utföra sina uppgifter. ESP bör vara ytterligare ett sätt att söka i centrala SIS, Europoluppgifter och Interpols databaser, som ett komplement till de befintliga särskilda gränssnitten.

(18) Biometriska uppgifter, såsom fingeravtryck och ansiktsbilder, är unika och ger därför en mycket mer tillförlitlig identifiering av en person än alfanumeriska uppgifter. Den gemensamma biometriska matchningstjänsten bör vara ett tekniskt verktyg för att stärka och underlätta arbetet för de relevanta EU-informationssystemen och de andra interoperabilitetskomponenterna. Huvudsyftet med den gemensamma biometriska matchningstjänsten bör vara att underlätta identifiering av en person som har registrerats i flera databaser, genom att använda en enda teknisk komponent för att matcha den personens biometriska uppgifter mellan olika system, i stället för flera komponenter. Den gemensamma biometriska matchningstjänsten bör främja säkerhet och ge fördelar i fråga om kostnader, underhåll och drift. Alla automatiska fingeravtrycksidentifieringssystem, även de som för närvarande används för Eurodac, VIS och SIS, använder biometriska mallar bestående av uppgifter som härrör från en särdragsextraktion från faktiska biometriska prov. Den gemensamma biometriska matchningstjänsten bör samla och lagra alla dessa biometriska mallar – logiskt åtskilda, enligt det informationssystem från vilket uppgifterna härrör – på ett enda ställe och därigenom underlätta jämförelser mellan systemen med användning av biometriska mallar och möjliggöra stordriftsfördelar vid utveckling och underhåll av de centrala EU-systemen.

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

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

([6]) Rådets gemensamma ståndpunkt 2005/69/RIF av den 24 januari 2005 om utbyte av vissa uppgifter med Interpol (EUT L 27, 29.1.2005, s. 61).

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

(19) De biometriska mallar som lagras i den gemensamma biometriska matchningstjänsten bör bestå av uppgifter som härrör från en särdragsextraktion från faktiska biometriska prov och erhållas på ett sådant sätt att det inte går att vända på extraktionsprocessen. De biometriska mallarna bör erhållas från biometriska uppgifter, men det bör inte vara möjligt att få fram dessa biometriska uppgifter från de biometriska mallarna. Eftersom handavtryck och DNA-profiler lagras endast i SIS och inte kan inte användas för att genomföra korskontroller mot uppgifter som finns i andra informationssystem, i enlighet med principerna om nödvändighet och proportionalitet, bör den gemensamma biometriska matchningstjänsten inte lagra DNA-profiler eller biometriska mallar som erhålls från handavtryck.

(20) Biometriska uppgifter utgör känsliga personuppgifter. Denna förordning bör fastställa grunden och skyddsåtgärder för behandlingen av sådana uppgifter i syfte att entydigt identifiera de berörda personerna.

(21) In- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN kräver en korrekt identifiering av de personer vars personuppgifter lagras i dem. CIR bör därför underlätta en korrekt identifiering av personer som har registrerats i dessa system.

(22) Personuppgifter som lagras i dessa EU-informationssystem kan avse samma personer men under olika eller ofullständiga identiteter. Medlemsstaterna förfogar över effektiva metoder att identifiera sina medborgare eller personer som är registrerade som varaktigt bosatta på deras territorium. Interoperabiliteten mellan EU-informationssystem bör bidra till en korrekt identifiering av personer som är registrerade i dessa system. CIR bör lagra de personuppgifter som behövs för att göra det möjligt att mer korrekt identifiera de personer vars uppgifter lagras i de systemen, inklusive deras identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter, oavsett vilket system uppgifterna ursprungligen samlades in i. Endast de personuppgifter som är absolut nödvändiga för att utföra en korrekt identitetskontroll bör lagras i CIR. De personuppgifter som registreras i CIR bör inte behållas längre än vad som är absolut nödvändigt för de underliggande systemens syften och bör raderas automatiskt när uppgifterna har raderats i det underliggande systemet i enlighet med den logiska separeringen.

(23) En ny behandling som består i lagring av sådana uppgifter i CIR i stället för lagring i vart och ett av de separata systemen är nödvändig för att det ska vara möjligt att förbättra identifieringens tillförlitlighet genom den automatiska jämförelsen och matchningen av uppgifterna. Det faktum att identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter lagras i CIR bör inte på något sätt hindra den behandling av uppgifter som sker med avseende på in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN, eftersom CIR bör vara en ny gemensam komponent i dessa underliggande system.

(24) Det är därför nödvändigt att skapa en personakt i CIR för varje person som har registrerats i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN, för att uppnå syftet med en korrekt identifiering av personer inom Schengenområdet och för att stödja MID i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. Personakten bör lagra all den identitetsinformation som avser en person på ett enda ställe och ge vederbörligen bemyndigade slutanvändare åtkomst till den.

(25) CIR bör således underlätta och rationalisera åtkomst för myndigheter med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott till de EU-informationssystem som inte har inrättats uteslutande i syfte att förebygga, förhindra, upptäcka eller utreda grov brottslighet.

(26) CIR bör tillhandahålla en gemensam lagringsplats för identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter om personer som har registrerats i in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN. CIR bör utgöra en del av den tekniska arkitekturen i dessa system och fungera som den gemensamma komponenten mellan dem för att lagra och söka i de identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter som de behandlar.

(27) Alla poster i CIR bör separeras logiskt genom att varje post automatiskt taggas med namnet på det underliggande system som äger den uppgiften. CIR:s åtkomstkontroller bör använda dessa taggar för att avgöra huruvida åtkomst till posten ska medges.

(28) Om en medlemsstats polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet, eller om det föreligger tvivel om de identitetsuppgifter som lämnats av den personen eller om resehandlingens äkthet eller dess innehavares identitet, eller om

personen inte kan eller vägrar att samarbeta, bör polismyndigheten i fråga kunna göra en sökning i CIR för att identifiera personen. För dessa ändamål bör polisen ta fingeravtryck med hjälp av tekniker för direktscanning av fingeravtryck, under förutsättning att förfarandet inleddes i den berörda personens närvaro. Sådana sökningar i CIR bör inte tillåtas för identifiering av minderåriga under 12 år, såvida de inte görs för barnets bästa.

(29) Om en persons biometriska uppgifter inte kan användas eller en sökning med dessa uppgifter misslyckas, bör sökningen utföras med personens identitetsuppgifter i kombination med resehandlingsuppgifter. Om sökningen visar att det finns uppgifter om personen i CIR bör medlemsstaternas myndigheter ha åtkomst till CIR för att ta del av den personens identitetsuppgifter och resehandlingsuppgifter, utan att det i CIR anges vilket EU-informationssystem uppgifterna tillhör.

(30) Medlemsstaterna bör anta nationella lagstiftningsåtgärder för att utse de myndigheter som är behöriga att utföra identitetskontroller med hjälp av CIR och fastställa förfarandena, villkoren och kriterierna för sådana kontroller, vilka bör vara förenliga med proportionalitetsprincipen. I synnerhet bör befogenheten för en anställd vid en sådan myndighet att ta biometriska uppgifter av en person under en identitetskontroll föreskrivas i nationell rätt.

(31) Genom denna förordning bör det också införas en ny möjlighet till rationaliserad åtkomst till andra uppgifter än identitetsuppgifter och resehandlingsuppgifter i in- och utresesystemet, VIS, Etias eller Eurodac för medlemsstaternas utsedda myndigheter med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott samt för Europol. Sådana uppgifter kan vara nödvändiga för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i ett specifikt fall där det finns rimliga skäl att anta att en konsultation av dem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrotten eller andra aktuella grova brott, särskilt om det finns misstankar om att en person som misstänks för, har begått eller utsatts för ett terroristbrott eller ett annat grovt brott är en person vars uppgifter lagras i in- och utresesystemet, VIS, Etias eller Eurodac.

(32) Fullständig åtkomst till uppgifter som finns i in- och utresesystemet, VIS, Etias eller Eurodac som är nödvändiga för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, utöver åtkomst till identitetsuppgifter eller resehandlingsuppgifter som finns i CIR, bör även i fortsättningen regleras genom de tillämpliga rättsliga instrumenten. De utsedda myndigheterna med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott samt Europol vet inte på förhand vilket EU-informationssystem som innehåller uppgifter om de personer de behöver göra sökningar om. Detta leder till förseningar och ineffektivitet. Den slutanvändare som har bemyndigats av den utsedda myndigheten bör därför ha rätt att se i vilket av dessa EU-informationssystem de uppgifter som motsvarar resultatet av en sökning är registrerade. Det berörda systemet skulle på så vis flaggas efter den automatiska kontrollen att det finns en träff i systemet (en så kallad flaggfunktion för träff).

(33) I detta sammanhang bör ett svar från CIR inte tolkas eller användas som en grund för en slutsats om eller en anledning att vidta åtgärder med avseende på en person, utan bör användas uteslutande i syfte att lämna in begäran om åtkomst till de underliggande EU-informationssystemen, med förbehåll för de villkor och förfaranden som fastställs i respektive rättsliga instrument som reglerar sådan åtkomst. Varje sådan begäran om åtkomst bör omfattas av kapitel VII i denna förordning och i tillämpliga fall av förordning (EU) 2016/679, direktiv (EU) 2016/680 eller Europaparlamentets och rådets förordning (EU) 2018/1725 ([8]).

(34) Som en allmän regel bör de utsedda myndigheterna eller Europol begära full åtkomst till minst ett av de berörda EU-informationssystemen, om en flaggning för träff anger att uppgifterna är registrerade i in- och utresesystemet, VIS, Etias eller Eurodac. Om sådan full åtkomst i undantagsfall inte begärs – till exempel därför att de utsedda myndigheterna eller Europol redan har erhållit uppgifterna på annat sätt eller att erhållandet av uppgifterna inte längre är tillåtet enligt nationell rätt – bör motiveringen till att inte begära åtkomst registreras.

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

(35) Loggarna över sökningarna i CIR bör visa syftet med sökningarna. Om en sådan sökning har gjorts med tvåstegsstrategin för sökningar bör loggarna innehålla en referens till den nationella akten för utredningen eller ärendet, och därmed ange att sökningen gjordes för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

(36) Den sökning i CIR som görs av de utsedda myndigheterna och Europol för att få ett svar i form av en flaggning som anger att uppgifterna finns i in- och utresesystemet, VIS, Etias eller Eurodac kräver automatiserad behandling av personuppgifter. En flaggning för träff bör inte avslöja några personuppgifter om den berörda personen, utan endast en angivelse om att vissa uppgifter om vederbörande lagras i ett av systemen. Den bemyndigade slutanvändaren bör inte fatta några negativa beslut om den berörda personen endast utifrån det faktum att en sökning gett en flaggning för träff. Slutanvändarens åtkomst till en flaggning för träff kommer därför utgöra ett mycket begränsat ingrepp i den berörda personens rätt till skydd av personuppgifter, samtidigt som det ger de utsedda myndigheterna och Europol möjlighet att på ett mer effektivt sätt begära åtkomst till personuppgifter.

(37) MID bör inrättas för att stödja CIR i dess funktion och för att stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. För att effektivt uppfylla sina respektive syften kräver alla dessa EU-informationssystem en korrekt identifiering av de personer vars personuppgifter lagras i dem.

(38) För att bättre förverkliga syftena med EU-informationssystemen bör de myndigheter som använder dessa system kunna utföra en tillräckligt tillförlitlig verifiering av identiteten på de personer vars uppgifter lagras i olika system. Den uppsättning identitetsuppgifter eller resehandlingsuppgifter som lagras i ett visst enskilt system kan vara inkorrekt, ofullständig eller falsk, och i dagsläget finns det inget sätt att upptäcka inkorrekta, ofullständiga eller falska identitetsuppgifter eller resehandlingsuppgifter genom jämförelser med uppgifter som lagras i ett annat system. För att råda bot på denna situation är det nödvändigt att på unionsnivå ha ett tekniskt instrument som möjliggör en korrekt identifiering av personer för dessa ändamål.

(39) MID bör skapa och lagra länkar mellan uppgifter i de olika EU-informationssystemen för att spåra multipla identiteter, i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. MID bör endast innehålla länkar mellan uppgifter om personer som har registrerats i fler än ett EU-informationssystem. De länkade uppgifterna bör vara strikt begränsade till de uppgifter som krävs för att verifiera att en person har registrerats på ett berättigat eller oberättigat sätt med olika identiteter i olika system, eller för att klargöra att två personer med liknandeidentitetsuppgifter kanske inte är samma person. Behandlingen av uppgifter genom ESP och den gemensamma biometriska matchningstjänsten för att länka personakter mellan olika system bör hållas till ett absolut minimum och är således begränsad till spårning av multipla identiteter, som ska ske vid den tidpunkt då nya uppgifter läggs till i ett av de system som har uppgifter lagrade i CIR eller som lagts till i SIS. MID bör omfatta skyddsåtgärder mot potentiell diskriminering och ogynnsamma beslut mot personer som lagligen har multipla identiteter.

(40) I denna förordning föreskrivs ny uppgiftsbehandling som syftar till att korrekt identifiera de berörda personerna. Detta utgör ett ingrepp i deras grundläggande rättigheter som skyddas genom artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Eftersom EU-informationssystemen är beroende av att de berörda personerna identifieras korrekt för att fungera effektivt är detta ingrepp motiverat av samma syften som lett till att vart och ett av dessa system har inrättats, nämligen en effektiv förvaltning av unionens gränser, den inre säkerheten i unionen och ett effektivt genomförande av unionens asyl- och viseringspolitik.

(41) ESP och den gemensamma biometriska matchningstjänsten bör jämföra uppgifter om personer i CIR och SIS när en nationell myndighet eller en unionsbyrå skapar eller laddar upp nya uppgifter. Dessa jämförelser bör göras automatiskt. CIR och SIS bör använda den gemensamma biometriska matchningstjänsten för att upptäcka möjliga länkar på grundval av biometriska uppgifter. CIR och SIS bör använda ESP för att upptäcka möjliga länkar på grundval av alfanumeriska uppgifter. CIR och SIS bör kunna identifiera identiska eller liknande uppgifter om en person vilka är lagrade i flera system. När så är fallet bör en länk som anger att det är samma person skapas. CIR och SIS bör konfigureras på ett sätt som gör att små translittereringsfel eller stavfel upptäcks, så att det inte skapar omotiverade olägenheter för den berörda personen.

(42) Den nationella myndighet eller unionsbyrå som registrerade uppgifterna i respektive EU-informationssystem bör bekräfta eller ändra länkarna. Denna nationella myndighet eller unionsbyrå bör ha åtkomst till de uppgifter som lagras i CIR eller SIS och i MID för manuell verifiering av olika identiteter.

(43) En manuell verifiering av olika identiteter bör säkerställas av den myndighet som skapat eller uppdaterat de uppgifter som lett till en träff som ger upphov till en länk med uppgifter som lagras i ett annat EU-informationssystem. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter bör bedöma om det finns multipla identiteter som på ett berättigat eller oberättigat sätt hänvisar till en och samma person. En sådan bedömning bör om möjligt utföras i den berörda personens närvaro och när så är nödvändigt genom att begära ytterligare klargöranden eller information. Bedömningen bör göras utan dröjsmål, i enlighet med de rättsliga kraven på korrekt information enligt unionsrätten och nationell rätt. Särskilt vid gränserna kommer de berörda personernas rörelsefrihet begränsas under tiden för verifieringen, som därför inte bör äga rum på obestämd tid. Förekomsten av en gul länk i MID bör inte i sig utgöra ett skäl för nekad inresa, och ett beslut om att tillåta eller neka inresa bör fattas endast på grundval av de tillämpliga bestämmelserna i Europaparlamentets och rådets förordning (EU) 2016/399 ([9]).

(44) För länkar som erhålls genom SIS med registreringar avseende personer som är efterlysta för att gripas och överlämnas eller för att utlämnas, försvunna eller utsatta personer, personer som söks för att delta i ett rättsligt förfarande och personer som omfattas av diskreta kontroller, undersökningskontroller eller särskilda kontroller bör den myndighet som ansvarar för manuell verifiering av olika identiteter vara Sirenekontoret i den medlemsstat som har skapat registreringen. Dessa kategorier av SIS-registreringar är känsliga och bör inte nödvändigtvis delas med de myndigheter som skapar eller uppdaterar uppgifter som länkas till dem i ett av de andra EU-informationssystemen. Skapandet av en länk med SIS-uppgifter bör inte påverka de åtgärder som ska vidtas i enlighet med Europaparlamentets och rådets förordningar (EU) 2018/1860 ([10]), (EU) 2018/1861 ([11]) och (EU) 2018/1862 ([12]).

(45) Skapandet av sådana länkar förutsätter öppenhet gentemot berörda personer. För att underlätta genomförandet av nödvändiga skyddsåtgärder i enlighet med unionens tillämpliga dataskyddsbestämmelser bör personer som är föremål för en röd länk eller en vit länk efter manuell verifiering av olika identiteter informeras skriftligen utan att det påverkar tillämpningen av begränsningar för att trygga säkerheten och den allmänna ordningen, förebygga och förhindra brott samt garantera att nationella utredningar inte äventyras. Dessa personer bör erhålla ett enda identifikationsnummer som gör det möjligt för dem att identifiera den myndighet till vilken de bör vända sig för att utöva sina rättigheter.

(46) Om en gul länk skapas bör den myndighet som ansvarar för manuell verifiering av olika identiteter ha åtkomst till MID. Om det finns en röd länk bör medlemsstaternas myndigheter och unionens byråer som har åtkomst till minst ett EU-informationssystem som ingår i CIR eller till SIS ha åtkomst till MID. En röd länk bör visa att en person använder olika identiteter på ett oberättigat sätt eller att en person använder någon annan persons identitet.

(47) När det förekommer en vit eller grön länk mellan uppgifter från två EU-informationssystem bör medlemsstaternas myndigheter och unionens byråer ha åtkomst till MID, om den berörda myndigheten eller byrån har åtkomst till båda informationssystemen. Sådan åtkomst bör beviljas endast i syfte att göra det möjligt för den myndigheten eller byrån att upptäcka potentiella fall där uppgifter har länkats inkorrekt eller behandlats i MID, CIR och SIS i strid med denna förordning samt för att vidta åtgärder för att avhjälpa bristerna och uppdatera eller radera länken.

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

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

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

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

(48) Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EU-LISA) bör inrätta automatiserade mekanismer för kvalitetskontroll av uppgifter och gemensamma indikatorer för uppgiftskvalitet. EU-LISA bör ansvara för att utveckla en central övervakningskapacitet för uppgiftskvalitet och regelbundet utarbeta dataanalysrapporter för att förbättra kontrollen av medlemsstaternas implementering av EU-informationssystemen. De gemensamma indikatorerna för uppgiftskvalitet bör inbegripa minimikvalitetsstandarder för lagring av uppgifter i EU-informationssystemen eller interoperabilitetskomponenter. Målet med sådana standarder för uppgiftskvalitet bör vara att EU-informationssystemen och interoperabilitetskomponenterna automatiskt ska kunna identifiera inmatade uppgifter som verkar vara inkorrekta eller inkonsekventa, så att ursprungsmedlemsstaten kan verifiera uppgifterna och vidta de korrigerande åtgärder som behövs.

(49) Kommissionen bör utvärdera EU-LISA:s kvalitetsrapporter och utfärda rekommendationer till medlemsstaterna när så är lämpligt. Medlemsstaterna bör ansvara för utarbetandet av en handlingsplan som beskriver åtgärder för att rätta till eventuella brister i uppgifternas kvalitet och bör regelbundet rapportera om framstegen.

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

(51) Möjligheten kan övervägas att införa UMF-standarden i VIS, SIS och alla andra befintliga eller nya gränsöverskridande modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor vilka utvecklas av medlemsstaterna.

(52) En central databas för rapporter och statistik (CRRS) bör inrättas för att generera systemöverskridande statistiska uppgifter och analytisk rapportering för verksamhetsstyrande och operativa syften samt för uppgiftskvalitet i enlighet med tillämpliga rättsliga instrument. EU-LISA bör inrätta, implementera och hysa CRRS i sina tekniska anläggningar. Den bör innehålla anonymiserade statistiska uppgifter från EU-informationssystemen, CIR, MID och den gemensamma biometriska matchningstjänsten. Uppgifterna i CRRS bör inte möjliggöra identifiering av enskilda personer. EU-LISA bör automatiskt anonymisera uppgifterna och registrera de anonymiserade uppgifterna i CRRS. Anonymiseringsprocessen bör vara automatisk, och EU-LISA:s personal bör inte beviljas direkt åtkomst till några personuppgifter som lagras i EU-informationssystemen eller i interoperabilitetskomponenterna.

(53) Förordning (EU) 2016/679 är tillämplig på de nationella myndigheternas behandling av personuppgifter i interoperabilitetssyfte inom ramen för denna förordning, förutom om behandlingen görs av medlemsstaternas utsedda myndigheter eller centrala kontaktpunkter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

(54) Direktiv (EU) 2016/680 är tillämpligt i de fall medlemsstaternas behandling av personuppgifter utförs av de behöriga myndigheterna i interoperabilitetssyfte i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

(55) Förordning (EU) 2016/679, förordning (EU) 2018/1725 eller, i tillämpliga fall, direktiv (EU) 2016/680 tillämpas på överföringar av personuppgifter till tredjeländer eller internationella organisationer som utförs enligt den här förordningen. Utan att det påverkar grunderna för överföring enligt kapitel V i förordning (EU) 2016/679 eller, i tillämpliga fall, direktiv (EU) 2016/680, bör en dom i en domstol eller ett beslut av en administrativ myndighet i ett tredjeland som kräver att en personuppgiftsansvarig eller ett personuppgiftsbiträde ska överföra eller offentliggöra personuppgifter erkännas eller verkställas på något sätt endast om domen eller beslutet grundar sig på ett internationellt avtal som är i kraft mellan det begärande tredjelandet och unionen eller en medlemsstat.

(56) De särskilda bestämmelserna om dataskydd i Europaparlamentets och rådets förordningar (EU) 2017/2226 ([13]), (EG) nr 767/2008 ([14]), (EU) 2018/1240 ([15]) och förordning (EU) 2018/1861 är tillämpliga på behandlingen av personuppgifter i de system som regleras genom dessa förordningar.

(57) Förordning (EU) 2018/1725 är tillämplig på behandling av personuppgifter som utförs av EU-LISA och unionens andra institutioner och organ när de fullgör sina skyldigheter enligt den här förordningen, utan att det påverkar tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/794 ([16]), som är tillämplig på Europols behandling av personuppgifter.

(58) De tillsynsmyndigheter som avses i förordning (EU) 2016/679 eller direktiv (EU) 2016/680 bör övervaka lagligheten i medlemsstaternas behandling av personuppgifter. Europeiska datatillsynsmannen bör övervaka unionsinstitutionernas och unionsorganens behandling av personuppgifter. Europeiska datatillsynsmannen och tillsynsmyndigheterna bör samarbeta med varandra vid övervakningen av interoperabilitetkomponenternas behandling av personuppgifter. För att Europeiska datatillsynsmannen ska kunna utföra sina uppgifter enligt den här förordningen krävs tillräckliga både personella och ekonomiska resurser.

(59) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ([17]) och avgav ett yttrande den 16 april 2018 ([18]).

(60) Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (artikel 29-gruppen) avgav ett yttrande den 11 april 2018.

(61) Både medlemsstaterna och EU-LISA bör ha säkerhetsplaner för att underlätta genomförandet av säkerhetsskyldigheterna och bör samarbeta med varandra för att hantera säkerhetsproblem. EU-LISA bör också se till att man fortlöpande utnyttjar den senaste tekniska utvecklingen för att säkerställa dataintegritet i fråga om utveckling, utformning och förvaltning av interoperabilitetskomponenterna. EU-LISA:s skyldigheter i detta avseende bör omfatta antagande av nödvändiga åtgärder för att förhindra åtkomst för obehöriga personer, såsom personal hos externa tjänsteleverantörer, till personuppgifter som behandlas genom interoperabilitetskomponenterna. Vid tilldelning av kontrakt för tillhandahållande av tjänster bör medlemsstaterna och EU-LISA överväga alla de åtgärder som krävs för att säkerställa efterlevnaden av lagar eller andra författningar om skydd av personuppgifter och den enskildes integritet eller för att skydda väsentliga säkerhetsintressen i enlighet med Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 ([19]) och tillämpliga internationella konventioner. EU-LISA bör tillämpa principerna om inbyggt integritetsskydd och integritetsskydd som standard under utvecklingen av interoperabilitetskomponenterna.

(62) Implementeringen av de interoperabilitetskomponenter som föreskrivs i denna förordning kommer att påverka hur kontroller utförs vid gränsövergångsställen. Denna påverkan följer av den kombinerade tillämpningen av de befintliga reglerna i förordning (EU) 2016/399 och de regler om interoperabilitet som fastställs i den här förordningen.

(63) Till följd av denna kombinerade tillämpning av reglerna bör ESP utgöra den huvudsakliga åtkomstpunkten för den obligatoriska, systematiska sökning i databaser avseende personer vid gränsövergångsställen vilken föreskrivs i förordning (EU) 2016/399. Dessutom bör gränskontrolltjänstemännen beakta de identitetsuppgifter eller resehandlingsuppgifter som har lett till att en länk i MID klassificerades som en röd länk när de bedömer

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

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

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

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

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

([18]) EUT C 233, 4.7.2018, s. 12.

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

huruvida en person uppfyller de inresevillkor som anges i förordning (EU) 2016/399. Förekomsten av en röd länk bör dock inte i sig utgöra ett skäl för nekad inresa, och de befintliga skäl för nekad inresa som anges i förordning (EU) 2016/399 bör därför inte ändras.

(64) Det vore lämpligt att uppdatera den praktiska handledningen för gränsbevakningspersonal för att uttryckligen förtydliga detta.

(65) Om en sökning i MID genom ESP resulterar i en gul länk eller upptäcker en röd länk, bör gränskontrolltjänstemannen söka i CIR eller SIS eller båda för att bedöma informationen om den person som kontrolleras, för att manuellt verifiera personens identitetsuppgifter och vid behov anpassa länkens färg.

(66) Till stöd för statistik och rapportering är det nödvändigt att bevilja bemyndigad personal vid de behöriga myndigheter, unionsinstitutioner och unionsbyråer som avses i denna förordning åtkomst till vissa uppgifter som rör vissa interoperabilitetskomponenter utan att möjliggöra identifiering av enskilda personer.

(67) För att de medlemsstaternas myndigheter och unionsbyråerna ska kunna anpassa sig till de nya kraven beträffande användningen av ESP är det nödvändigt att föreskriva en övergångsperiod. Likaledes bör övergångsåtgärder fastställas för driftsättningen av MID för att den ska fungera konsekvent och optimalt.

(68) Eftersom målet för denna förordning, nämligen att inrätta en ram för interoperabilitet mellan EU-informationssystem, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(69) Det återstående beloppet i den budget som öronmärkts för smarta gränser i Europaparlamentets och rådets förordning (EU) nr 515/2014 ([20]) bör omfördelas till den här förordningen, i enlighet med artikel 5.5 b i förordning (EU) nr 515/2014, för att täcka kostnaderna för utveckling av interoperabilitetskomponenterna.

(70) För att komplettera vissa detaljerade tekniska aspekter i denna förordning bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) delegeras till kommissionen med avseende på

— förlängning av övergångsperioden för användning av ESP,

— förlängning av övergångsperioden för spårning av multipla identiteter som utförs av Etias centralenhet,

— förfarandena för att fastställa de fall där identitetsuppgifterna kan betraktas som desamma eller liknande,

— reglerna för driften av CRRS, däribland särskilda skyddsåtgärder för behandling av personuppgifter och säkerhetsregler tillämpliga på databasen, samt

— närmare regler om driften av webbportalen.

Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([21]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

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

([20]) Europaparlamentets och rådets förordning (EU) nr 515/2014 av den 16 april 2014 om inrättande, som en del av fonden för inre säkerhet, av ett instrument för ekonomiskt stöd för yttre gränser och visering och om upphävande av beslut nr 574/2007/EG (EUT L 150, 20.5.2014, s. 143).

([21]) EUT L 123, 12.5.2016, s. 1.

(72) Kommissionen bör även tilldelas genomförandebefogenheter med avseende på antagande av närmare bestämmelser om tekniska detaljer i användarprofilerna för ESP, specifikationer för den tekniska lösningen som gör det möjligt att utföra sökningar i EU-informationssystemen, Europoluppgifter och Interpols databaser genom ESP samt formatet för svaren från ESP, tekniska regler för att skapa länkar i MID mellan uppgifter från olika EU-informationssystem, innehållet i och utformningen av det formulär som ska användas för att informera den registrerade när en röd länk skapas, prestandakrav och prestandaövervakning för den gemensamma biometriska matchningstjänsten, mekanismer, förfaranden och indikatorer för automatiserad kontroll av uppgiftskvalitet, utveckling av UMF-standarden, det samarbetsförfarande som ska användas i händelse av säkerhetsincidenter, samt specifikationerna för den tekniska lösningen för medlemsstaternas hantering av åtkomstbegäranden från användare. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([22]).

(73) Eftersom interoperabilitetskomponenterna kommer att medföra behandling av betydande mängder känsliga personuppgifter är det viktigt att personer vars uppgifter behandlas genom dessa komponenter i praktiken kan utöva sina rättigheter som registrerade i enlighet med förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725. De registrerade bör få tillgång till en webbportal som gör det lättare för dem att utöva sin rätt till åtkomst till och rättelse, radering och begränsning av behandlingen av deras personuppgifter. EU-LISA bör inrätta och förvalta en sådan webbportal.

(74) En av huvudprinciperna i samband med dataskydd är uppgiftsminimering. Enligt artikel 5.1 c i förordning (EU) 2016/679 ska de personuppgifter som behandlas vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Interoperabilitetskomponenterna bör därför inte lagra några nya personuppgifter, med undantag för de länkar som kommer att lagras i MID och som utgör det minimum som krävs för tillämpningen av den här förordningen.

(75) Denna förordning bör innehålla tydliga bestämmelser om ansvar och rätten till ersättning vid otillåten behandling av personuppgifter och vid någon annan åtgärd som är oförenlig med den. Sådana bestämmelser bör inte påverka rätten till ersättning från samt ansvaret för den personuppgiftsansvarige eller personuppgiftsbiträdet enligt förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725. EU-LISA bör vara ansvarig för skada som den orsakat i sin egenskap av personuppgiftsbiträde om byrån inte har fullgjort de skyldigheter som den specifikt har ålagts enligt den här förordningen eller om den har agerat utanför eller i strid med lagenliga instruktioner från den medlemsstat som är personuppgiftsansvarig.

(76) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2004/38/EG ([23]).

(77) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, deltar Danmark inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Danmark. Eftersom denna förordning är en utveckling av Schengenregelverket ska Danmark, i enlighet med artikel 4 i det protokollet, inom sex månader efter det att denna förordning har antagits, besluta huruvida landet ska genomföra den i sin nationella rätt.

(78) Denna förordning utgör en utveckling av de bestämmelser i Schengenregelverket i vilka Förenade kungariket inte deltar i enlighet med rådets beslut 2000/365/EG ([24]). Förenade kungariket deltar därför inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Förenade kungariket.

(79) Denna förordning utgör en utveckling av de bestämmelser i Schengenregelverket i vilka Irland inte deltar i enlighet med rådets beslut 2002/192/EG ([25]). Irland deltar därför inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Irland.

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

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

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

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

(80) När det gäller Island och Norge utgör denna förordning, i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([26]), en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.A, 1.B, 1.C och 1.G i rådets beslut 1999/437/EG ([27]).

(81) När det gäller Schweiz utgör denna förordning, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av de bestämmelser i Schengenregelverket ([28]) som omfattas av det område som avses i artikel 1.A, 1.B, 1.C och 1.G i beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2008/146/EG ([29]).

(82) När det gäller Liechtenstein utgör denna förordning, i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av de bestämmelser i Schengenregelverket ([30]) som omfattas av det område som avses i artikel 1.A, 1.B, 1.C och 1.G i beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2011/350/EU ([31]).

(83) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns i synnerhet i Europeiska unionens stadga om de grundläggande rättigheterna, och bör tillämpas i enlighet med dessa rättigheter och principer.

(84) För att denna förordning ska passa in i den befintliga rättsliga ramen bör förordningarna (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 ([32]) och 2008/633/RIF ([33]) ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. Genom denna förordning tillsammans med Europaparlamentets och rådets förordning (EU) 2019/818 ([34]) 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).

([26]) EGT L 176, 10.7.1999, s. 36.
([27]) Rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtal som har ingåtts mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EGT L 176, 10.7.1999, s. 31.)
([28]) EUT L 53, 27.2.2008, s. 52.
([29]) Rådets beslut 2008/146/EG av den 28 januari 2008 om ingående på Europeiska gemenskapens vägnar av avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 53, 27.2.2008, s. 1.)
([30]) EUT L 160, 18.6.2011, s. 21.
([31]) Rådets beslut 2011/350/EU av den 7 mars 2011 om ingående på Europeiska unionens vägnar av protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, om avskaffande av kontroller vid de inre gränserna och om personers rörlighet (EUT L 160, 18.6.2011, s. 19).
([32]) Rådets beslut 2004/512/EG av den 8 juni 2004 om inrättande av Informationssystemet för viseringar (VIS) (EUT L 213, 15.6.2004, s. 5).
([33]) Rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott (EUT L 218, 13.8.2008, s. 129).
([34]) Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och rättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816 (se sidan 85 i detta nummer av EUT).

2. Denna ram ska omfatta följande interoperabilitetskomponenter:

a) En europeisk sökportal (ESP).

b) En gemensam biometrisk matchningstjänst.

c) En gemensam databas för identitetsuppgifter (CIR).

d) En detektor för multipla identiteter (MID).

3. Denna förordning innehåller också bestämmelser om kraven på uppgifternas kvalitet, ett universellt meddelandeformat (UMF), en central databas för rapporter och statistik (CRRS) och om ansvarsområden för medlemsstaterna och Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EU-LISA) vad gäller utformningen, utvecklingen och driften av interoperabilitetskomponenterna.

4. Genom denna förordning anpassas också förfarandena och villkoren för att de utsedda myndigheterna och Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) ska få åtkomst till in- och utresesystemet, VIS, Etias och Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

5. I denna förordning fastställs också ramar för verifiering av personers identitet och för identifiering av personer.

Artikel 2

Mål

1. Genom att säkerställa interoperabilitet har denna förordning följande mål:

a) Förbättra ändamålsenligheten och effektiviteten hos in- och utresekontrollerna vid de yttre gränserna.

b) Bidra till att förebygga och bekämpa olaglig invandring.

c) Bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, bland annat att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier.

d) Förbättra genomförandet av den gemensamma viseringspolitiken.

e) Bistå vid prövningen av en ansökan om internationellt skydd.

f) Bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott.

g) Underlätta identifieringen av okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor vid en naturkatastrof, olycka eller ett terrordåd.

2. De mål som avses i punkt 1 ska uppnås genom att

a) säkerställa en korrekt identifiering av personer,

b) bidra till kampen mot identitetsbedrägerier,

c) förbättra uppgiftskvaliteten och harmonisera kvalitetskraven på uppgifter som lagras i EU-informationssystemen, samtidigt som kraven avseende uppgiftsbehandling i de rättsliga instrument som reglerar de enskilda systemen samt normerna och principerna för dataskydd respekteras,

d) underlätta och stödja medlemsstaternas tekniska implementering och operativa drift av EU-informationssystem.

e) skärpa och förenkla de villkor för datasäkerhet och dataskydd som reglerar de respektive EU-informationssystemen och göra dem mer enhetliga, utan att det påverkar det särskilda skyddet och de särskilda skyddsåtgärderna för vissa kategorier av uppgifter,

f) rationalisera villkoren för utsedda myndigheters åtkomst till in- och utresesystemet, VIS, Etias och Eurodac, samtidigt som nödvändiga och proportionella villkor för denna åtkomst säkerställs,

g) stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

Artikel 3

Tillämpningsområde

1. Denna förordning ska tillämpas på in- och utresesystemet, VIS, Etias och SIS.

2. Denna förordning ska tillämpas på personer vars personuppgifter får behandlas i de EU-informationssystem som avses i punkt 1 i den här artikeln och vilkas uppgifter samlas in för de ändamål som fastställs i artiklarna 1 och 2 i förordning (EG) nr 767/2008, artikel 1 i förordning (EU) 2017/2226, artiklarna 1 och 4 i förordning (EU) 2018/1240, artikel 1 i förordning (EU) 2018/1860 och artikel 1 i förordning (EU) 2018/1861.

Artikel 4

Definitioner

I denna förordning avses med

1. *yttre gränser*: yttre gränser enligt definitionen i artikel 2.2 i förordning (EU) 2016/399,

2. *in- och utresekontroller*: in- och utresekontroller enligt definitionen i artikel 2.11 i förordning (EU) 2016/399,

3. *gränsmyndighet*: den gränskontrolltjänsteman som i enlighet med nationell rätt tilldelats uppgiften att genomföra in- och utresekontroller,

4. *tillsynsmyndigheter*: den tillsynsmyndighet som avses i artikel 51.1 i förordning (EU) 2016/679 och den tillsynsmyndighet som avses i artikel 41.1 i direktiv (EU) 2016/680,

5. *verifiering*: förfarandet att jämföra en uppsättning uppgifter med en annan för att fastställa om en påstådd identitet är riktig (*one-to-one-check*),

6. *identifiering*: förfarandet att fastställa en persons identitet genom en databassökning mot flera grupper av uppgifter (*one-to-many-check*),

7. *alfanumeriska uppgifter*: uppgifter som återges med bokstäver, siffror, specialtecken, mellanslag och skiljetecken,

8. *identitetsuppgifter*: de uppgifter som avses i artikel 27.3 a–e,

9. *fingeravtrycksuppgifter*: bilder av fingeravtryck och bilder av fingeravtryckssp˚r som på grund av sin unika karaktär och de referenspunkter som de innefattar möjliggör exakta och entydiga jämförelser för att fastställa en persons identitet,

10. *ansiktsbild*: digitala bilder av en persons ansikte,

11. *biometriska uppgifter*: fingeravtrycksuppgifter eller ansiktsbilder, eller båda,

12. *biometrisk mall*: en matematisk representation som erhålls genom särdragsextraktion från biometriska uppgifter och som är begränsad till de egenskaper som är nödvändiga för att utföra identifikationer och verifieringar,

13. *resehandling*: pass eller motsvarande handling som ger innehavaren rätt att passera de yttre gränserna och i vilken en visering kan föras in,

14. *resehandlingsuppgifter*: resehandlingens typ, nummer och utfärdandeland samt sista giltighetsdag och koden på tre bokstäver för det land som utfärdat resehandlingen,

15. *EU-informationssystem*: in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN,

16. *Europoluppgifter*: de personuppgifter som behandlas av Europol för det syfte som avses i artikel 18.2 a, b och c i förordning (EU) 2016/794,

17. *Interpols databaser*: Interpols databas över stulna och förkomna resehandlingar (SLTD-databasen) och Interpols databas för resehandlingar som är föremål för ett meddelande (TDAWN-databasen),

18. *träff*: förekomsten av en motsvarighet till följd av en automatisk jämförelse mellan personuppgifter som har registrerats eller håller på att registreras i ett informationssystem eller en databas,

19. *polismyndighet*: behörig myndighet enligt definitionen i artikel 3.7 i direktiv (EU) 2016/680,

20. *utsedda myndigheter*: medlemsstaternas utsedda myndigheter enligt definitionen i artikel 3.1.26 i förordning (EU) 2017/2226, artikel 2.1 e i beslut 2008/633/RIF och artikel 3.1.21 i förordning (EU) 2018/1240,

21. *terroristbrott*: ett brott enligt nationell rätt som motsvarar eller är likvärdigt med ett av de brott som avses i Europaparlamentets och rådets direktiv (EU) 2017/541 ([35]),

22. *grovt brott*: ett brott som motsvarar eller är likvärdigt med ett av de brott som avses i artikel 2.2 i rådets rambeslut 2002/584/RIF ([36]) om det enligt nationell rätt kan leda till fängelse eller annan frihetsberövande åtgärd under en maximal tidsperiod på minst tre år,

23. *in- och utresesystemet*: det in- och utresesystem som inrättats genom förordning (EU) 2017/2226,

24. *Informationssystemet för viseringar* eller *VIS*: det informationssystem för viseringar som inrättats genom förordning (EG) nr 767/2008,

25. *EU-systemet för reseuppgifter och resetillstånd* eller *Etias*: det EU-system för reseuppgifter och resetillstånd som inrättats genom förordning (EU) 2018/1240,

26. *Eurodac*: som inrättats genom Europaparlamentets och rådets förordning (EU) nr 603/2013 ([37]),

27. *Schengens informationssystem* eller *SIS*: Schengens informationssystem som inrättats genom förordning (EU) 2018/1860, förordning (EU) 2018/1861 och förordning (EU) 2018/1862,

28. *Ecris-TCN*: det centraliserade system för identifiering av medlemsstater som innehar uppgifter ur kriminalregister avseende tredjelandsmedborgare och statslösa personer som inrättats genom Europaparlamentets och rådets förordning (EU) 2019/816 ([38]).

Artikel 5

Icke-diskriminering och grundläggande rättigheter

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

KAPITEL II

Den europeiska sökportalen

Artikel 6

Den europeiska sökportalen

1. En europeisk sökportal (ESP) ska inrättas för att underlätta medlemsstaternas myndigheters och unionsbyråernas möjligheter att få snabb, kontinuerlig, effektiv, systematisk och kontrollerad åtkomst till EU-informationssystemen, Europoluppgifter och Interpols databaser som krävs för att de ska kunna utföra sina uppgifter, i enlighet med sina åtkomsträttigheter och målen för och syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

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

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

([37]) Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 180, 29.6.2013, s. 1).

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

2. ESP ska bestå av följande:

a) En central infrastruktur, inbegripet en sökportal som gör det möjligt att samtidigt söka i in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN samt i Europoluppgifter och Interpols databaser.

b) En säker kommunikationskanal mellan ESP, medlemsstaterna och de unionsbyråer som har rätt att använda sökportalen.

c) En säker kommunikationsinfrastruktur mellan ESP och in- och utresesystemet, VIS, Etias, Eurodac, centrala SIS, Ecris-TCN, Europoluppgifter och Interpols databaser samt mellan ESP och de centrala infrastrukturerna för CIR och MID.

3. EU-LISA ska utveckla ESP och säkerställa dess tekniska förvaltning.

Artikel 7

Användning av den europeiska sökportalen

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

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

2. De myndigheter i medlemsstaterna och de unionsbyråer som avses i punkt 1 ska använda ESP för att söka uppgifter om personer eller deras resehandlingar i in- och utresesystemets, VIS och Etias centrala system i enlighet med sina åtkomsträttigheter enligt de rättsliga instrument som reglerar dessa EU-informationssystem och nationell rätt. De ska också använda ESP för att söka i CIR i enlighet med sina åtkomsträttigheter enligt denna förordning för de syften som avses i artiklarna 20, 21 och 22.

3. De myndigheter i medlemsstaterna som avses i punkt 1 får använda ESP för att söka på uppgifter om personer eller deras resehandlingar i det centrala SIS som avses i förordningarna (EU) 2018/1860 och (EU) 2018/1861.

4. När så föreskrivs enligt unionsrätten ska de unionsbyråer som avses i punkt 1 använda ESP för att söka på uppgifter om personer eller deras resehandlingar i centrala SIS.

5. De myndigheter i medlemsstaterna och de unionsbyråer som avses i punkt 1 får använda ESP för att söka på uppgifter om resehandlingar i Interpols databaser när så föreskrivs och i enlighet med sina åtkomsträttigheter enligt unionsrätten och nationell rätt.

Artikel 8

Profiler för användarna av ESP

1. För att det ska vara möjligt att använda ESP ska EU-LISA i samarbete med medlemsstaterna skapa en profil för varje kategori av ESP-användare och på det syfte som de har med sökningarna, i enlighet med de tekniska detaljer och åtkomsträttigheter som avses i punkt 2. Varje profil ska, i enlighet med unionsrätten och nationell rätt, inbegripa följande information:

a) De uppgiftsfält som ska användas vid sökningar.

b) De EU-informationssystem, Europoluppgifter och Interpols databaser som ska vara föremål för sökningar, de som kan vara föremål för sökningar och de som ska tillhandahålla användaren ett svar.

c) De specifika uppgifter i EU-informationssystemen, Europoluppgifterna och Interpols databaser som får vara föremål för sökningar.

d) De kategorier av uppgifter som får tillhandahållas i varje svar.

2. Kommissionen ska anta genomförandeakter för att närmare ange de tekniska detaljerna för de profiler som avses i punkt 1 i enlighet med ESP-användarnas åtkomsträttigheter enligt de rättsliga instrument som reglerar EU-informationssystemen och nationell rätt. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

3. De profiler som avses i punkt 1 ska regelbundet ses över av EU-LISA i samarbete med medlemsstaterna, minst en gång om året, och vid behov uppdateras.

Artikel 9

Sökningar

1. Användarna av ESP ska inleda en sökning genom att mata in alfanumeriska eller biometriska uppgifter i ESP. När en sökning har inletts ska ESP samtidigt söka i in- och utresesystemet, Etias, VIS, SIS, Eurodac, Ecris-TCN och CIR samt i Europoluppgifter och Interpols databaser med de uppgifter som användaren matat in och i enlighet med användarprofilen.

2. De kategorier av uppgifter som används för att inleda en sökning via ESP ska motsvara de kategorier av uppgifter i fråga om personer eller resehandlingar som kan användas för att söka i de olika EU-informationssystemen, Europoluppgifter och Interpols databaser i enlighet med de rättsliga instrument som reglerar dem.

3. EU-LISA ska i samarbete med medlemsstaterna ta fram ett dokument för gränssnittskontroll för ESP på grundval av det UMF som avses i artikel 38.

4. När en sökning inleds av en ESP-användare ska in- och utresesystemet, Etias, VIS, SIS, Eurodac, Ecris-TCN, CIR och MID samt Europoluppgifter och Interpols databaser som svar på sökningen tillhandahålla de uppgifter som de innehåller.

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

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

5. Alla sökningar i Interpols databaser genom ESP ska göras på ett sådant sätt att ingen information röjs för ägaren av Interpolregistreringen.

6. ESP ska så snart som uppgifter finns tillgängliga tillhandahålla användaren svar från något av EU-informationssystemen, Europoluppgifterna eller Interpols databaser. Dessa svar får endast innehålla de uppgifter som användaren har åtkomst till enligt unionsrätten och nationell rätt.

7. Kommissionen ska anta en genomförandeakt för att specificera det tekniska förfarandet för ESP:s sökningar i EU-informationssystemen, Europoluppgifterna och Interpols databaser och formatet för ESP:s svar. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 10

Registerföring av loggar

1. Utan att det påverkar tillämpningen av artikel 46 i förordning (EU) 2017/2226, artikel 34 i förordning (EG) nr 767/2008, artikel 69 i förordning (EU) 2018/1240 och artiklarna 12 och 18 i förordning (EU) 2018/1861, ska EU-LISA föra logg över all uppgiftsbehandling i ESP. Dessa loggar ska omfatta följande:

a) Den medlemsstat eller unionsbyrå som inlett sökningen och den ESP-profil som används.

b) Datum och tidpunkt för sökningen.

c) De EU-informationssystem och de av Interpols databaser som varit föremål för sökning.

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

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

Artikel 11

Reservförfaranden om det är tekniskt omöjligt att använda den europeiska sökportalen

1. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera av de EU-informationssystem eller i CIR, på grund av ett fel i ESP, ska ESP-användare automatiskt underrättas av EU-LISA.

2. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera EU-informationssystem eller i CIR, på grund av ett fel i en medlemsstats nationella infrastruktur, ska den medlemsstaten automatiskt underrätta EU-LISA och kommissionen.

3. I de fall som avses i punkterna 1 och 2 i denna artikel och till dess att det tekniska felet har åtgärdats ska den skyldighet som avses i artikel 7.2 och 7.4 inte tillämpas och medlemsstaterna ska ha åtkomst till EU-informationssystemen eller till CIR direkt när så krävs enligt unionsrätten eller nationell rätt.

4. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera EU-informationssystem eller i CIR, på grund av ett fel i en unionsbyrås infrastruktur, ska den byrån automatiskt underrätta EU-LISA och kommissionen.

KAPITEL III

En gemensam biometrisk matchningstjänst

Artikel 12

En gemensam biometrisk matchningstjänst

1. Det ska inrättas en gemensam biometrisk matchningstjänst för lagring av biometriska mallar som erhållits från de biometriska uppgifter som avses i artikel 13, vilka är lagrade i CIR och SIS, och för möjliggörande av sökningar med biometriska uppgifter i flera EU-informationssystem för att stödja CIR och MID och målen för in- och utresesystemet, VIS, Eurodac, SIS och Ecris-TCN.

2. Den gemensamma biometriska matchningstjänsten ska bestå av följande:

a) En central infrastruktur som ska ersätta de centrala systemen för in- och utresesystemet, VIS, SIS, Eurodac respektive Ecris-TCN i den mån den ska lagra biometriska mallar och möjliggöra sökning med biometriska uppgifter.

b) En säker kommunikationsinfrastruktur mellan den gemensamma biometriska matchningstjänsten, centrala SIS och CIR.

3. EU-LISA ska utveckla den gemensamma biometriska matchningstjänsten och säkerställa den tekniska förvaltningen.

Artikel 13

Lagring av biometriska mallar i den gemensamma biometriska matchningstjänsten

1. Den gemensamma biometriska matchningstjänsten ska lagra de biometriska mallar som den ska få från följande biometriska uppgifter:

a) De uppgifter som avses i artiklarna 16.1 d, 17.1 b och c och 18.2 a, b och c i förordning (EU) 2017/2226.

b) De uppgifter som avses i artikel 9.6 i förordning (EG) nr 767/2008.

c) De uppgifter som avses i artikel 20.2 w och x i förordning (EU) 2018/1861, med undantag för uppgifter om handavtryck.

d) De uppgifter som avses i artikel 4.3 u och v i förordning (EU) 2018/1860, med undantag för uppgifter om handavtryck.

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

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

3. Biometriska mallar ska registreras i den gemensamma biometriska matchningstjänsten endast efter en automatisk kvalitetskontroll av de biometriska uppgifter som läggs in i ett av EU-informationssystemen, vilken utförs av den gemensamma biometriska matchningstjänsten för att säkerställa att en minimistandard för uppgifternas kvalitet uppfylls.

4. Lagringen av de uppgifter som avses i punkt 1 ska uppfylla de kvalitetsstandarder som avses i artikel 37.2.

5. Kommissionen ska genom en genomförandeakt fastställa prestandakrav och praktiska arrangemang för att övervaka den gemensamma biometriska matchningstjänstens prestanda, i syfte att säkerställa att effektiviteten i de biometriska sökningarna är förenlig med tidskritiska förfaranden, såsom in- och utresekontroller och identifieringar. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 14

Sökning på biometriska uppgifter med den gemensamma biometriska matchningstjänsten

För att söka på de biometriska uppgifter som lagrats i CIR och SIS ska CIR och SIS använda de biometriska mallar som lagrats i den gemensamma biometriska matchningstjänsten. Sökningar med biometriska uppgifter ska äga rum i enlighet med de syften som anges i denna förordning och i förordningarna (EG) nr 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 och (EU) 2019/816.

Artikel 15

Lagring av uppgifter i den gemensamma biometriska matchningstjänsten

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

Artikel 16

Registerföring av loggar

1. Utan att det påverkar tillämpningen av artikel 46 i förordning (EU) 2017/2226, artikel 34 i förordning (EG) nr 767/2008 och artiklarna 12 och 18 i förordning (EU) 2018/1861, ska EU-LISA föra logg över all uppgiftsbehandling i den gemensamma biometriska matchningstjänsten. Dessa loggar ska omfatta följande:

a) Den medlemsstat eller unionsbyrå som inlett sökningen.

b) Historiken för skapandet och lagringen av biometriska mallar.

c) De EU-informationssystem som varit föremål för sökning med de biometriska mallar som lagrats i den gemensamma biometriska matchningstjänsten.

d) Datum och tidpunkt för sökningen.

e) Den typ av biometriska uppgifter som används för att inleda sökningen.

f) Resultaten av sökningen och datum och tidpunkt för resultatet.

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

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

KAPITEL IV

En gemensam databas för identitetsuppgifter

Artikel 17

En gemensam databas för identitetsuppgifter

1. Det ska inrättas en gemensam databas för identitetsuppgifter (CIR), varigenom det skapas en personakt för varje person som är registrerad i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN och som innehåller de uppgifter som avses i artikel 18, för att underlätta och bistå vid en korrekt identifiering av personer som är registrerade i in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN i enlighet med artikel 20, stödja funktionen av MID i enlighet med artikel 21 och underlätta och rationalisera de utsedda myndigheternas och Europols åtkomst till in- och utresesystemet, VIS, Etias och Eurodac, om det är nödvändigt för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i enlighet med artikel 22.

2. CIR ska bestå av följande:

a) En central infrastruktur som ska ersätta de centrala systemen för in- och utresesystemet, VIS, Etias, Eurodac respektive Ecris-TCN i den mån den ska lagra de uppgifter som avses i artikel 18.

b) En säker kommunikationskanal mellan CIR, medlemsstaterna och de unionsbyråer som har rätt att använda CIR i enlighet med unionsrätten och nationell rätt.

c) En säker kommunikationsinfrastruktur mellan CIR och in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN samt de centrala infrastrukturerna för ESP, den gemensamma biometriska matchningstjänsten och MID.

3. EU-LISA ska utveckla CIR och säkerställa den tekniska förvaltningen.

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

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

Artikel 18

Uppgifter i den gemensamma databasen för identitetsuppgifter

1. CIR ska lagra följande uppgifter, logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör:

a) De uppgifter som avses i artiklarna 16.1 a–d, 17.1 a, b och c samt 18.1 och 18.2 i förordning (EU) 2017/2226.

b) De uppgifter som avses i artikel 9.4 a–c, 9.5 och 9.6 i förordning (EG) nr 767/2008.

c) De uppgifter som avses i artikel 17.2 a–e i förordning (EU) 2018/1240.

2. För varje uppsättning uppgifter som avses i punkt 1 ska CIR innehålla en hänvisning till de EU-informationssystem som uppgifterna tillhör.

3. De myndigheter som har åtkomst till CIR ska handla i enlighet med sina åtkomsträttigheter enligt de rättsliga instrument som reglerar EU-informationssystemen och enligt nationell rätt och i enlighet med sina åtkomsträttigheter enligt denna förordning för de syften som avses i artiklarna 20, 21 och 22.

4. För varje uppsättning uppgifter som avses i punkt 1 ska CIR innehålla en hänvisning till den konkreta post i EU-informationssystemen som uppgifterna tillhör.

5. Lagringen av de uppgifter som avses i punkt 1 ska uppfylla de kvalitetsstandarder som avses i artikel 37.2.

Artikel 19

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

1. Om uppgifter läggs till, ändras eller raderas i in- och utresesystemet, VIS och Etias ska de uppgifter som avses i artikel 18 och som lagras i personakten i CIR automatiskt läggas till, ändras eller raderas.

2. Om en vit eller en röd länk skapas i MID i enlighet med artikel 32 eller 33 mellan uppgifter i två eller flera av EU-informationssystemen som utgör CIR, ska CIR i stället för att skapa en ny personakt lägga till de nya uppgifterna i den personakt som innehåller de länkade uppgifterna.

Artikel 20

Åtkomst till den gemensamma databasen för identitetsuppgifter i identifieringssyfte

1. Sökningar i CIR får utföras av en polismyndighet i enlighet med punkterna 2 och 5 endast under följande omständigheter:

a) Om en polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet.

b) Om det föreligger tvivel om de identitetsuppgifter som lämnats av en person.

c) Om det föreligger tvivel om äktheten i den resehandling eller en annan trovärdig handling som lämnats av en person.

d) Om det föreligger tvivel om identiteten på innehavaren av en resehandling eller en annan trovärdig handling.

e) Om en person inte kan eller vägrar att samarbeta.

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

2. Om någon av de omständigheter som förtecknas i punkt 1 uppstår och en polismyndighet har bemyndigats genom de nationella lagstiftningsåtgärder som avses i punkt 5, får myndigheten, endast i syfte att identifiera en person, söka i CIR med den personens biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro.

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

Om personens biometriska uppgifter inte kan användas eller om sökningen med dessa uppgifter misslyckas, ska sökningen utföras med vederbörandes identitetsuppgifter i kombination med resehandlingsuppgifter eller med de identitetsuppgifter som tillhandahållits av personen.

4. Om en polismyndighet har bemyndigats genom de nationella lagstiftningsåtgärder som avses i punkt 6, får den, i händelse av en naturkatastrof, en olycka eller ett terrordåd och endast i syfte att identifiera okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor, söka i CIR med dessa personers biometriska uppgifter.

5. Medlemsstater som vill utnyttja den möjlighet som anges i punkt 2 ska anta nationella lagstiftningsåtgärder. När medlemsstaterna gör detta ska de ta hänsyn till att ingen diskriminering av tredjelandsmedborgare får förekomma. I sådana lagstiftningsåtgärder ska de exakta syftena med identifieringen anges inom ramen för de mål som avses i artikel 2.1 b och c. De behöriga polismyndigheterna ska utses, och förfaranden, villkor och kriterier för sådana kontroller ska fastställas i dessa lagstiftningsåtgärder.

6. Medlemsstater som vill utnyttja den möjlighet som anges i punkt 4 ska anta nationella lagstiftningsåtgärder som fastställer förfarandena, villkoren och kriterierna.

Artikel 21

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

1. Om en sökning i CIR resulterar i en gul länk i enlighet med artikel 28.4, ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter i enlighet med artikel 29 enbart i verifieringssyfte ha åtkomst till de uppgifter som avses i artikel 18.1 och 18.2, som lagrats i CIR och som är kopplade genom en gul länk.

2. Om en sökning i CIR ger upphov till en röd länk i enlighet med artikel 32, ska de myndigheter som avses i artikel 26.2 enbart i syfte att bekämpa identitetsbedrägerier ha åtkomst till de uppgifter som avses i artikel 18.1 och 18.2, som lagrats i CIR och som är kopplade genom en röd länk.

Artikel 22

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

1. Om det i ett specifikt fall finns rimliga skäl att anta att en sökning i EU-informationssystem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, särskilt om det finns misstankar om att en person som misstänks för, har begått eller utsatts för ett terroristbrott eller ett annat grovt brott är en person vars uppgifter lagras i in- och utresesystemet, VIS eller Etias, får de utsedda myndigheterna och Europol söka i CIR för att få information om huruvida det finns uppgifter om en viss person i in- och utresesystemet, VIS eller Etias.

2. Om ett svar på en sökning i CIR visar att det finns uppgifter om den personen i in- och utresesystemet, VIS eller Etias ska CIR tillhandahålla de utsedda myndigheterna och Europol ett svar i form av en hänvisning som avses i artikel 18.2 som anger vilka av dessa EU-informationssystem som innehåller motsvarande uppgifter. CIR ska svara på ett sådant sätt att uppgifternas säkerhet inte äventyras.

Det svar som anger att uppgifter om personen i fråga förekommer i något av de EU-informationssystem som avses i punkt 1 får användas endast i syfte att lämna in en begäran om full åtkomst som omfattas av de villkor och förfaranden som fastställs i respektive rättsliga instrument där sådan åtkomst regleras.

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

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

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

Artikel 23

Lagring av uppgifter i den gemensamma databasen för identitetsuppgifter

1. De uppgifter som avses i artikel 18.1, 18.2 och 18.4 ska automatiskt raderas från CIR i enlighet med bestämmelserna om lagring av uppgifter i förordningarna (EU) 2017/2226, (EG) nr 767/2008 respektive (EU) 2018/1240.

2. Personakten ska lagras i CIR endast så länge de motsvarande uppgifterna lagras i minst ett av de EU-informationssystem vars uppgifter finns i CIR. Skapandet av en länk ska inte påverka lagringsperioden för varje post av de länkade uppgifterna.

Artikel 24

Registerföring av loggar

1. Utan att det påverkar tillämpningen av artikel 46 i förordning (EU) 2017/2226, artikel 34 i förordning (EG) nr 767/2008 och artikel 69 i förordning (EU) 2018/1240, ska EU-LISA föra logg över all uppgiftsbehandling i CIR i enlighet med punkterna 2, 3 och 4 i den här artikeln.

2. EU-LISA ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 20 i CIR. Dessa loggar ska omfatta följande:

a) Den medlemsstat eller den unionsbyrå som inlett sökningen.

b) Syftet med användarens åtkomst för att söka via CIR.

c) Datum och tidpunkt för sökningen.

d) Den typ av uppgifter som används för att inleda sökningen.

e) Sökningens resultat.

3. EU-LISA ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 21 i CIR. Dessa loggar ska omfatta följande:

a) Den medlemsstat eller den unionsbyrå som inlett sökningen.

b) Syftet med användarens åtkomst för att söka via CIR.

c) Datum och tidpunkt för sökningen.

d) I fall där en länk skapas, de uppgifter som används för att inleda sökningen och sökningens resultat med angivelse av det EU-informationssystem som uppgifterna erhållits från.

4. EU-LISA ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 22 i CIR. Dessa loggar ska omfatta följande:

a) Datum och tidpunkt för sökningen.

b) De uppgifter som används för att inleda sökningen.

c) Sökningens resultat.

d) Den medlemsstat eller den unionsbyrå som söker i CIR.

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

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

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

a) Referensnummer för den nationella akten.

b) Syftet med åtkomsten.

c) I enlighet med nationella regler, den unika användaridentitet som anger vilken tjänsteman som utförde sökningen och vilken tjänsteman som beordrade sökningen.

6. I enlighet med förordning (EU) 2016/794 ska Europol för all åtkomst till CIR i enlighet med artikel 22 i den här förordningen föra logg över den unika användaridentitet som anger vilken tjänsteman som utförde sökningen och vilken tjänsteman som beordrade sökningen.

7. De loggar som avses i punkterna 2–6 får endast användas för övervakning av dataskyddet, inbegripet för kontroll av om en sökning är tillåten och om uppgifter har behandlats på ett lagligt sätt samt för att säkerställa datasäkerhet och dataintegritet. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats. För det fall de behövs för övervakningsförfaranden som redan har inletts, ska de emellertid raderas så snart loggarna i fråga inte längre behövs för övervakningsförfarandena.

8. EU-LISA ska lagra loggarna över historiken avseende uppgifterna i personakter. EU-LISA ska automatiskt radera sådana loggar så snart uppgifterna har raderats.

KAPITEL V

Detektorn för multipla identiteter

Artikel 25

Detektorn för multipla identiteter

1. Det ska inrättas en detektor för multipla identiteter (MID) som skapar och lagrar akter med identitetsbekräftelse som avses i artikel 34, som innehåller länkar mellan uppgifter i de EU-informationssystem som ingår i CIR och SIS och som gör det möjligt att spåra multipla identiteter, med det dubbla syftet att underlätta identitetskontroller och bekämpa identitetsbedrägerier, för att stödja CIR:s funktion och målen för in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

2. MID ska bestå av följande:

a) En central infrastruktur som lagrar länkar och hänvisningar till EU-informationssystem.

b) En säker kommunikationsinfrastruktur som kopplar MID till SIS och ESP:s och CIR:s centrala infrastrukturer.

3. EU-LISA ska utveckla MID och säkerställa den tekniska förvaltningen.

Artikel 26

Åtkomst till MID

1. För den manuella verifiering av olika identiteter som avses i artikel 29 ska åtkomst till de uppgifter som avses i artikel 34 och som är lagrade i MID beviljas

a) de behöriga myndigheter som utsetts i enlighet med artikel 9.2 i förordning (EU) 2017/2226 när de skapar eller uppdaterar en personakt i in- och utresesystemet i enlighet med artikel 14 i den förordningen,

b) de viseringsmyndigheter som avses i artikel 6.1 i förordning (EG) nr 767/2008 när de skapar eller uppdaterar en ansökningsakt i VIS i enlighet med den förordningen,

c) Etias centralenhet och Etias nationella enheter när de utför den behandling som avses i artiklarna 22 och 26 i förordning (EU) 2018/1240,

d) Sirenekontoret i den medlemsstat som skapar eller uppdaterar en registrering i SIS i enlighet med förordningarna (EU) 2018/1860 och (EU) 2018/1861,

2. De myndigheter i medlemsstaterna och de unionsbyråer som har åtkomst till minst ett av de EU-informationssystem som ingår i CIR eller till SIS ska ha åtkomst till de uppgifter som avses i artikel 34 a och b vad gäller samtliga röda länkar som avses i artikel 32.

3. Myndigheterna i medlemsstaterna och unionsbyråerna ska ha åtkomst till de vita länkar som avses i artikel 33 om de har åtkomst till de två EU-informationssystem som innehåller uppgifter mellan vilka den vita länken skapats.

4. Myndigheterna i medlemsstaterna och unionsbyråerna ska ha åtkomst till de gröna länkar som avses i artikel 31 om de har åtkomst till de två EU-informationssystem som innehåller uppgifter mellan vilka den gröna länken skapats och en sökning i dessa informationssystem gett en träff med de två uppsättningarna länkade uppgifter.

Artikel 27

Spårning av multipla identiteter

1. Spårning av multipla identiteter ska i följande fall inledas i CIR och i SIS:

a) En personakt skapas eller uppdateras i in- och utresesystemet i enlighet med artikel 14 i förordning (EU) 2017/2226.

b) En ansökningsakt skapas eller uppdateras i VIS i enlighet med förordning (EG) nr 767/2008.

c) En ansökningsakt skapas eller uppdateras i Etias i enlighet med artikel 19 i förordning (EU) 2018/1240.

d) En registrering om en person skapas eller uppdateras i SIS i enlighet med artikel 3 i förordning (EU) 2018/1860 och kapitel V i förordning (EU) 2018/1861.

2. Om de uppgifter i ett EU-informationssystem som avses i punkt 1 innehåller biometriska uppgifter ska CIR och centrala SIS använda den gemensamma biometriska matchningstjänsten för att utföra en spårning av multipla identiteter. Den gemensamma biometriska matchningstjänsten ska jämföra de biometriska mallar som erhållits från nya biometriska uppgifter med de biometriska mallar som redan finns i den gemensamma biometriska matchningstjänsten i syfte att verifiera huruvida uppgifter som tillhör samma person redan finns lagrade i CIR eller i centrala SIS.

3. Utöver det förfarande som avses i punkt 2 ska CIR och centrala SIS använda ESP för att söka i uppgifter som lagrats i centrala SIS respektive CIR med hjälp av följande uppgifter:

a) Efternamn (familjenamn), förnamn, födelsedatum, medborgarskap och kön enligt artiklarna 16.1 a, 17.1 och 18.1 i förordning (EU) 2017/2226.

b) Efternamn (familjenamn), förnamn, födelsedatum, kön, födelseort, födelseland och medborgarskap enligt artikel 9.4 a och aa i förordning (EG) nr 767/2008.

c) Efternamn (familjenamn), förnamn, efternamn som ogift, alias, födelsedatum, födelseort, kön och nuvarande medborgarskap enligt artikel 17.2 i förordning (EU) 2018/1240.

d) Efternamn, förnamn, namn vid födelsen och tidigare använda namn och alias, födelseort, födelsedatum, kön och samtliga medborgarskap enligt artikel 20.2 i förordning (EU) 2018/1861.

e) Efternamn, förnamn, namn vid födelsen och tidigare använda namn och alias, födelseort, födelsedatum, kön och samtliga medborgarskap enligt artikel 4 i förordning (EU) 2018/1860.

4. Utöver det förfarande som avses i punkterna 2 och 3 ska CIR och centrala SIS använda ESP för att söka i uppgifter som lagrats i centrala SIS respektive CIR med hjälp av resehandlingsuppgifter.

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

Artikel 28

Resultat av en spårning av multipla identiteter

1. Om de sökningar som avses i artikel 27.2, 27.3 och 27.4 inte ger någon träff ska de förfaranden som avses i artikel 27.1 fortsätta i enlighet med rättsliga instrument genom vilka de regleras.

2. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 ger en eller flera träffar ska CIR och, i förekommande fall, SIS skapa en länk mellan de uppgifter som används för att inleda sökningen och de uppgifter som gett upphov till träffen.

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

3. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är desamma eller liknande, ska en vit länk skapas i enlighet med artikel 33.

4. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 ger en eller flera träffar och identitetsuppgifterna i de länkade akterna inte kan anses vara liknande, ska en gul länk skapas i enlighet med artikel 30 och det förfarande som avses i artikel 29 ska tillämpas.

5. Kommissionen ska anta delegerade akter i enlighet med artikel 73 för att fastställa förfarandena för att avgöra ärenden där identitetsuppgifter kan anses vara desamma eller liknande.

6. Länkarna ska lagras i den akt med identitetsbekräftelse som avses i artikel 34.

7. Kommissionen ska, i samarbete med EU-LISA, fastställa de tekniska reglerna för att skapa länkar mellan uppgifter från olika EU-informationssystem genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 29

Manuell verifiering av olika identiteter och ansvariga myndigheter

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

a) Den behöriga myndighet som utsetts i enlighet med artikel 9.2 i förordning (EU) 2017/2226 för träffar som uppstår när de skapar eller uppdaterar en personakt i in- och utresesystemet i enlighet med den förordningen.

b) De viseringsmyndigheter som avses i artikel 6.1 i förordning (EG) nr 767/2008 för träffar som uppstår när de skapar eller uppdaterar en ansökningsakt i VIS i enlighet med den förordningen.

c) Etias centralenhet och Etias nationella enheter för träffar som uppstår när de skapar eller uppdaterar en ansökningsakt i enlighet med förordning (EU) 2018/1240.

d) Sirenekontoret i medlemsstaten för träffar som uppstår när en registrering i SIS skapas eller uppdateras i enlighet med förordning (EU) 2018/1860 och förordning (EU) 2018/1861.

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

2. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter i akten med identitetsbekräftelse ska vara Sirenekontoret i den medlemsstat som skapade registreringen om det skapas en länk till uppgifterna i en registrering om

a) personer som är efterlysta för att gripas och överlämnas eller för att utlämnas enligt artikel 26 i förordning (EU) 2018/1862,

b) försvunna eller sårbara personer enligt artikel 32 i förordning (EU) 2018/1862,

c) personer som söks för att delta i ett rättsligt förfarande enligt artikel 34 i förordning (EU) 2018/1862,

d) personer för diskreta kontroller, undersökningskontroller eller särskilda kontroller enligt artikel 36 i förordning (EU) 2018/1862.

3. Utan att det påverkar tillämpningen av punkt 4 i denna artikel ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter ha åtkomst till de länkade uppgifterna i den relevanta akten med identitetsbekräftelse och till de identitetsuppgifter som är länkade i CIR och, i förekommande fall, i SIS. Den ska bedöma de olika identiteterna utan dröjsmål. När den bedömningen slutförts ska den uppdatera länken i enlighet med artiklarna 31, 32 och 33 samt utan dröjsmål lägga till den i akten med identitetsbekräftelse.

4. Om den myndighet som ansvarar för manuell verifiering av olika identiteter i akten med identitetsbekräftelse är den behöriga myndighet som utsetts i enlighet med artikel 9.2 i förordning (EU) 2017/2226 och som skapar eller uppdaterar en personakt i in- och utresesystemet i enlighet med artikel 14 i den förordningen och en gul länk skapas, ska den myndigheten utföra ytterligare verifiering. Den myndigheten ska endast för detta syfte ha åtkomst till de relaterade uppgifter som finns i den relevanta akten med identitetsbekräftelse. Den ska bedöma de olika identiteterna, uppdatera länken i enlighet med artiklarna 31, 32 och 33 i den här förordningen och lägga till den i akten med identitetsbekräftelse.

Sådan manuell verifiering av olika identiteter ska inledas i närvaro av den berörda personen, som ska ges möjlighet att förklara omständigheterna för den ansvariga myndigheten, som ska beakta dessa förklaringar.

I fall där den manuella verifieringen av olika identiteter äger rum vid gränsen, ska den om möjligt äga rum inom 12 timmar från det att en gul länk skapas i enlighet med artikel 28.4.

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

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

Artikel 30

Gul länk

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

a) De länkade uppgifterna innehåller samma biometriska uppgifter men har liknande eller olika identitetsuppgifter.

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

c) De länkade uppgifterna innehåller samma identitetsuppgifter men har olika biometriska uppgifter.

d) De länkade uppgifterna har liknande eller olika identitetsuppgifter, och innehåller samma resehandlingsuppgifter men har olika biometriska uppgifter.

2. Om en länk klassificeras som gul i enlighet med punkt 1 ska förfarandet i artikel 29 tillämpas.

Artikel 31

Grön länk

1. En länk mellan uppgifter från två eller flera EU-informationssystem ska klassificeras som grön om

a) de länkade uppgifterna har olika biometriska uppgifter men innehåller samma identitetsuppgifter och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer,

b) de länkade uppgifterna har olika biometriska uppgifter, har liknande eller olika identitetsuppgifter, innehåller samma resehandlingsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer,

c) de länkade uppgifterna har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter, minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer.

2. Om en sökning görs i CIR eller SIS och om det finns en grön länk mellan två eller fler av EU-informationssystemen, ska MID ange att identitetsuppgifterna i de länkade uppgifterna inte gäller samma person.

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

Artikel 32

Röd länk

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

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

b) De länkade uppgifterna har samma, liknande eller olika identitetsuppgifter och har samma resehandlingsuppgifter men olika biometriska uppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer, av vilka åtminstone en person använder en och samma resehandling på ett oberättigat sätt.

c) De länkade uppgifterna innehåller samma identitetsuppgifter men har olika biometriska uppgifter och olika eller inga resehandlingsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer på ett oberättigat sätt.

d) De länkade uppgifterna har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter, minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till en och samma person på ett oberättigat sätt.

2. Om CIR eller SIS är föremål för sökning och om det finns en röd länk mellan uppgifter i två eller fler av EU-informationssystemen, ska MID ange de uppgifter som avses i artikel 34. En uppföljning av en röd länk ska ske i enlighet med unionsrätten och nationell rätt, och eventuella rättsliga följder för den berörda personen ska bygga uteslutande på de relevanta uppgifterna om personen i fråga. Inga rättsliga följder för den berörda personen ska uppstå enbart till följd av att det finns en röd länk.

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

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

5. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter ska skriftligen tillhandahålla den information som avses i punkt 4 i form av ett standardformulär. Kommissionen ska genom genomförandeakter fastställa innehållet i och utformningen av det formuläret. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

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

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

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

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

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

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

Artikel 33

Vit länk

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

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

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

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

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

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

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

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

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

6. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter ska skriftligen tillhandahålla den information som avses i punkt 4 i form av ett standardformulär. Kommissionen ska genom genomförandeakter fastställa innehållet i och utformningen av det formuläret. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 34

Akt med identitetsbekräftelse

Akten med identitetsbekräftelse ska innehålla följande uppgifter:

a) De länkar som avses i artiklarna 30–33.

b) En hänvisning till de EU-informationssystem i vilka de länkade uppgifterna finns.

c) Ett enda identifikationsnummer som gör det möjligt att hämta de länkade uppgifterna från de motsvarande EU-informationssystemen.

d) Den myndighet som ansvarar för den manuella verifieringen av olika identiteter.

e) Datum för skapande av länken eller uppdatering därav.

Artikel 35

Lagring av uppgifter i detektorn för multipla identiteter

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

Artikel 36

Registerföring av loggar

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

a) Den medlemsstat som inlett sökningen.

b) Syftet med användarens åtkomst.

c) Datum och tidpunkt för sökningen.

d) Den typ av uppgifter som används för att inleda sökningen.

e) Hänvisning till de länkade uppgifterna.

f) Historik tillhörande akten med identitetsbekräftelse.

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

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

KAPITEL VI

Åtgärder till stöd för interoperabilitet

Artikel 37

Uppgifternas kvalitet

1. Utan att det påverkar medlemsstaternas ansvar för kvaliteten på de uppgifter som förs in i systemen ska EU-LISA inrätta automatiska mekanismer och förfaranden för kontroll av uppgifternas kvalitet avseende de uppgifter som lagras i in- och utresesystemet, VIS, Etias, SIS, den gemensamma biometriska matchningstjänsten och CIR.

2. EU-LISA ska införa mekanismer för utvärdering av den gemensamma biometriska matchningstjänstens exakthet, gemensamma indikatorer för uppgifternas kvalitet och minimikvalitetsstandarder för lagring av uppgifter i in- och utresesystemet, VIS, Etias, SIS, den gemensamma biometriska matchningstjänsten och CIR.

Endast uppgifter som uppfyller minimikvalitetsstandarderna får föras in i in- och utresesystemet, VIS, Etias, SIS, den gemensamma biometriska matchningstjänsten, CIR och MID.

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

4. Detaljerna om de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma indikatorerna för uppgifternas kvalitet samt minimikvalitetsstandarderna för lagring av uppgifter i in- och utresesystemet, VIS, Etias, SIS, den gemensamma biometriska matchningstjänsten och CIR, särskilt vad gäller biometriska uppgifter, ska fastställas i genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

5. Ett år efter inrättandet av de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma indikatorerna för uppgifternas kvalitet samt minimikvalitetsstandarderna för uppgifter, och varje år därefter, ska kommissionen utvärdera medlemsstaternas genomförande av uppgifters kvalitet och lämna nödvändiga rekommendationer. Medlemsstaterna ska förse kommissionen med en handlingsplan för att avhjälpa de brister som konstaterats i utvärderingsrapporten och, i synnerhet, problem med uppgiftskvalitet vilka härrör från felaktiga uppgifter i EU-informationssystem. Medlemsstaterna ska regelbundet rapportera till kommissionen om vilka framsteg som har gjorts med denna handlingsplan till dess att den genomförts fullt ut.

Kommissionen ska överlämna utvärderingsrapporten till Europaparlamentet, rådet, Europeiska datatillsynsmannen, Europeiska dataskyddsstyrelsen och Europeiska unionens byrå för grundläggande rättigheter, som inrättades genom rådets förordning (EG) nr 168/2007 ([39]).

Artikel 38

Universellt meddelandeformat

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

2. UMF-standarden ska användas vid utvecklingen av in- och utresesystemet, Etias, ESP, CIR, MID och, när så är lämpligt, EU-LISA:s eller andra unionsbyråers utveckling av nya modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor.

3. Kommissionen ska anta en genomförandeakt för att fastställa och utveckla den UMF-standard som avses i punkt 1 i denna artikel. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 39

Den centrala databasen för rapporter och statistik

1. Det ska inrättas en central databas för rapporter och statistik (CRRS) för att stödja målen för in- och utresesystemet, VIS, Etias och SIS, i enlighet med de respektive rättsliga instrument som reglerar de systemen, och för att tillhandahålla systemöverskridande statistiska uppgifter och analysrapporter för politiska och operativa syften samt för uppgiftskvaliteten.

2. EU-LISA ska inrätta, implementera och hysa i sina tekniska anläggningar CRRS som innehåller de uppgifter och den statistik som avses i artikel 63 i förordning (EU) 2017/2226, artikel 17 i förordning (EG) nr 767/2008, artikel 84 i förordning (EU) 2018/1240, artikel 60 i förordning (EU) 2018/1861 och artikel 16 i förordning (EU) 2018/1860, logiskt åtskilda per EU-informationssystem. Åtkomst till CRRS ska beviljas via kontrollerad, säkrad åtkomst och specifika användarprofiler, enbart för rapportering och statistik, till de myndigheter som avses i artikel 63 i förordning (EU) 2017/2226, artikel 17 i förordning (EG) nr 767/2008, artikel 84 i förordning (EU) 2018/1240 och artikel 60 i förordning (EU) 2018/1861.

3. EU-LISA ska anonymisera uppgifterna och registrera de anonymiserade uppgifterna i CRRS. Förfarandet för att anonymisera uppgifterna ska vara automatiskt.

Uppgifterna i CRRS ska inte möjliggöra identifiering av enskilda personer.

4. CRRS ska bestå av följande:

a) De verktyg som är nödvändiga för anonymisering av uppgifter.

b) En central infrastruktur som består av en databas med anonymiserade uppgifter.

c) En säker kommunikationsinfrastruktur för att ansluta CRRS till in- och utresesystemet, VIS, Etias och SIS samt de centrala infrastrukturerna för den gemensamma biometriska matchningstjänsten, CIR och MID.

5. Kommissionen ska anta en delegerad akt i enlighet med artikel 73 för att fastställa detaljerade bestämmelser om driften av CRRS, inbegripet särskilda skyddsåtgärder för behandlingen av personuppgifter enligt punkterna 2 och 3 i den här artikeln och de säkerhetsregler som är tillämpliga på databasen.

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

KAPITEL VII

Dataskydd

Artikel 40

Personuppgiftsansvarig

1. När det gäller behandling av uppgifter i den gemensamma biometriska matchningstjänsten ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för in- och utresesystemet, VIS respektive SIS vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 avseende de biometriska mallar som erhållits från de uppgifter som avses i artikel 13 i den här förordningen och som de för in i de underliggande systemen och ska ansvara för behandlingen av de biometriska mallarna i den gemensamma biometriska matchningstjänsten.

2. När det gäller behandling av uppgifter i CIR ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för in- och utresesystemet, VIS respektive Etias vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 avseende de uppgifter som avses i artikel 18 i den här förordningen och som de för in i de underliggande systemen och ska ansvara för behandlingen av de personuppgifterna i CIR.

3. När det gäller behandling av uppgifter i MID gäller följande:

a) Europeiska gräns- och kustbevakningsbyrån ska vara personuppgiftsansvarig i den mening som avses i artikel 3.8 i förordning (EU) 2018/1725 när det gäller den behandling av personuppgifter som utförs av Etias centralenhet.

b) De av medlemsstaternas myndigheter som lägger till eller ändrar uppgifter i akten med identitetsbekräftelse ska vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 och ska ansvara för behandlingen av personuppgifter i MID.

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

Artikel 41

Personuppgiftsbiträde

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

Artikel 42

Säkerhet vid behandling

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

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

3. EU-LISA ska i synnerhet vidta nödvändiga åtgärder, inbegripet en säkerhetsplan, en kontinuitetsplan och en katastrofplan, i syfte att

a) fysiskt skydda uppgifter, bland annat genom att utarbeta beredskapsplaner för skydd av kritisk infrastruktur,

b) hindra obehöriga från åtkomst till utrustning eller anläggningar för uppgiftsbehandling,

c) förhindra obehörig läsning, kopiering, ändring eller obehörigt avlägsnande av datamedier,

d) hindra obehörig inmatning av uppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter,

e) förhindra obehörig behandling av uppgifter och obehörig kopiering, ändring eller radering av uppgifter,

f) hindra obehöriga från att med hjälp av datakommunikationsutrustning använda automatiserade system för uppgiftsbehandling,

g) säkerställa att personer som har åtkomstbehörighet till interoperabilitetskomponenterna har åtkomst endast till de uppgifter för vilka de är behöriga och endast genom individuella användaridentiteter och skyddade åtkomstmetoder,

h) säkerställa att det finns möjlighet att kontrollera och fastställa till vilka organ personuppgifter får överföras med hjälp av datakommunikationsutrustning,

i) säkerställa att det finns möjlighet att kontrollera och fastställa vilka uppgifter som har behandlats i interoperabilitetskomponenterna, när detta har gjorts, av vem och i vilket syfte,

j) hindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av personuppgifter till eller från interoperabilitetskomponenterna eller under transport av datamedier, särskilt med hjälp av lämplig krypteringsteknik,

k) säkerställa att installerade system i händelse av driftavbrott kan återställas till normal drift,

l) säkerställa driftsäkerhet genom att se till att eventuella driftfel hos interoperabilitetskomponenterna rapporteras på korrekt sätt,

m) övervaka att de säkerhetsåtgärder som avses i denna punkt är verksamma och vidta nödvändiga organisatoriska åtgärder i fråga om intern övervakning för att säkerställa att denna förordning efterlevs och för att bedöma dessa säkerhetsåtgärder mot bakgrund av utvecklingen av ny teknik.

4. Medlemsstaterna, Europol och Etias centralenhet ska vidta åtgärder som är likvärdiga med de som avses i punkt 3 vad gäller säkerheten vid behandling av personuppgifter som utförs av de myndigheter som har rätt till åtkomst till någon av interoperabilitetskomponenterna.

Artikel 43

Säkerhetstillbud

1. Alla händelser som har eller kan ha inverkan på interoperabilitetskomponenternas säkerhet och som kan orsaka skada på eller förlust av uppgifter lagrade i dem ska betraktas som säkerhetstillbud, särskilt om obehörig åtkomst till uppgifter kan ha inträffat eller om uppgifters tillgänglighet, integritet och konfidentialitet har äventyrats eller kan ha äventyrats.

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

3. Utan att det påverkar anmälan av och information om personuppgiftsincidenter i enlighet med artikel 33 i förordning (EU) 2016/679, artikel 30 i direktiv (EU) 2016/680, eller båda, ska medlemsstaterna utan dröjsmål underrätta kommissionen, EU-LISA, de behöriga tillsynsmyndigheterna och Europeiska datatillsynsmannen om alla säkerhetstillbud.

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

Om ett säkerhetstillbud inträffar avseende interoperabilitetskomponenternas centrala infrastruktur ska EU-LISA utan dröjsmål underrätta kommissionen och Europeiska datatillsynsmannen.

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

5. De berörda medlemsstaterna, Etias centralenhet, Europol och EU-LISA ska samarbeta om ett säkerhetstillbud inträffar. Kommissionen ska fastställa specifikationer för detta samarbete genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 44

Egenkontroll

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

De personuppgiftsansvariga som avses i artikel 40 ska vidta nödvändiga åtgärder för att övervaka att uppgiftsbehandlingen sker i enlighet med denna förordning, inklusive genom frekventa kontroller av de loggar som avses i artiklarna 10, 16, 24 och 36, och vid behov samarbeta med tillsynsmyndigheterna och med Europeiska datatillsynsmannen.

Artikel 45

Sanktioner

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

Artikel 46

Skadeståndsansvar

1. Utan att det påverkar rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet, eller dessas skadeståndsansvar i enlighet med förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725, ska följande gälla:

a) Varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en otillåten behandling av personuppgifter eller av någon annan åtgärd från en medlemsstats sida som är oförenlig med denna förordning ska ha rätt till ersättning från den berörda medlemsstaten.

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

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

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

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

Artikel 47

Rätt till information

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

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

3. De personer vars uppgifter registrerats i in- och utresesystemet, VIS eller Etias ska underrättas om behandlingen av personuppgifter vid tillämpningen av denna förordning i enlighet med punkt 1 i följande fall:

a) En personakt skapas eller uppdateras i in- och utresesystemet i enlighet med artikel 14 i förordning (EU) 2017/2226.

b) En ansökningsakt skapas eller uppdateras i VIS i enlighet med artikel 8 i förordning (EG) nr 767/2008.

c) En ansökningsakt skapas eller uppdateras i Etias i enlighet med artikel 19 i förordning (EU) 2018/1240.

Artikel 48

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

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

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

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

4. Om en begäran om rättelse eller radering av personuppgifter ställs till en medlemsstat där Etias centralenhet ansvarade för den manuella verifieringen av olika identiteter, ska den medlemsstat till vilken begäran ställdes kontakta Etias centralenhet inom sju dagar och begära att den avger ett yttrande. Etias centralenhet ska avge sitt yttrande utan otillbörligt dröjsmål, dock senast inom 30 dagar efter det att den kontaktades. Denna period får vid behov förlängas med ytterligare 15 dagar, med beaktande av hur komplicerade och hur många begärandena är. Den berörda personen ska informeras om det fortsatta förfarandet av den medlemsstat som kontaktade Etias centralenhet.

5. Om det efter en prövning visar sig att de uppgifter som lagrades i MID är oriktiga eller har registrerats på ett olagligt sätt, ska den medlemsstat som ansvarade för den manuella verifieringen av olika identiteter eller – om det inte fanns någon medlemsstat som ansvarade för den manuella verifieringen av olika identiteter eller om Etias centralenhet ansvarade för den manuella verifieringen av olika identiteter – den medlemsstat till vilken begäran har ställts utan otillbörligt dröjsmål rätta eller radera dessa uppgifter. Den berörda personen ska informeras skriftligen om att hans eller hennes uppgifter har rättats eller raderats.

6. Om uppgifter som lagras i MID ändras av en medlemsstat under lagringsperioden, ska den medlemsstaten utföra den behandling som avses i artikel 27 och, i förekommande fall, artikel 29 för att avgöra huruvida de ändrade uppgifterna ska länkas. Om behandlingen inte ger någon träff ska den medlemsstaten radera uppgifterna från akten med identitetsbekräftelse. Om den automatiska behandlingen ger en eller flera träffar ska den medlemsstaten skapa eller uppdatera den relevanta länken i enlighet med de relevanta bestämmelserna i denna förordning.

7. Om den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts inte instämmer i att uppgifter som lagras i MID är oriktiga eller har registrerats på ett olagligt sätt, ska den medlemsstaten utan dröjsmål anta ett administrativt beslut med en skriftlig förklaring till den berörda personen om varför den inte är beredd att rätta eller radera uppgifter som rör honom eller henne.

8. Det beslut som avses i punkt 7 ska även ge den berörda personen information om möjligheten att invända mot det beslut som fattats med avseende på begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter och, i tillämpliga fall, information om hur talan kan väckas vid eller klagomål inges till behöriga myndigheter eller domstolar samt möjligheterna till bistånd, även från tillsynsmyndigheterna.

9. En begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter ska innehålla den information som behövs för att den berörda personen ska kunna identifieras. Denna information ska användas uteslutande för att de rättigheter som avses i denna artikel ska kunna utövas och ska sedan omedelbart raderas.

10. Den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts ska spara skriftlig dokumentation av att en begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter har gjorts och hur den behandlats, och ska utan dröjsmål tillhandahålla tillsynsmyndigheterna denna dokumentation.

11. Denna artikel påverkar inte begränsningar och inskränkningar av de rättigheter som anges i denna artikel i enlighet med förordning (EU) 2016/679 och direktiv (EU) 2016/680.

Artikel 49

Webbportal

1. En webbportal inrättas för att underlätta utövandet av rätten till åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter.

2. Webbportalen ska innehålla information om de rättigheter och förfaranden som avses i artiklarna 47 och 48 och ett användargränssnitt som gör det möjligt för personer vars uppgifter behandlas i MID och som underrättats om förekomsten av en röd länk i enlighet med artikel 32.4 att få kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter.

3. För att få kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter bör den person vars uppgifter behandlas i MID uppge referensen för den myndighet som ansvarar för den manuella verifieringen av olika identiteter enligt vad som avses i artikel 34 d. Webbportalen ska använda denna referens för att hämta kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter. Webbportalen ska också inkludera en mall för ett e-postmeddelande för att underlätta kommunikationen mellan portalanvändaren och den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter. Detta e-postmeddelande ska innehålla ett fält för det enda identifikationsnummer som avses i artikel 34 c, så att den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter kan identifiera de berörda uppgifterna.

4. Medlemsstaterna ska ge EU-LISA kontaktuppgifter till alla myndigheter som är behöriga att pröva och besvara varje sådan begäran som avses i artiklarna 47 och 48 och ska regelbundet se över huruvida dessa kontaktuppgifter är aktuella.

5. EU-LISA ska utveckla webbportalen och säkerställa dess tekniska förvaltning.

6. Kommissionen ska anta en delegerad akt i enlighet med artikel 73 för at fastställa närmare bestämmelser om driften av webbportalen, inklusive användargränssnittet, de språk på vilka webbportalen ska finnas tillgänglig och e-postmallen.

Artikel 50

Överföring av personuppgifter till tredjeländer, internationella organisationer och privata parter

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

Artikel 51

Tillsynsmyndigheternas övervakning

1. Varje medlemsstat ska se till att tillsynsmyndigheterna på ett oberoende sätt övervakar lagligheten i den berörda medlemsstatens behandling av personuppgifter enligt den här förordningen, inklusive överföringen av dem till och från interoperabilitetskomponenterna.

2. Varje medlemsstat ska se till att de nationella lagar, föreskrifter och administrativa bestämmelser som antas i enlighet med direktiv (EU) 2016/680 vid behov är tillämpliga också på polismyndigheters och utsedda myndigheters åtkomst till interoperabilitetskomponenterna, även med avseende på rättigheterna för de personer vars uppgifter åtkomsten gäller.

3. Tillsynsmyndigheterna ska säkerställa att en revision av den behandling av personuppgifter som utförs av de ansvariga nationella myndigheterna vid tillämpningen av denna förordning genomförs i enlighet med relevanta internationella revisionsstandarder minst vart fjärde år.

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

4. Medlemsstaterna ska se till att deras tillsynsmyndigheter har de resurser och den expertis som krävs för att fullgöra de uppgifter som de åläggs enligt denna förordning.

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

Artikel 52

Europeiska datatillsynsmannens revisioner

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

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

Artikel 53

Samarbete mellan tillsynsmyndigheterna och Europeiska datatillsynsmannen

1. Tillsynsmyndigheterna och Europeiska datatillsynsmannen ska, var och en inom ramen för sina respektive befogenheter, aktivt samarbeta inom ramen för sina respektive ansvarsområden och säkerställa en samordnad tillsyn av användningen av interoperabilitetskomponenterna och tillämpningen av övriga bestämmelser i denna förordning, i synnerhet om Europeiska datatillsynsmannen eller en tillsynsmyndighet upptäcker stora skillnader mellan praxis i medlemsstaterna eller upptäcker eventuellt olagliga överföringar genom interoperabilitetskomponenternas kommunikationskanaler.

2. I de fall som avses i punkt 1 i den här artikeln ska en samordnad tillsyn säkerställas i enlighet med artikel 62 i förordning (EU) 2018/1725.

3. Europeiska dataskyddsstyrelsen ska senast den 12 juni 2021, och därefter vartannat år, skicka en gemensam rapport om sina aktiviteter enligt denna artikel till Europaparlamentet, rådet, kommissionen, Europol, Europeiska gräns- och kustbevakningsbyrån och EU-LISA. Denna rapport ska innehålla ett kapitel om varje medlemsstat som utarbetats av den berörda medlemsstatens tillsynsmyndighet.

KAPITEL VIII

Ansvarsområden

Artikel 54

EU-LISA:s ansvarsområden under utformnings- och utvecklingsfasen

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

2. Interoperabilitetskomponenterna ska hysas av EU-LISA vid dess tekniska anläggningar och ska tillhandahålla de funktioner som fastställs i denna förordning i enlighet med de krav på säkerhet, tillgänglighet, kvalitet och prestanda som anges i artikel 55.1.

3. EU-LISA ska ansvara för interoperabilitetskomponenternas utveckling, för de anpassningar som krävs för att upprätta interoperabilitet mellan de centrala systemen för in- och utresesystemet, VIS, Etias, SIS, Eurodac, Ecris-TCN, ESP, den gemensamma biometriska matchningstjänsten, CIR, MID och CRRS.

Utan att det påverkar tillämpningen av artikel 66 ska EU-LISA inte ha tillgång till några av de personuppgifter som behandlas i ESP, den gemensamma biometriska matchningstjänsten, CIR eller MID.

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

EU-LISA ska utveckla och implementera interoperabilitetskomponenterna så snart som möjligt efter ikraftträdandet av denna förordning och kommissionens antagande av de åtgärder som föreskrivs i artiklarna 8.2, 9.7, 28.5 och 28.7, 37.4, 38.3, 39.5, 43.5 och 78.10.

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

4. En förvaltningsgrupp för programmet bestående av högst tio medlemmar ska inrättas under utformnings- och utvecklingsfasen. Den ska bestå av sju medlemmar som utses av EU-LISA:s styrelse bland dess ledamöter eller ställföreträdare, ordföranden för den rådgivande grupp för interoperabilitet som avses i artikel 75, en medlem som företräder EU-LISA och som utses av dess verkställande direktör samt en medlem som utses av kommissionen. De medlemmar som utses av EU-LISA:s styrelse ska väljas enbart från de medlemsstater som enligt unionsrätten fullt ut omfattas av de rättsliga instrument som reglerar utveckling, inrättande, drift och användning av samtliga EU-informationssystem och som kommer att delta i interoperabilitetskomponenterna.

5. Förvaltningsgruppen för programmet ska sammanträda regelbundet och minst tre gånger i kvartalet. Den ska säkerställa en lämplig hantering av interoperabilitetskomponenternas utformnings- och utvecklingsfas.

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

6. EU-LISA:s styrelse ska fastställa arbetsordningen för förvaltningsgruppen för programmet, vilken i synnerhet ska innehålla bestämmelser om följande:

a) Ordförandeskap.

b) Mötesplatser.

c) Mötesförberedelser.

d) Tillträde för experter till mötena.

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

Ordförandeskapet ska innehas av en medlemsstat som enligt unionsrätten fullt ut omfattas av de rättsliga instrument som reglerar utveckling, inrättande, drift och användning av samtliga EU-informationssystem och som kommer att delta i interoperabilitetskomponenterna.

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

Den rådgivande grupp för interoperabilitet som avses i artikel 75 ska sammanträda regelbundet till dess att interoperabilitetskomponenterna tas i drift. Den ska rapportera till förvaltningsgruppen för programmet efter varje möte. Den ska tillhandahålla teknisk expertis till stöd för förvaltningsgruppens uppgifter och följa upp medlemsstaternas förberedelser.

Artikel 55

EU-LISA:s ansvarsområden före och efter idrifttagandet

1. Efter det att respektive interoperabilitetskomponent tagits i drift ska EU-LISA ansvara för den tekniska förvaltningen av den centrala infrastrukturen för interoperabilitetskomponenterna, inbegripet underhållet av dem och den tekniska utvecklingen. I samarbete med medlemsstaterna ska byrån se till att bästa tillgängliga teknik används, med förbehåll för en kostnads-nyttoanalys. EU-LISA ska också ansvara för den tekniska förvaltningen av den kommunikationsinfrastruktur som avses i artiklarna 6, 12, 17, 25 och 39.

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

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

2. Utan att det påverkar tillämpningen av artikel 17 i tjänsteföreskrifterna för tjänstemän vid Europeiska unionen ska EU-LISA tillämpa lämpliga regler avseende tystnadsplikt eller motsvarande konfidentialitetskrav på all personal som arbetar med uppgifter som lagras i interoperabilitetskomponenterna. Denna skyldighet ska gälla även efter det att den anställda i fråga lämnat sin tjänst eller anställning eller upphört med sin verksamhet.

Utan att det påverkar tillämpningen av artikel 66 ska EU-LISA inte ha tillgång till några av de personuppgifter som behandlas i ESP, den gemensamma biometriska matchningstjänsten, CIR och MID.

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

4. EU-LISA ska också utföra uppgifter avseende tillhandahållandet av utbildning om interoperabilitetskomponenternas tekniska användning.

Artikel 56

Medlemsstaternas ansvarsområden

1. Varje medlemsstat ska ansvara för följande:

a) Anslutning till ESP:s och CIR:s kommunikationsinfrastruktur.

b) Integration av de befintliga nationella systemen och infrastrukturerna med ESP, CIR och MID.

c) Organisation, förvaltning, drift och underhåll av den befintliga nationella infrastrukturen och dess anslutning till interoperabilitetskomponenterna.

d) Förvaltning av och föreskrifter för åtkomst för vederbörligen bemyndigad personal vid de behöriga nationella myndigheterna till ESP, CIR och MID i enlighet med denna förordning och upprättande och regelbunden uppdatering av en förteckning över denna personal och deras profiler.

e) Antagande av de lagstiftningsåtgärder som avses i artikel 20.5 och 20.6 för att få åtkomst till CIR i identifieringssyfte.

f) Den manuella verifiering av olika identiteter som avses i artikel 29.

g) Efterlevnad av de krav på uppgiftskvalitet som fastställs i unionsrätten.

h) Efterlevnad av reglerna i varje EU-informationssystem beträffande personuppgifternas säkerhet och integritet.

i) Avhjälpande av eventuella brister som konstaterats i kommissionens utvärderingsrapport om uppgifternas kvalitet som avses i artikel 37.5.

2. Varje medlemsstat ska ansluta sina utsedda myndigheter till CIR.

Artikel 57

Etias centralenhets ansvarsområden

Etias centralenhet ska ansvara för följande:

a) Den manuella verifieringen av olika identiteter i enlighet med artikel 29.

b) Genomförande av en spårning av multipla identiteter bland de uppgifter som lagras i in- och utresesystemet, VIS, Eurodac och SIS enligt vad som avses i artikel 69.

KAPITEL IX

Ändringar av andra unionsinstrument

Artikel 58

Ändringar av förordning (EG) nr 767/2008

Förordning (EG) nr 767/2008 ska ändras på följande sätt:

1. I artikel 1 ska följande stycke läggas till:

"Genom att lagra identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter i den gemensamma databas för identitetsuppgifter (CIR) som inrättas genom artikel 17.1 i Europaparlamentets och rådets förordning (EU) 2019/817 (*), bidrar VIS till att underlätta och stödja den korrekta identifieringen av personer som registreras i VIS på de villkor och för de syften som avses i artikel 20 i den förordningen.

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

2. I artikel 4 ska följande led läggas till:

"12. *VIS-uppgifter*: alla uppgifter som lagras i centrala VIS och i CIR i enlighet med artiklarna 9–14,

13. *identitetsuppgifter*: de uppgifter som avses i artikel 9.4 a och aa,

14. *fingeravtrycksuppgifter*: uppgifter om de fem fingeravtrycken av högra handens pekfinger, långfinger, ringfinger, lillfinger och tumme och, om dessa finns, från vänstra handen."

3. I artikel 5 ska följande punkt införas:

"1a. CIR ska innehålla de uppgifter som avses i artikel 9.4 a–c, 9.5 och 9.6. Återstående VIS-uppgifter ska lagras i centrala VIS."

4. Artikel 6.2 ska ersättas med följande:

"2. Åtkomst till VIS för att inhämta uppgifter ska uteslutande förbehållas den vederbörligen bemyndigade personal vid de nationella myndigheterna i varje medlemsstat som är behörig för de ändamål som anges i artiklarna 15–22 samt den vederbörligen bemyndigade personal vid de nationella myndigheterna i varje medlemsstat och vid unionsbyråerna som är behörig för de ändamål som anges i artiklarna 20 och 21 i förordning (EU) 2019/817. Sådan åtkomst ska ges med den begränsningen att uppgifterna ska vara nödvändiga för utförandet av deras uppgifter för dessa ändamål och stå i proportion till de mål som eftersträvas."

5. I artikel 9.4 ska leden a–c ersättas med följande:

"a) Efternamn (familjenamn), förnamn, födelsedatum, kön.

aa) Efternamn vid födseln (tidigare efternamn), födelseort och födelseland, nuvarande medborgarskap och medborgarskap vid födseln.

b) Resehandlingens eller resehandlingarnas typ och nummer och trebokstavskoden för det land som utfärdat resehandlingen eller resehandlingarna.

c) Resehandlingens eller resehandlingarnas sista giltighetsdag.

ca) Den myndighet som utfärdat resehandlingen och dag för utfärdande."

Artikel 59

Ändringar av förordning (EU) 2016/399

I artikel 8 ska följande punkt införas:

"4a. Om sökningen i relevanta databaser vid in- eller utresa, inklusive detektorn för multipla identiteter via den europeiska sökportal som inrättas genom artiklarna 25(1) och 6(1) i Europaparlamentets och rådets förordning (EU) 2019/817 (*) resulterar i en gul länk respektive upptäcker en röd länk, ska gränskontrolltjänstemannen konsultera den gemensamma databas för identitetsuppgifter som inrättas genom artikel 17.1 i den förordningen eller SIS eller båda för att bedöma skillnaderna mellan de länkade identitetsuppgifterna eller resehandlingsuppgifterna. Gränskontrolltjänstemannen ska utföra all ytterligare verifiering som krävs för att fatta ett beslut om länkens status och färg.

I enlighet med artikel 69.1 i förordning (EU) 2019/817 ska denna punkt tillämpas från och med det att detektorn för multipla identiteter tas i bruk enligt artikel 72.4 i den förordningen.

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

Artikel 60

Ändringar av förordning (EU) 2017/2226

Förordning (EU) 2017/2226 ska ändras på följande sätt:

1. I artikel 1 ska följande punkt läggas till:

"3. Genom att lagra identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter i den gemensamma databas för identitetsuppgifter (CIR) som inrättas genom artikel 17.1 i Europaparlamentets och rådets förordning (EU) 2019/817 (*) bidrar in- och utresesystemet till att underlätta och stödja den korrekta identifieringen av personer som registreras i in- och utresesystemet på de villkor och för de syften som avses i artikel 20 i den förordningen.

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

2. Artikel 3.1 ska ändras på följande sätt:

a) Led 22 ska ersättas med följande:

"22. *uppgifter i in- och utresesystemet*: alla uppgifter som lagras i in- och utresesystemets centrala system och i CIR i enlighet med artiklarna 15–20."

b) Följande led ska införas:

"22a. *identitetsuppgifter*: de uppgifter som avses i artikel 16.1 a samt de relevanta uppgifter som avses i artiklarna 17.1 och 18.1."

c) följande led ska läggas till:

"32. *ESP*: den europeiska sökportal som inrättas genom artikel 6.1 i förordning (EU) 2019/817.

33. *CIR*: den gemensamma databas för identitetsuppgifter som inrättas i genom artikel 17.1 i förordning (EU) 2019/817."

3. I artikel 6.1 ska följande led läggas till:

"j) säkerställa en korrekt identifiering av personer."

4. Artikel 7 ska ändras på följande sätt:

a) Punkt 1 ska ändras på följande sätt:

i) Följande led ska införas:

"aa) den centrala infrastrukturen för CIR som avses i artikel 17.2 a i förordning (EU) 2019/817,".

ii) Led f ska ersättas med följande:

"f) en säker kommunikationsinfrastruktur mellan in- och utresesystemets centrala system och de centrala infrastrukturerna för ESP och CIR."

b) Följande punkt ska införas:

"1a. CIR ska innehålla de uppgifter som avses i artiklarna 16.1 a–d, 17.1 a, b och c samt 18.1 och 18.2. Återstående uppgifter i in- och utresesystemet ska lagras i in- och utresesystemets centrala system."

5. I artikel 9 ska följande punkt läggas till:

"4. Åtkomst till de uppgifter i in- och utresesystemet som lagras i CIR ska uteslutande förbehållas vederbörligen bemyndigad personal vid de nationella myndigheterna i varje medlemsstat och vederbörligen bemyndigad personal vid de unionsbyråer som är behöriga för de syften som anges i artiklarna 20 och 21 i förordning (EU) 2019/817. Åtkomsten ska begränsas till den utsträckning som uppgifterna är nödvändiga för utförandet av deras arbetsuppgifter för dessa syften och stå i proportion till de mål som eftersträvas."

6. Artikel 21 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

"1. När det är tekniskt omöjligt att föra in uppgifter i in- och utresesystemets centrala system eller CIR, eller vid fel på in- och utresesystemets centrala system eller CIR, ska de uppgifter som avses i artiklarna 16–20 tillfälligt lagras i det enhetliga nationella gränssnittet. När detta är omöjligt ska uppgifterna tillfälligt lagras lokalt i elektroniskt format. I båda fallen ska uppgifterna föras in i in- och utresesystemets centrala system eller CIR så snart det är tekniskt möjligt eller felet har åtgärdats. Medlemsstaterna ska vidta lämpliga åtgärder och tillhandahålla den infrastruktur, den utrustning och de resurser som krävs för att säkerställa att sådan tillfällig lokal lagring får utföras vid vilken tidpunkt som helst och vid samtliga gränsövergångsställen."

b) I punkt 2 ska första stycket ersättas med följande:

"2. Utan att det påverkar skyldigheten att utföra in- och utresekontroller enligt förordning (EU) 2016/399 ska gränsmyndigheten, i de exceptionella fall då det är tekniskt omöjligt att föra in uppgifter i antingen in- och utresesystemets centrala system och CIR eller i det enhetliga nationella gränssnittet och tekniskt omöjligt att tillfälligt lagra uppgifterna lokalt i elektroniskt format, manuellt lagra uppgifter som avses i artiklarna 16–20 i den här förordningen, med undantag av biometriska uppgifter, och påföra tredjelandsmedborgarens resehandling en inrese- eller utresestämpel. Dessa uppgifter ska föras in i in- och utresesystemets centrala system och CIR så snart det är tekniskt möjligt."

7. Artikel 23 ska ändras på följande sätt:

a) följande punkt ska införas:

"2a. För de verifieringar som anges i punkt 1 i denna artikel ska gränsmyndigheten inleda en sökning genom att använda ESP för att jämföra uppgifterna om tredjelandsmedborgaren med de relevanta uppgifterna i in- och utresesystemet och VIS."

b) I punkt 4 ska första stycket ersättas med följande:

"4. Om sökningen på grundval av de alfanumeriska uppgifter som anges i punkt 2 i denna artikel visar att uppgifter om tredjelandsmedborgaren inte har registrerats i in- och utresesystemet, om verifieringen av tredjelandsmedborgaren i enlighet med punkt 2 i denna artikel inte lyckas eller om det råder oklarhet om tredjelandsmedborgarens identitet ska gränsmyndigheterna ha åtkomst till uppgifter för identifiering i enlighet med artikel 27 i syfte att skapa eller uppdatera en personakt i enlighet med artikel 14."

8. I artikel 32 ska följande punkt införas:

"1a. I fall där de utsedda myndigheterna har inlett en sökning i CIR i enlighet med artikel 22 i förordning (EU) 2019/817 får de ha åtkomst till in- och utresesystemet för sökningar, om de villkor som fastställs i den här artikeln är uppfyllda och om det erhållna svar som avses i artikel 22.2 i förordning (EU) 2019/817 visar att det finns uppgifter i in- och utresesystemet."

9. I artikel 33 ska följande punkt införas:

"1a. I fall där Europol har inlett en sökning i CIR i enlighet med artikel 22 i förordning (EU) 2019/817 får byrån ha åtkomst till in- och utresesystemet för sökningar, om de villkor som fastställs i den här artikeln är uppfyllda och om det erhållna svar som avses i artikel 22.2 i förordning (EU) 2019/817 visar att det finns uppgifter i in- och utresesystemet."

10. Artikel 34 ska ändras på följande sätt:

a) I punkterna 1 och 2 ska orden "i in- och utresesystemets centrala system" ersättas med orden "i CIR och i in- och utresesystemets centrala system".

b) I punkt 5 ska orden "från in- och utresesystemets centrala system" ersättas med orden "från in- och utresesystemets centrala system och CIR".

11. Artikel 35.7 ska ersättas med följande:

"7. In- och utresesystemets centrala system och CIR ska omedelbart informera alla medlemsstater om radering av uppgifter i in- och utresesystemet eller CIR samt, i tillämpliga fall, avlägsna dem från den förteckning över identifierade personer som avses i artikel 12.3."

12. I artikel 36 ska orden "in- och utresesystemets centrala system" ersättas med orden "in- och utresesystemets centrala system och CIR".

13. Artikel 37 ska ändras på följande sätt:

a) I punkt 1 ska första stycket ersättas med följande:

"1. EU-LISA ska ansvara för utvecklingen av in- och utresesystemets centrala system och CIR, de enhetliga nationella gränssnitten, kommunikationsinfrastrukturen och den säkra kommunikationskanalen mellan in- och utresesystemets centrala system och centrala VIS. EU-LISA ska också ansvara för utvecklingen av den webbtjänst som avses i artikel 13 i enlighet med de närmare bestämmelser som avses i artikel 13.7 och de specifikationer och villkor som antagits enligt artikel 36 första stycket h samt för utvecklingen av det uppgiftsregister som avses i artikel 63.2."

b) I punkt 3 ska första stycket ersättas med följande:

"3. EU-LISA ska ansvara för den operativa förvaltningen av in- och utresesystemets centrala system och CIR, de enhetliga nationella gränssnitten, den säkra kommunikationskanalen mellan in- och utresesystemets centrala system och centrala VIS. EU-LISA ska i samarbete med medlemsstaterna och med förbehåll för en kostnads-nyttoanalys säkerställa att bästa tillgängliga teknik alltid används i in- och utresesystemets centrala system och CIR, de enhetliga nationella gränssnitten, kommunikationsinfrastrukturen, den säkra kommunikationskanalen mellan in- och utresesystemets centrala system och centrala VIS, den webbtjänst som avses i artikel 13 och det uppgiftsregister som avses i artikel 63.2. EU-LISA ska också ansvara för den operativa förvaltningen av kommunikationsinfrastrukturen mellan in- och utresesystemets centrala system och de enhetliga nationella gränssnitten, den webbtjänst som avses i artikel 13 och det uppgiftsregister som avses i artikel 63.2."

14. I artikel 46.1 ska följande led läggas till:

"f) en hänvisning till användningen av ESP för sökning i in- och utresesystemet enligt vad som avses i artikel 7.2 i förordning (EU) 2019/817."

15. Artikel 63 ska ändras på följande sätt:

a) Punkt 2 ska ersättas med följande:

"2. Vid tillämpningen av punkt 1 i denna artikel ska EU-LISA lagra de uppgifter som avses i den punkten i den centrala databas för rapporter och statistik som avses i artikel 39 i förordning (EU) 2019/817."

b) I punkt 4 ska följande stycke läggas till:

"Den dagliga statistiken ska lagras i den centrala databasen för rapporter och statistik."

Artikel 61

Ändringar av förordning (EU) 2018/1240

Förordning (EU) 2018/1240 ska ändras på följande sätt:

1. I artikel 1 ska följande punkt läggas till:

"3. Genom att lagra identitetsuppgifter och resehandlingsuppgifter i den gemensamma databas för identitetsuppgifter (CIR) som inrättas genom artikel 17.1 i Europaparlamentets och rådets förordning (EU) 2019/817 (*) bidrar Etias till att underlätta och stödja den korrekta identifieringen av personer som registreras i Etias på de villkor och för de ändamål som anges i artikel 20 i den förordningen.

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

2. I artikel 3.1 ska följande led läggas till:

"23. *CIR*: den gemensamma databas för identitetsuppgifter som inrättas genom artikel 17.1 i förordning (EU) 2019/817.

24. *ESP*: den europeiska sökportal som inrättas genom artikel 6.1 i förordning (EU) 2019/817.

25. *Etias centrala system*: det centrala system som avses i artikel 6.2 a, tillsammans med CIR i den mån CIR innehåller de uppgifter som avses i artikel 6.2a.

26. *identitetsuppgifter*: de uppgifter som avses i artikel 17.2 a, b och c.

27. *resehandlingsuppgifter*: de uppgifter som avses i artikel 17.2 d och e och trebokstavskoden för det land som utfärdat resehandlingen enligt vad som avses i artikel 19.3 c."

3. I artikel 4 ska följande led läggas till:

"g) Bidra till en korrekt identifiering av personer."

4. Artikel 6 ska ändras på följande sätt:

a) Punkt 2 ska ändras på följande sätt:

i) Led a ska ersättas med följande:

"a) ett centralt system, inklusive Etias bevakningslista som avses i artikel 34,".

ii) Följande led ska införas:

"a) CIR,".

iii) Led d ska ersättas med följande:

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

b) Följande punkt ska införas:

"2a. CIR ska innehålla identitetsuppgifter och resehandlingsuppgifter. De återstående uppgifterna ska lagras i det centrala systemet."

5. Artikel 13 ska ändras på följande sätt:

a) Följande punkt ska införas:

"4a. Åtkomst till identitets- och resehandlingsuppgifterna i Etias som lagras i CIR ska också uteslutande förbehållas vederbörligen bemyndigad personal vid de nationella myndigheterna i varje medlemsstat och vederbörligen bemyndigad personal vid de unionsbyråer som är behöriga för de ändamål som anges i artiklarna 20 och 21 i förordning (EU) 2019/817. Sådan åtkomst ska ges med den begränsningen att uppgifterna ska vara nödvändiga för att de ska kunna utföra sina arbetsuppgifter i enlighet med dessa ändamål och stå i proportion till mål som eftersträvas."

b) Punkt 5 ska ersättas med följande:

"5. Varje medlemsstat ska utse de behöriga nationella myndigheter som avses i punkterna 1, 2, 4 och 4a i denna artikel och ska översända en förteckning över dessa myndigheter till EU-LISA utan dröjsmål, i enlighet med artikel 87.2. I denna förteckning ska det anges för vilka ändamål den vederbörligen bemyndigade personalen vid varje myndighet ska få åtkomst till uppgifterna i Etias informationssystem i enlighet med punkterna 1, 2, 4 och 4a i den här artikeln."

6. Artikel 172 ska ändras på följande sätt:

a) Led a ska ersättas med följande:

"a) Efternamn (familjenamn), förnamn, efternamn vid födseln, födelsedatum, födelseort, kön, nuvarande medborgarskap."

b) Följande led ska införas:

"aa) Födelseland, föräldrarnas förnamn."

7. I artikel 19.4 ska orden "artikel 17.2 a" ersättas med orden "artikel 17.2 a och 17.2 aa".

8. Artikel 20 ska ändras på följande sätt:

a) I punkt 2 ska första stycket ersättas med följande:

"2. Etias centrala system ska inleda en sökning genom att använda ESP för att jämföra de relevanta uppgifter som avses i artikel 17.2 a, aa, b, c, d, f, g, j, k och m och 17.8 med uppgifterna i ett register, en akt eller en registrering i en ansökningsakt i Etias centrala system, SIS, in- och utresesystemet, VIS, Eurodac, Europoluppgifter och Interpols databaser SLTD och TDAWN."

b) I punkt 4 ska orden "artikel 17.2 a, b, c, d, f, g, j, k och m" ersättas med orden "artikel 17.2 a, aa, b, c, d, f, g, j, k och m".

c) I punkt 5 ska orden "artiklarna 17.2 a, c, f, h och i " ersättas med orden "artikel 17.2 a, aa, c, f, h och i".

9. Artikel 23.1 ska ersättas med följande:

"1. Etias centrala system ska inleda en sökning genom att använda ESP för att jämföra de relevanta uppgifter som avses i artikel 17.2 a, aa, b och d med uppgifter i SIS för att avgöra om sökanden är föremål för någon av följande registreringar:

a) En registrering om försvunna personer.

b) En registrering om personer som söks för att delta i ett rättsligt förfarande.

c) En registrering om personer som omfattas av diskreta eller särskilda kontroller."

10. I artikel 52 ska följande punkt införas:

"1a. I fall där de utsedda myndigheterna har inlett en sökning i CIR i enlighet med artikel 22 i förordning (EU) 2019/817 får de ha åtkomst till ansökningsakter i Etias centrala system i enlighet med den här artikeln för sökningar om det erhållna svar som avses i artikel 22.2 i förordning (EU) 2019/817 visar att det finns uppgifter i ansökningsakterna i Etias centrala system."

11. I artikel 53 ska följande punkt införas:

"1a. I fall där Europol har inlett en sökning i CIR i enlighet med artikel 22 i förordning (EU) 2019/817. får byrån ha åtkomst till ansökningsakter i Etias centrala system i enlighet med den här artikeln för sökningar om det erhållna svar som avses i artikel 22.2 i förordning (EU) 2019/817 visar att det finns uppgifter i ansökningsakterna i Etias centrala system."

12. I artikel 65.3 femte stycket ska orden "artikel 17.2 a, b, d, e och f" ersättas med orden "artikel 17.2 a, aa, b, d, e och f".

13. I artikel 69.1 ska följande led införas:

"ca) i tillämpliga fall en hänvisning till att ESP använts för sökning i Etias centrala system enligt vad som avses i artikel 7.2 i förordning (EU) 2019/817,".

14. I artikel 73.2 ska orden "centralregistret" ersättas med orden "den centrala databas för rapporter och statistik som avses i artikel 39 i förordning (EU) 2019/817, i den mån den innehåller uppgifter från Etias centrala system i enlighet med artikel 84 i den här förordningen,".

15. I artikel 74.1 ska första stycket ersättas med följande:

"1. När Etias tagits i drift ska EU-LISA ansvara för den tekniska förvaltningen av Etias centrala system och de enhetliga nationella gränssnitten. EU-LISA ska också ansvara för all teknisk provning som krävs för inrättandet och uppdateringen av Etias sökregler. Byrån ska i samarbete med medlemsstaterna om inte annat följer av en kostnads-nyttoanalys säkerställa att bästa tillgängliga teknik alltid används. EU-LISA ska också ansvara för den tekniska förvaltningen av kommunikationsinfrastrukturen mellan Etias centrala system och de enhetliga nationella gränssnitten samt för den offentliga webbplatsen, appen för mobila enheter, e-posttjänsten, den säkra kontotjänsten, kontrollverktyget för sökande, samtyckesverktyget för sökande, bedömningsverktyget för Etias bevakningslista, nätportalen för transportörer, webbtjänsten och programvaran för att behandla ansökningarna."

16. I artikel 84.2 ska första stycket ersättas med följande:

"2. Vid tillämpningen av punkt 1 i denna artikel ska EU-LISA lagra de uppgifter som avses i den punkten i den centrala databas för rapporter och statistik som avses i artikel 39 i förordning (EU) 2019/817. I enlighet med artikel 39.1 i den förordningen ska systemöverskridande statistiska uppgifter och analysrapporter ge de myndigheter som avses i punkt 1 i den här artikeln möjlighet att få anpassade rapporter och statistik, för att stödja genomförandet av Etias sökregler som avses i artikel 33, för att bättre kunna bedöma säkerhetsrisken, risken för olaglig invandring och den höga epidemirisken, för att effektivisera in- och utresekontroller samt för att hjälpa Etias centralenhet och de nationella Etiasenheterna att behandla ansökningar om resetillstånd."

17. I artikel 84.4 ska följande stycke läggas till:

"Den dagliga statistiken ska lagras i den centrala databasen för rapporter och statistik som avses i artikel 39 i förordning (EU) 2019/817."

Artikel 62

Ändringar av förordning (EU) 2018/1726

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

1. Artikel 12 ska ersättas med följande:

"*Artikel 12*

Uppgifternas kvalitet

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

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

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

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

2. Artikel 19.1 ska ändras på följande sätt:

a) Följande led ska införas:

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

b) Led ff ska ersättas med följande:

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

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

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

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

c) Led hh ska ersättas med följande:

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

d) Led mm ska ersättas med följande:

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

3. Artikel 22.4 ska ersättas med följande:

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

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

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

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

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

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

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

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

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

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

5. Artikel 27 ska ändras på följande sätt:

a) I punkt 1 ska följande led införas:

"da) Den rådgivande gruppen för interoperabilitet."

b) Punkt 3 ska ersättas med följande:

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

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

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

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

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

Artikel 63

Ändringar av förordning (EU) 2018/1861

Förordning (EU) 2018/1861 ska ändras på följande sätt:

1. I artikel 3 ska följande led läggas till:

"22. *ESP*: den europeiska sökportal som inrättas genom artikel 6.1 i Europaparlamentets och rådets förordning (EU) 2019/817 (*).

23. *den gemensamma biometriska matchningstjänsten*: den gemensamma biometriska matchningstjänst som inrättas genom artikel 12.1 i förordning (EU) 2019/817.

24. *CIR*: den gemensamma databas för identitetsuppgifter som inrättas genom artikel 17.1 i förordning (EU) 2019/817.

25. *MID*: den detektor för multipla identiteter som inrättas genom artikel 25.1 i förordning (EU) 2019/817.

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

2. Artikel 4 ska ändras på följande sätt:

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

"b) Ett nationellt system (nedan kallat *N.SIS*) i var och en av medlemsstaterna, bestående av de nationella datasystem som står i förbindelse med det centrala SIS, inklusive minst en nationell eller gemensam backup av N.SIS.

c) En kommunikationsinfrastruktur som förenar CS-SIS och dess backup samt NI-SIS (nedan kallad *kommunikationsinfrastrukturen*) och som tillhandahåller ett krypterat virtuellt nätverk särskilt avsett för SIS-uppgifter och utbytet av uppgifter mellan Sirenekontoren i enlighet med vad som avses i artikel 7.2.

d) En säker kommunikationsinfrastruktur mellan CS-SIS och de centrala infrastrukturerna för ESP, den gemensamma biometriska matchningstjänsten och MID."

b) Följande punkter ska läggas till:

"8. Utan att det påverkar tillämpningen av punkterna 1–5 får sökningar i SIS-uppgifter göras också via ESP.

9. Utan att det påverkar tillämpningen av punkterna 1–5 får SIS-uppgifter också överföras via den säkra kommunikationsinfrastruktur som avses i punkt 1 d. Dessa överföringar ska begränsas till den utsträckning i vilken uppgifterna krävs för tillämpningen av förordning (EU) 2019/817."

3. I artikel 7 ska följande punkt införas:

"2a. Sirenekontoren ska också säkerställa den manuella verifieringen av olika identiteter i enlighet med artikel 29 i förordning (EU) 2019/817. I den utsträckning som krävs för att utföra denna uppgift ska Sirenekontoren ha åtkomst till uppgifterna i CIR och MID för de ändamål som anges i artiklarna 21 och 26 i förordning (EU) 2019/817."

4. Artikel 12.1 ska ersättas med följande:

"1. Medlemsstaterna ska säkerställa att all åtkomst till och alla utbyten av personuppgifter i CS-SIS loggas i landets N.SIS för att möjliggöra kontroll av huruvida sökningen var laglig, övervakning av att uppgiftsbehandlingen sker på ett lagligt sätt, egenkontroll, säkerställande av att N.SIS fungerar tillfredsställande samt för dataintegritet och datasäkerhet. Detta gäller inte de automatiska processer som avses i artikel 4.6 a, b och c.

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

5. I artikel 34.1 ska följande led läggas till:

"g) Verifiering av olika identiteter och bekämpande av identitetsbedrägeri i enlighet med kapitel V i förordning (EU) 2019/817."

6. Artikel 60.6 ska ersättas med följande:

"6. Vid tillämpningen av artikel 15.4 och punkterna 3, 4 och 5 i den här artikeln ska EU-LISA lagra de uppgifter som avses i artikel 15.4 och i punkt 3 i den här artikeln, vilka inte ska möjliggöra identifiering av enskilda personer, i den centrala databas för rapporter och statistik som avses i artikel 39 i förordning (EU) 2019/817.

EU-LISA ska låta kommissionen och de organ som avses i punkt 5 i denna artikel få skräddarsydd rapportering och statistik. På begäran ska EU-LISA bevilja medlemsstaterna, kommissionen, Europol och Europeiska gräns- och kustbevakningsbyrån åtkomst till den centrala databasen för rapporter och statistik i enlighet med artikel 39 i förordning (EU) 2019/817."

Artikel 64

Ändringar av beslut 2004/512/EG

I beslut 2004/512/EG ska artikel 1.2 ersättas med följande:

"2. Informationssystemet för viseringar ska vara baserat på en centraliserad struktur och bestå av

a) den centrala infrastrukturen för den gemensamma databas för identitetsuppgifter som avses i artikel 17.2 a i Europaparlamentets och rådets förordning (EU) 2019/817 (*),

b) ett centralt informationssystem, nedan kallat *Centrala informationssystemet för viseringar* (CS-VIS),

c) ett gränssnitt i varje medlemsstat, nedan kallat *Nationella gränssnittet* (NI-VIS), som ska utgöra en förbindelse med den berörda centrala nationella myndigheten i respektive medlemsstat,

d) en infrastruktur för kommunikation mellan Centrala informationssystemet för viseringar och de nationella gränssnitten,

e) en säker kommunikationskanal mellan in- och utresesystemets centrala system och CS-VIS,

f) en säker kommunikationsinfrastruktur mellan centrala VIS och de centrala infrastrukturerna för den europeiska sökportal som inrättas genom artikel 6.1 i förordning (EU) 2019/817 och den gemensamma databas för identitetsuppgifter som inrättas genom artikel 17.1 i förordning (EU) 2019/817.

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

Artikel 65

Ändringar av rådets beslut 2008/633/RIF

Beslut 2008/633/RIF ska ändras på följande sätt:

1. I artikel 5 ska följande punkt införas:

”1a. I fall där de utsedda myndigheterna har inlett en sökning i den gemensamma databasen för identitetsuppgifter (CIR) i enlighet med artikel 22 i Europaparlamentets och rådets förordning (EU) 2019/817 (*), och de villkor för åtkomst som fastställs i den här artikeln är uppfyllda, får de ha åtkomst till VIS för sökningar om det svar som erhålls enligt artikel 22.2 i den förordningen visar att det finns uppgifter i VIS.

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

2. I artikel 7 ska följande punkt införas:

”1a. I fall där Europol har inlett en sökning i CIR i enlighet med artikel 22 i förordning (EU) 2019/817, och de villkor för åtkomst som fastställs i den här artikeln är uppfyllda, får byrån ha åtkomst till VIS för sökningar om det svar som erhålls enligt artikel 22.2 i den förordningen visar att det finns uppgifter i VIS.”

KAPITEL X

Slutbestämmelser

Artikel 66

Rapportering och statistik

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

a) Antalet sökningar per ESP-användarprofil.

b) Antalet sökningar i var och en av Interpols databaser.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

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

a) Antalet sökningar för de syften som avses i artiklarna 20, 21 och 22.

b) Personens medborgarskap, kön och födelseår.

c) Typ av resehandling och trebokstavskoden för det utfärdande landet.

d) Antalet sökningar som utförts med och utan biometriska uppgifter.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

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

a) Antalet sökningar som utförts med och utan biometriska uppgifter.

b) Antalet länkar per typ och de EU-informationssystem som innehåller de länkade uppgifterna.

c) Den tidsperiod under vilken en gul och en röd länk har blivit kvar i systemet.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

4. Den vederbörligen bemyndigade personalen vid Europeiska gräns- och kustbevakningsbyrån ska ha åtkomst för att söka på de uppgifter som avses i punkterna 1, 2 och 3 i denna artikel i syfte att utföra de riskanalyser och sårbarhetsanalyser som avses i artiklarna 11 och 13 i Europaparlamentets och rådets förordning (EU) 2016/1624 ([40]).

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

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

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

Artikel 67

Övergångsperiod för användning av den europeiska sökportalen

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

2. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 73 för att ändra denna förordning genom att förlänga den period som avses i punkt 1 den här artikeln en gång med högst ett år, om en bedömning av genomförandet av ESP visar att en sådan förlängning är nödvändig, särskilt mot bakgrund av de konsekvenser som idrifttagandet av ESP skulle ha för organisationen och varaktigheten av in- och utresekontroller.

Artikel 68

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

Artiklarna 22, 60.8 och 60.9, 61.10 och 61.11 och 65 ska tillämpas från och med den dag för idrifttagande av CIR som avses i artikel 72.3.

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

Artikel 69

Övergångsperiod för spårning av multipla identiteter

1. Under en ettårsperiod efter det att EU-LISA har anmält slutförandet av det test av MID som avses i artikel 72.4 b och innan MID tas i drift ska Etias centralenhet ansvara för att utföra spårning av multipla identiteter med användning av de uppgifter som lagras i in- och utresesystemet, VIS, Eurodac och SIS. Spårningarna av multipla identiteter ska utföras med hjälp av enbart biometriska uppgifter.

2. Om sökningen ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är desamma eller liknande, ska en vit länk skapas i enlighet med artikel 33.

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

Vid flera träffar ska en länk skapas mellan alla uppgifter som gett upphov till träffen.

3. Om en gul länk skapas ska MID bevilja Etias centralenhet åtkomst till de identitetsuppgifter som finns i de olika EU-informationssystemen.

4. Om det skapas en länk till en registrering i SIS, förutom en registrering som skapats enligt artikel 3 i förordning (EU) 2018/1860, artiklarna 24 och 25 i förordning (EU) 2018/1861 eller artikel 38 i förordning (EU) 2018/1862, ska MID bevilja Sirenekontoret i den medlemsstat som skapade registreringen åtkomst till de identitetsuppgifter som finns i de olika informationssystemen.

5. Etias centralenhet eller, i de fall som avses i punkt 4 i denna artikel, Sirenekontoret i den medlemsstat som skapade registreringen ska ha åtkomst till de uppgifter som finns i akten med identitetsbekräftelse och ska bedöma de olika identiteterna samt uppdatera länken i enlighet med artiklarna 31, 32 och 33 och lägga till den i akten med identitetsbekräftelse.

6. Etias centralenhet ska underrätta kommissionen i enlighet med artikel 71.3 först efter det alla gula länkar har verifierats manuellt och deras status uppdaterats till antingen gröna, vita eller röda länkar.

7. Medlemsstaterna ska vid behov bistå Etias centralenhet med att utföra spårning av multipla identiteter enligt denna artikel.

8. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 73 för att ändra denna förordning genom att förlänga den period som avses i punkt 1 i den här artikeln med sex månader, vilken kan förlängas två gånger med sex månader i taget. En sådan förlängning ska beviljas endast efter en bedömning av den uppskattade tiden för slutförande av spårning av multipla identiteter enligt denna artikel som visar att spårningen av multipla identiteter inte kan slutföras före utgången av den period som återstår antingen enligt punkt 1 i den här artikeln eller av en pågående förlängning, av skäl som ligger utanför Etias centralenhets kontroll, och att inga avhjälpande åtgärder kan tillämpas. Bedömningen ska genomföras senast tre månader före utgången av en sådan period eller av en pågående förlängning.

Artikel 70

Kostnader

1. Kostnaderna i samband med inrättandet och driften av ESP, den gemensamma biometriska matchningstjänsten, CIR och MID ska belasta unionens allmänna budget.

2. Kostnaderna i samband med integreringen av befintliga nationella infrastrukturer och deras anslutning till de enhetliga nationella gränssnitten samt i samband med förvaltandet av de enhetliga nationella gränssnitten ska belasta unionens allmänna budget.

Följande kostnader ska vara undantagna:

a) Medlemsstaternas projektledningskontor (möten, tjänsteresor, kontor).

b) Hysande av nationella it-system (lokaler, implementering, elektricitet, kylning).

c) Drift av nationella it-system (operatörs- och supportavtal).

d) Utformning, utveckling, implementering, drift och underhåll av nationella kommunikationsnätverk.

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

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

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

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

Artikel 71

Underrättelser

1. Medlemsstaterna ska underrätta EU-LISA om de myndigheter som avses i artiklarna 7, 20, 21 och 26 och som får använda eller ha åtkomst till ESP, CIR respektive MID.

En konsoliderad förteckning över dessa myndigheter ska offentliggöras i *Europeiska unionens officiella tidning* inom tre månader efter den dag då respektive interoperabilitetskomponent togs i drift i enlighet med artikel 72. Om förteckningen ändras ska EU-LISA en gång om året offentliggöra en uppdaterad konsoliderad förteckning.

2. EU-LISA ska underrätta kommissionen om att det test som avses i artikel 72.1 b, 72.2 b, 72.3 b, 72.4 b, 72.5 b och 72.6 b har slutförts på ett framgångsrikt sätt.

3. Etias centralenhet ska underrätta kommissionen om att den övergångsperiod som avses i artikel 69 har slutförts på ett framgångsrikt sätt.

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

Artikel 72

Driftsstart

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

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

b) EU-LISA har förklarat att ett övergripande test av ESP, vilket ska utföras av EU-LISA i samarbete med medlemsstaternas myndigheter och de unionsbyråer som får använda ESP, har slutförts på ett framgångsrikt sätt.

c) EU-LISA har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 8.1 och har anmält dessa till kommissionen.

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

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

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

a) De åtgärder som avses i artiklarna 13.5 och 43.5 har antagits.

b) EU-LISA har förklarat att ett övergripande test av den gemensamma biometriska matchningstjänsten, vilket ska utföras av EU-LISA i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.

c) EU-LISA har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 13 och har anmält dessa till kommissionen.

d) EU-LISA har förklarat att det test som avses i punkt 5 b har slutförts på ett framgångsrikt sätt.

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

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

a) De åtgärder som avses i artiklarna 43.5 och 78.10 har antagits.

b) EU-LISA har förklarat att ett övergripande test av CIR, vilket ska utföras av EU-LISA i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.

c) EU-LISA har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 18 och har anmält dessa till kommissionen.

d) EU-LISA har förklarat att det test som avses i punkt 5 b har slutförts på ett framgångsrikt sätt.

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

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

a) De åtgärder som avses i artiklarna 28.5, 28.7, 32.5, 33.6, 43.5 och 49.6 har antagits.

b) EU-LISA har förklarat att ett övergripande test av MID, vilket ska utföras av EU-LISA i samarbete med medlemsstaternas myndigheter och Etias centralenhet, har slutförts på ett framgångsrikt sätt.

c) EU-LISA har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 34 och har anmält dessa till kommissionen.

d) Etias centralenhet har underrättat kommissionen i enlighet med artikel 71.3.

e) EU-LISA har förklarat att de tester som avses i punkterna 1 b, 2 b, 3 b och 5 b har slutförts på ett framgångsrikt sätt.

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

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

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

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

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

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

a) De åtgärder som avses i artiklarna 39.5 och 43.5 har antagits.

b) EU-LISA har förklarat att ett övergripande test av CRRS, vilket ska utföras av EU-LISA i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.

c) EU-LISA har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 39 och har anmält dessa till kommissionen.

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

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

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

Artikel 73

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 28.5, 39.5, 49.6, 67.2 och 69.8 ska ges till kommissionen för en period på fem år från och med den 11 juni 2019. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av femårsperioden. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i artiklarna 28.5, 39.5, 49.6, 67.2 och 69.8 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning* eller vid ett senare datum som anges i beslutet. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 28.5, 39.5, 49.6, 67.2 och 69.8 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 74

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

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

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

Artikel 75

Rådgivande grupp

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

Artikel 76

Utbildning

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

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

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

Artikel 77

Handbok

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

Artikel 78

Övervakning och utvärdering

1. EU-LISA ska säkerställa att det finns förfaranden för att övervaka utvecklingen av interoperabilitetskomponenterna och deras anslutning till det enhetliga nationella gränssnittet mot bakgrund av målen för planering och kostnader samt för att övervaka interoperabilitetskomponenternas funktion mot bakgrund av målen för tekniska resultat, kostnadseffektivitet, säkerhet och tjänsternas kvalitet.

2. Senast den 12 december 2019 och därefter var sjätte månad under interoperabilitetskomponenternas utvecklingsfas ska EU-LISA lämna en rapport till Europaparlamentet och rådet om hur utvecklingen av interoperabilitetskomponenterna och deras anslutning till det enhetliga nationella gränssnittet fortskrider. Så snart utvecklingsarbetet har slutförts ska en rapport lämnas till Europaparlamentet och rådet med en ingående redogörelse för hur målen för framför allt planering och kostnader har uppfyllts samt vad eventuella avvikelser beror på.

3. Fyra år efter det att respektive interoperabilitetskomponent har tagits i drift i enlighet med artikel 72 och därefter vart fjärde år, ska EU-LISA rapportera till Europaparlamentet, rådet och kommissionen om interoperabilitetskomponenternas tekniska funktion, inbegripet ur säkerhetssynpunkt.

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

a) En bedömning av tillämpningen av denna förordning.

b) En granskning av uppnådda resultat i relation till denna förordnings mål och dess inverkan på de grundläggande rättigheterna, inbegripet i synnerhet en bedömning av påverkan av interoperabilitetskomponenterna på rätten till icke-diskriminering.

c) En bedömning av hur webbportalen fungerar, inklusive sifferuppgifter om användningen av webbportalen och antalet tillgodosedda begäranden.

d) En bedömning av huruvida de förutsättningar som ligger till grund för interoperabilitetskomponenterna fortfarande är giltiga.

e) En bedömning av säkerheten i interoperabilitetskomponenterna.

f) En bedömning av användningen av CIR för identifiering.

g) En bedömning av användningen av CIR för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

h) En bedömning av eventuella konsekvenser, inbegripet eventuell oproportionellt stor inverkan på trafikflödet vid gränsövergångsställena, samt budgetkonsekvenser för unionens allmänna budget.

i) En bedömning av sökningar i Interpols databaser via ESP, inbegripet information om antalet träffar i Interpols databaser samt information om eventuella problem som uppstått.

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

5. Senast den 12 juni 2020 och därefter varje år fram till dess att kommissionen har antagit de genomförandeakter som avses i artikel 72 ska kommissionen lägga fram en rapport för Europaparlamentet och rådet om läget i fråga om förberedelserna för ett fullständigt genomförande av denna förordning. Denna rapport ska även innehålla detaljerad information om de kostnader som uppkommit och information om eventuella risker som kan påverka de totala kostnaderna.

6. Två år efter idrifttagande av MID i enlighet med artikel 72.4 ska kommissionen göra en granskning av hur MID påverkar rätten till icke-diskriminering. Efter denna första rapport ska granskningen av hur MID påverkar rätten till icke-diskriminering vara en del av den granskning som avses i punkt 4 b i den här artikeln.

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

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

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

a) de exakta syftena med sökningarna, däribland vilken typ av terroristbrott eller andra grova brott det gällt,

b) de välgrundade skälen att tro att en person som misstänks för, har begått eller utsatts för ett brott omfattas av förordning (EU) 2017/2226, förordning (EG) nr 767/2008 eller förordning (EU) 2018/1240,

c) antalet begäranden om åtkomst till CIR i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott,

d) antalet och de typer av ärenden som har lett till identifieringar,

e) behovet och utnyttjandet av möjligheten att åberopa brådskande undantagsfall, inklusive de fall där brådska inte godtogs som skäl vid den kontroll i efterhand som genomfördes av den centrala åtkomstpunkten.

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

10. En teknisk lösning ska göras tillgänglig för medlemsstaterna i syfte att hantera åtkomstbegäranden från användare enligt vad som avses i artikel 22 och underlätta insamlingen av informationen enligt i punkterna 7 och 9 i den här artikeln i syfte att generera de rapporter och den statistik som avses i de punkterna. Kommissionen ska anta genomförandeakter för att fastställa specifikationerna för den tekniska lösningen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 74.2.

Artikel 79

Ikraftträdande och tillämplighet

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

De bestämmelser i denna förordning som rör ESP ska tillämpas från den dag som fastställs av kommissionen i enlighet med artikel 72.1.

De bestämmelser i denna förordning som rör den gemensamma biometriska matchningstjänsten ska tillämpas från den dag som fastställs av kommissionen i enlighet med artikel 72.2.

De bestämmelser i denna förordning som rör CIR, ska tillämpas från den dag som fastställs av kommissionen i enlighet med artikel 72.3.

De bestämmelser i denna förordning som rör MID, ska tillämpas från den dag som fastställs av kommissionen i enlighet med artikel 72.4.

De bestämmelser i denna förordning som rör de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma uppgiftskvalitetsindikatorerna samt minimikvalitetsstandarderna för uppgifter ska tillämpas från den dag som fastställs av kommissionen i enlighet med artikel 72.5.

De bestämmelser i denna förordning som rör CRRS ska tillämpas från och med den dag som fastställs av kommissionen i enlighet med artikel 72.6.

Artiklarna 6, 12, 17, 25, 38, 42, 54, 56, 57, 70, 71, 73, 74, 75, 77 och 78.1 ska tillämpas från och med den 11 juni 2019.

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

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

Utfärdad i Bryssel 20 maj 2019.

På Europaparlamentets vägnar	*På rådets vägnar*
A. TAJANI	G. CIAMBA
Ordförande	*Ordförande*

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/818

av den 20 maj 2019

om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

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

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande [1],

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet [2], och

av följande skäl:

(1) Kommissionen underströk i sitt meddelande av den 6 april 2016 med titeln *Starkare och smartare informationssystem för gränser och säkerhet* behovet av att förbättra unionens uppgiftshanteringsstruktur för gränsförvaltning och säkerhet. Meddelandet inledde arbetet för att uppnå interoperabilitet mellan EU-informationssystem för säkerhet, gränser och migrationshantering, i syfte att komma till rätta med de strukturella brister i systemen som hindrar de nationella myndigheternas arbete och att säkerställa att gränskontrolltjänstemän, tullmyndigheter, poliser och rättsliga myndigheter har tillgång till den information de behöver.

(2) Rådet identifierade i sin Färdplan för förbättring av informationsutbytet och informationshanteringen, inbegripet interoperabilitetslösningar på området för rättsliga och inrikes frågor av den 6 juni 2016 olika rättsliga, tekniska och operativa utmaningar när det gäller interoperabilitet mellan EU-informationssystem och efterlyste en strävan efter lösningar.

(3) I sin resolution av den 6 juli 2016 om de strategiska prioriteringarna för kommissionens arbetsprogram 2017 [3] efterlyste Europaparlamentet förslag för att förbättra och utveckla befintliga EU-informationssystem, åtgärda luckor i informationen och gå i riktning mot interoperabilitet samt förslag om obligatoriskt informationsutbyte på EU-nivå åtföljda av de bestämmelser om dataskydd som krävs.

(4) I sina slutsatser av den 15 december 2016 uppmanade Europeiska rådet till ansträngningar för att fortsatt tillhandahålla resultat i fråga om interoperabilitet mellan EU:s informationssystem och databaser.

(5) Expertgruppen för informationssystem och interoperabilitet konstaterade i sin slutrapport av den 11 maj 2017 att det var nödvändigt och tekniskt genomförbart att eftersträva praktiska lösningar för interoperabilitet och att interoperabilitet i princip både kan ge operativa vinster och erhållas i överensstämmelse med dataskyddskraven.

(6) Kommissionen presenterade i sitt meddelande av den 16 maj 2017 med titeln *Sjunde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*, i enlighet med sitt meddelande av den 6 april 2016 och resultaten och rekommendationerna från expertgruppen för informationssystem och interoperabilitet, en ny strategi för uppgiftshantering när det gäller gränser, säkerhet och migration där alla EU-informationssystem för säkerhet, gränsförvaltning och migrationshantering kommer att vara interoperabla på ett sätt som fullt ut respekterar de grundläggande rättigheterna.

[1] EUT C 283, 10.8.2018, s. 48.
[2] Europaparlamentets ståndpunkt av den 16 april 2019 (ännu ej offentliggjord i EUT) och rådets beslut av den 14 maj 2019.
[3] EUT C 101, 16.3.2018, s. 116.

(7) I sina slutsatser av den 9 juni 2017 om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabiliteten mellan EU-informationssystem uppmanade rådet kommissionen att i sitt arbete följa de lösningar för interoperabilitet som expertgruppen föreslagit.

(8) I sina slutsatser av den 23 juni 2017 underströk Europeiska rådet behovet av att förbättra interoperabiliteten mellan databaser och uppmanade kommissionen att så snart som möjligt utarbeta förslag till lagstiftning på grundval av förslagen från expertgruppen för informationssystem och interoperabilitet.

(9) I syfte att förbättra ändamålsenligheten och effektiviteten i kontrollerna vid de yttre gränserna, bidra till att förebygga och bekämpa olaglig invandring och främja en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen – bland annat att upprätthålla den allmänna säkerheten och allmänna ordningen och trygga säkerheten inom medlemsstaternas territorier förbättra genomförandet av den gemensamma viseringspolitiken, bistå vid prövningen av ansökningar om internationellt skydd, bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott, underlätta identifieringen av okända personer vid en naturkatastrof, en olycka eller ett terrordåd, i syfte att upprätthålla allmänhetens förtroende för unionens migrations- och asylsystem, unionens säkerhetsåtgärder och unionens förmåga att förvalta de yttre gränserna, bör interoperabilitet inrättas mellan EU-informationssystemen, dvs. in- och utresesystemet, Informationssystemet för viseringar (VIS), EU-systemet för reseuppgifter och resetillstånd (Etias), Eurodac, Schengens informationssystem (SIS) och det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN), så att dessa EU-informationssystem och de uppgifter som de innehåller kompletterar varandra, med respekt för den enskildes grundläggande rättigheter, i synnerhet rätten till skydd av personuppgifter. För att uppnå detta bör en europeisk sökportal (ESP), en gemensam biometrisk matchningstjänst, en gemensam databas för identitetsuppgifter (CIR) och en detektor för multipla identiteter (MID) inrättas som interoperabilitetskomponenter.

(10) Interoperabiliteten mellan EU-informationssystem bör göra det möjligt för dessa system att komplettera varandra för att underlätta korrekt identifiering av personer, däribland okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor, bidra till att bekämpa identitetsbedrägeri, förbättra och harmonisera kvalitetskraven på uppgifterna i respektive EU-informationssystem, underlätta medlemsstaternas tekniska implementering och operativa drift av EU-informationssystem, stärka de skyddsåtgärder för datasäkerhet och dataskydd som reglerar respektive EU-informationssystem, rationalisera åtkomst till in- och utresesystemet, VIS, Etias och Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, samt stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

(11) Interoperabilitetskomponenterna bör omfatta in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. De bör också omfatta Europoluppgifter, men endast i den mån som krävs för att Europoluppgifter ska kunna sökas samtidigt med dessa EU-informationssystem.

(12) Interoperabilitetskomponenterna bör behandla personuppgifterna för personer vars personuppgifter behandlas i de underliggande EU-informationssystemen och av Europol.

(13) ESP bör inrättas för att tekniskt underlätta medlemsstaternas myndigheters och unionsbyråernas snabba, smidiga, effektiva, systematiska och kontrollerade åtkomst till EU-informationssystem, Europoluppgifter och Internationella kriminalpolisorganisationens (Interpol) databaser i den mån som krävs för att de ska kunna utföra sina uppgifter, i enlighet med deras åtkomsträttigheter. ESP bör även inrättas för att stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS, Ecris-TCN och Europoluppgifter. Genom att göra det möjligt att utföra parallella sökningar i alla relevanta EU-informationssystem, Europoluppgifter och Interpols databaser bör ESP fungera som en gemensam kontaktpunkt eller *meddelandehanterare* för att söka i de olika centrala systemen och smidigt hämta den nödvändiga informationen, med full respekt för de underliggande systemens åtkomstkontroll och dataskyddskrav.

(14) Utformningen av ESP bör, vid en sökning i Interpols databaser, säkerställa att de uppgifter som används av en ESP-användare för att inleda en sökning inte delas med ägarna av Interpols uppgifter. Utformningen av ESP bör även säkerställa att sökningar i Interpols databaser enbart sker i enlighet med tillämplig unionsrätt och nationell rätt.

(15) De ESP-användare som har åtkomsträtt till Europoluppgifter enligt Europaparlamentets och rådets förordning (EU) 2016/794 [4] bör kunna göra sökningar i Europoluppgifter samtidigt med de EU-informationssystem som de har åtkomst till. All ytterligare behandling av uppgifter efter en sådan sökning bör ske i enlighet med förordning (EU) 2016/794, inklusive restriktioner i fråga om åtkomst eller användning som dataleverantören har fastställt.

(16) ESP bör utvecklas och konfigureras så att det endast går att göra sådana sökningar med uppgifter som rör personer eller resehandlingar som finns i ett EU-informationssystem, i Europoluppgifter eller i Interpols databaser.

(17) För att säkerställa systematisk användning av de relevanta EU-informationssystemen bör ESP användas för att söka i CIR, in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN. En nationell uppkoppling till de olika EU-informationssystemen bör dock behållas som en teknisk reserv. ESP bör också användas av unionens byråer för att göra sökningar i centrala SIS i enlighet med deras åtkomsträttigheter och för att de ska kunna utföra sina uppgifter. ESP bör vara ytterligare ett sätt att söka i centrala SIS, Europoluppgifter och Interpols databaser, som ett komplement till de befintliga särskilda gränssnitten.

(18) Biometriska uppgifter, såsom fingeravtryck och ansiktsbilder, är unika och ger därför en mycket mer tillförlitlig identifiering av en person än alfanumeriska uppgifter. Den gemensamma biometriska matchningstjänsten bör vara ett tekniskt verktyg för att stärka och underlätta arbetet för de relevanta EU-informationssystemen och de andra interoperabilitetskomponenterna. Huvudsyftet med den gemensamma biometriska matchningstjänsten bör vara att underlätta identifiering av en person som har registrerats i flera databaser, genom att använda en enda teknisk komponent för att matcha den personens biometriska uppgifter mellan olika system, i stället för flera komponenter. Den gemensamma biometriska matchningstjänsten bör främja säkerhet och ge fördelar i fråga om kostnader, underhåll och drift. Alla automatiska fingeravtrycksidentifieringssystem, även de som för närvarande används för Eurodac, VIS och SIS, använder biometriska mallar bestående av uppgifter som härrör från en särdragsextraktion från faktiska biometriska prov. Den gemensamma biometriska matchningstjänsten bör samla och lagra alla dessa biometriska mallar – logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör – på ett enda ställe och därigenom underlätta jämförelser mellan systemen med användning av biometriska mallar och möjliggöra stordriftsfördelar vid utveckling och underhåll av de centrala EU-systemen.

(19) De biometriska mallar som lagras i den gemensamma biometriska matchningstjänsten och bör bestå av uppgifter som härrör från en särdragsextraktion från faktiska biometriska prov och erhållas på ett sådant sätt att det inte går att vända på extraktionsprocessen. De biometriska mallarna bör erhållas från biometriska uppgifter, men det bör inte vara möjligt att få fram dessa biometriska uppgifter från de biometriska mallarna. Eftersom handavtryck och DNA-profiler lagras endast i SIS, och inte kan inte användas för att genomföra korskontroller mot uppgifter som finns i andra informationssystem, i enlighet med principerna om nödvändighet och proportionalitet, bör den gemensamma biometriska matchningstjänsten inte lagra DNA-profiler eller biometriska mallar som erhålls från handavtryck.

(20) Biometriska uppgifter utgör känsliga personuppgifter. Denna förordning bör fastställa grunden och skyddsåtgärder för behandlingen av sådana uppgifter i syfte att entydigt identifiera de berörda personerna.

(21) In- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN kräver en korrekt identifiering av de personer vars personuppgifter lagras i dem. CIR bör därför underlätta en korrekt identifiering av personer som har registrerats i dessa system.

(22) Personuppgifter som lagras i dessa EU-informationssystem kan avse samma personer men under olika eller ofullständiga identiteter. Medlemsstaterna förfogar över effektiva metoder att identifiera sina medborgare eller personer som är registrerade som varaktigt bosatta på deras territorium. Interoperabiliteten mellan EU-informationssystem bör bidra till en korrekt identifiering av personer som är registrerade i dessa system. CIR bör lagra de personuppgifter som behövs för att göra det möjligt att mer korrekt identifiera de personer vars uppgifter lagras i de systemen, inklusive deras identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter, oavsett vilket system uppgifterna ursprungligen samlades in i. Endast de personuppgifter som är absolut nödvändiga för att utföra en korrekt identitetskontroll bör lagras i CIR. De personuppgifter som registreras i CIR bör inte behållas längre än vad som är absolut nödvändigt för de underliggande systemens syften och bör raderas automatiskt när uppgifterna har raderats i det underliggande systemet i enlighet med den logiska separeringen.

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

(23) En ny behandling, som består i lagring av sådana uppgifter i CIR i stället för lagring i vart och ett av de separata systemen är nödvändig för att det ska vara möjligt att förbättra identifieringens tillförlitlighet genom den automatiska jämförelsen och matchningen av uppgifterna. Det faktum att identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter lagras i CIR bör inte på något sätt hindra den behandling av uppgifter som sker med avseende på in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN, eftersom CIR bör vara en ny gemensam komponent i dessa underliggande system.

(24) Det är därför nödvändigt att skapa en personakt i CIR för varje person som har registrerats i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN, för att uppnå syftet med en korrekt identifiering av personer inom Schengenområdet och för att stödja MID i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. Personakten bör lagra all den identitetsinformation som avser en person på ett enda ställe och ge vederbörligen bemyndigade slutanvändare åtkomst till den.

(25) CIR således underlätta och rationalisera åtkomst för myndigheter med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott till de EU-informationssystem som inte har inrättats uteslutande i syfte att förebygga, förhindra, upptäcka eller utreda grov brottslighet.

(26) CIR bör tillhandahålla en gemensam lagringsplats för identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter om personer som har registrerats i in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN. CIR bör utgöra en del av den tekniska arkitekturen i dessa system och fungera som den gemensamma komponenten mellan dem för att lagra och söka i de identitetsuppgifter, resehandlingsuppgifter och biometriska uppgifter som de behandlar.

(27) Alla poster i CIR bör separeras logiskt genom att varje post automatiskt taggas med namnet på det underliggande system som äger den uppgiften. CIR:s åtkomstkontroller bör använda dessa taggar för att avgöra huruvida åtkomst till posten ska medges.

(28) Om en medlemsstats polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet, eller om det föreligger tvivel om de identitetsuppgifter som lämnats av den personen eller om resehandlingens äkthet eller dess innehavares identitet eller om personen inte kan eller vägrar att samarbeta, bör polismyndigheten i fråga kunna göra en sökning i CIR för att identifiera personen. För dessa ändamål bör polisen ta fingeravtryck med hjälp av tekniker för direktscanning av fingeravtryck, under förutsättning att förfarandet inleddes i den berörda personens närvaro. Sådana sökningar i CIR bör inte tillåtas för identifiering av minderåriga under 12 år, såvida de inte görs för barnets bästa.

(29) Om en persons biometriska uppgifter inte kan användas eller en sökning med dessa uppgifter misslyckas bör sökningen utföras med personens identitetsuppgifter i kombination med resehandlingsuppgifter. Om sökningen visar att det finns uppgifter om personen i CIR bör medlemsstaternas myndigheter ha åtkomst till CIR för att ta del av den personens identitetsuppgifter och resehandlingsuppgifter, utan att det i CIR anges vilket EU-informationssystem uppgifterna tillhör.

(30) Medlemsstaterna bör anta nationella lagstiftningsåtgärder för att utse de myndigheter som är behöriga att utföra identitetskontroller med hjälp av CIR och fastställa förfarandena, villkoren och kriterierna för sådana kontroller, vilka bör vara förenliga med proportionalitetsprincipen. I synnerhet bör befogenheten för en anställd vid en sådan myndighet att ta biometriska uppgifter av en person under en identitetskontroll föreskrivas i nationell rätt.

(31) Genom denna förordning bör det också införas en ny möjlighet till rationaliserad åtkomst till andra uppgifter än identitetsuppgifter och resehandlingsuppgifter i in- och utresesystemet, VIS, Etias eller Eurodac för medlemsstaternas utsedda myndigheter med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott samt för Europol. Sådana uppgifter kan vara nödvändiga för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i ett specifikt fall där det finns rimliga skäl att anta att en konsultation av dem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrotten eller andra aktuella grova brott, särskilt om det finns misstankar om att en person som misstänks för, har begått eller utsatts för ett terroristbrott eller ett annat grovt brott är en person vars uppgifter lagras i in- och utresesystemet, VIS, Etias eller Eurodac.

(32) Fullständig åtkomst till uppgifter som finns i EU-informationssystemen som är nödvändig för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, utöver åtkomst till identitetsuppgifter eller resehandlingsuppgifter som finns i CIR, bör även i fortsättningen regleras genom de tillämpliga rättsliga instrumenten. De utsedda myndigheterna med ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott samt Europol vet inte på förhand vilket EU-informationssystem som innehåller uppgifter om de personer de behöver göra sökningar om. Detta leder till förseningar och ineffektivitet. Den slutanvändare som har bemyndigats av den utsedda myndigheten bör därför ha rätt att se i vilket av dessa EU-informationssystem de uppgifter som motsvarar resultatet av en sökning är registrerade. Det berörda systemet skulle på så vis flaggas efter den automatiska kontrollen att det finns en träff i systemet (en så kallad flaggfunktion för träff).

(33) I detta sammanhang bör ett svar från CIR inte tolkas eller användas som en grund för en slutsats om eller en anledning att vidta åtgärder med avseende på en person, utan bör användas uteslutande i syfte att lämna in begäran om åtkomst till de underliggande EU-informationssystemen, med förbehåll för de villkor och förfaranden som fastställs i respektive rättsliga instrument som reglerar sådan åtkomst. Varje sådan begäran om åtkomst bör omfattas av kapitel VII i denna förordning och i tillämpliga fall av Europaparlamentets och rådets förordning (EU) 2016/679 ([5]), Europaparlamentets och rådets direktiv (EU) 2016/680 ([6]) eller Europaparlamentets och rådets förordning (EU) 2018/1725 ([7]).

(34) Som en allmän regel bör de utsedda myndigheterna eller Europol begära full åtkomst till minst ett av de berörda EU-informationssystemen, om en flaggning för träff anger att uppgifterna är registrerade i Eurodac. Om sådan full åtkomst i undantagsfall inte begärs – till exempel därför att de utsedda myndigheterna eller Europol redan har erhållit uppgifterna på annat sätt eller att erhållandet av uppgifterna inte längre är tillåtet enligt nationell rätt – bör motiveringen till att inte begära åtkomst registreras.

(35) Loggarna över sökningarna i CIR bör visa syftet med sökningarna. Om en sådan sökning har gjorts med tvåstegsstrategin för sökningar bör loggarna innehålla en referens till den nationella akten för utredningen eller ärendet, och därmed ange att sökningen gjordes för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

(36) Den sökning i CIR som görs av de utsedda myndigheterna och Europol för att få ett svar i form av en flaggning som anger att uppgifterna finns i in- och utresesystemet, VIS, Etias eller Eurodac kräver automatiserad behandling av personuppgifter. En flaggning för träff bör inte avslöja några personuppgifter om den berörda personen, utan endast en angivelse om att vissa uppgifter om vederbörande lagras i ett av systemen. Den bemyndigade slutanvändaren bör inte fatta några negativa beslut om den berörda personen endast utifrån det faktum att en sökning gett en flaggning för träff. Slutanvändarens åtkomst till en flaggning för träff kommer därför utgöra ett mycket begränsat ingrepp i den berörda personens rätt till skydd av personuppgifter, samtidigt som det ger de utsedda myndigheterna och Europol möjlighet att på ett mer effektivt sätt begära åtkomst till personuppgifter.

(37) MID bör inrättas för att stödja CIR i dess funktion och för att stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN. För att effektivt uppfylla sina respektive syften kräver alla dessa EU-informationssystem en korrekt identifiering av de personer vars personuppgifter lagras i dem.

(38) För att bättre förverkliga syftena med EU-informationssystemen bör de myndigheter som använder dessa system kunna utföra en tillräckligt tillförlitlig verifiering av identiteten på de personer vars uppgifter lagras i olika system. Den uppsättning identitetsuppgifter eller resehandlingsuppgifter som lagras i ett visst enskilt system kan vara

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

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

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

inkorrekt, ofullständig eller falsk, och i dagsläget finns det inget sätt att upptäcka inkorrekta, ofullständiga eller falska identitetsuppgifter eller resehandlingsuppgifter genom jämförelser med uppgifter som lagras i ett annat system. För att råda bot på denna situation är det nödvändigt att på unionsnivå ha ett tekniskt instrument som möjliggör en korrekt identifiering av personer för dessa ändamål.

(39) MID bör skapa och lagra länkar mellan uppgifter i de olika EU-informationssystemen för att spåra multipla identiteter, i det dubbla syftet att underlätta identitetskontroller för resenärer med ärligt uppsåt och bekämpa identitetsbedrägeri. MID bör endast innehålla länkar mellan uppgifter om personer som har registrerats i fler än ett EU-informationssystem. De länkade uppgifterna bör vara strikt begränsade till de uppgifter som krävs för att verifiera att en person har registrerats på ett berättigat eller oberättigat sätt med olika identiteter i olika system, eller för att klargöra att två personer med liknande identitetsuppgifter kanske inte är samma person. Behandlingen av uppgifter genom ESP och den gemensamma biometriska matchningstjänsten för att länka personakter mellan olika system bör hållas till ett absolut minimum och är således begränsad till spårning av multipla identiteter, som ska ske vid den tidpunkt då nya uppgifter läggs till i ett av de system som har uppgifter lagrade i CIR eller som lagts till i SIS. MID bör omfatta skyddsåtgärder mot potentiell diskriminering och ogynnsamma beslut mot personer som lagligen har multipla identiteter.

(40) I denna förordning föreskrivs ny uppgiftsbehandling som syftar till att korrekt identifiera de berörda personerna. Detta utgör ett ingrepp i deras grundläggande rättigheter som skyddas genom artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Eftersom EU-informationssystemen är beroende av att de berörda personerna identifieras korrekt för att fungera effektivt är detta ingrepp motiverat av samma syften som lett till att vart och ett av dessa system har inrättats, nämligen en effektiv förvaltning av unionens gränser, den inre säkerheten i unionen och ett effektivt genomförande av unionens asyl- och viseringspolitik.

(41) ESP och den gemensamma biometriska matchningstjänsten bör jämföra uppgifter om personer i CIR och SIS när en nationell myndighet eller en unionsbyrå skapar eller laddar upp nya uppgifter. Dessa jämförelser bör göras automatiskt. CIR och SIS bör använda den gemensamma biometriska matchningstjänsten för att upptäcka möjliga länkar på grundval av biometriska uppgifter. CIR och SIS bör använda ESP för att upptäcka möjliga länkar på grundval av alfanumeriska uppgifter. CIR och SIS bör kunna identifiera identiska eller liknande uppgifter om en person vilka är lagrade i flera system. När så är fallet bör en länk som anger att det är samma person skapas. CIR och SIS bör konfigureras på ett sätt som gör att små translittereringsfel eller stavfel upptäcks, så att det inte skapar omotiverade olägenheter för den berörda personen.

(42) Den nationella myndighet eller unionsbyrå som registrerade uppgifterna i respektive EU-informationssystem bör bekräfta eller ändra länkarna. Denna nationella myndighet eller unionsbyrå bör ha åtkomst till de uppgifter som lagras i CIR eller SIS och i MID för manuell verifiering av olika identiteter.

(43) En manuell verifiering av olika identiteter bör säkerställas av den myndighet som skapat eller uppdaterat de uppgifter som lett till en träff som ger upphov till en länk med uppgifter som lagras i ett annat EU-informationssystem. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter bör bedöma om det finns multipla identiteter som på ett berättigat eller oberättigat sätt hänvisar till en och samma person. En sådan bedömning bör om möjligt utföras i den berörda personens närvaro och när så är nödvändigt genom att begära ytterligare klargöranden eller information. Bedömningen bör göras utan dröjsmål, i enlighet med de rättsliga kraven på korrekt information enligt unionsrätten och nationell rätt.

(44) För länkar som erhålls genom SIS med registreringar avseende personer som är efterlysta för att gripas och överlämnas eller för att utlämnas, försvunna eller utsatta personer, personer som söks för att delta i ett rättsligt förfarande och personer som omfattas av diskreta kontroller eller undersökningskontroller bör den myndighet som ansvarar för manuell verifiering av olika identiteter vara Sirenekontoret i den medlemsstat som har skapat registreringen. Dessa kategorier av SIS-registreringar är känsliga och bör inte nödvändigtvis delas med de

myndigheter som skapar eller uppdaterar uppgifter som länkas till dem i ett av de andra EU-informationssystemen. Skapandet av en länk med SIS-uppgifter bör inte påverka de åtgärder som ska vidtas i enlighet med Europaparlamentets och rådets förordningar (EU) 2018/1860 ([8]), (EU) 2018/1861 ([9]) och (EU) 2018/1862 ([10]).

(45) Skapandet av sådana länkar förutsätter öppenhet gentemot berörda personer. För att underlätta genomförandet av nödvändiga skyddsåtgärder i enlighet med unionens tillämpliga dataskyddsbestämmelser bör personer som är föremål för en röd länk eller en vit länk efter manuell verifiering av olika identiteter informeras skriftligen utan att det påverkar tillämpningen av begränsningar för att trygga säkerheten och den allmänna ordningen, förebygga och förhindra brott samt garantera att nationella utredningar inte äventyras. Dessa personer bör erhålla ett enda identifikationsnummer som gör det möjligt för dem att identifiera den myndighet till vilken de bör vända sig för att utöva sina rättigheter.

(46) Om en gul länk skapas bör den myndighet som ansvarar för manuell verifiering av olika identiteter ha åtkomst till MID. Om det finns en röd länk bör medlemsstaternas myndigheter och unionens byråer som har åtkomst till minst ett EU-informationssystem som ingår i CIR eller till SIS ha åtkomst till MID. En röd länk bör visa att en person använder olika identiteter på ett oberättigat sätt eller att en person använder någon annan persons identitet.

(47) När det förekommer en vit eller grön länk mellan uppgifter från två EU-informationssystem bör medlemsstaternas myndigheter och unionens byråer ha åtkomst till MID, om den berörda myndigheten eller byrån har åtkomst till båda informationssystemen. Sådan åtkomst bör beviljas endast i syfte att göra det möjligt för den myndigheten eller byrån att upptäcka potentiella fall där uppgifter har länkats inkorrekt eller behandlats i MID, CIR och SIS i strid med denna förordning samt för att vidta åtgärder för att avhjälpa bristerna och uppdatera eller radera länken.

(48) Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-Lisa) bör inrätta automatiserade mekanismer för kvalitetskontroll av uppgifter och gemensamma indikatorer för uppgiftskvalitet. eu-Lisa bör ansvara för att utveckla en central övervakningskapacitet för uppgiftskvalitet och regelbundet utarbeta dataanalysrapporter för att förbättra kontrollen av medlemsstaternas implementering av EU-informationssystemen. De gemensamma indikatorerna för uppgiftskvalitet bör inbegripa minimikvalitetsstandarder för lagring av uppgifter i EU-informationssystemen eller interoperabilitetskomponenter. Målet med sådana standarder för uppgiftskvalitet bör vara att EU-informationssystemen och interoperabilitetskomponenterna automatiskt ska kunna identifiera inmatade uppgifter som verkar vara inkorrekta eller inkonsekventa, så att ursprungsmedlemsstaten kan verifiera uppgifterna och vidta de korrigerande åtgärder som behövs.

(49) Kommissionen bör utvärdera eu-Lisas kvalitetsrapporter och utfärda rekommendationer till medlemsstaterna när så är lämpligt. Medlemsstaterna bör ansvara för utarbetandet av en handlingsplan som beskriver åtgärder för att rätta till eventuella brister i uppgifternas kvalitet och bör regelbundet rapportera om framstegen.

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

(51) Möjligheten kan övervägas att införa UMF-standarden i VIS, SIS och alla andra befintliga eller nya gränsöverskridande modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor vilka utvecklas av medlemsstaterna.

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

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

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

(52) En central databas för rapporter och statistik (CRRS) bör inrättas för att generera systemöverskridande statistiska uppgifter och analytisk rapportering för verksamhetsstyrande och operativa syften samt för uppgiftskvalitet i enlighet med tillämpliga rättsliga instrument. eu-Lisa bör inrätta, implementera och hysa CRRS i sina tekniska anläggningar. Den bör innehålla anonymiserade statistiska uppgifter från EU-informationssystemen, CIR, MID och den gemensamma biometriska matchningstjänsten. Uppgifterna i CRRS bör inte möjliggöra identifiering av enskilda personer. eu-Lisa bör automatiskt anonymisera uppgifterna och registrera de anonymiserade uppgifterna i CRRS. Anonymiseringsprocessen bör vara automatisk, och eu-Lisas personal bör inte beviljas direkt åtkomst till några personuppgifter som lagras i EU-informationssystemen eller i interoperabilitetskomponenterna.

(53) Förordning (EU) 2016/679 är tillämplig på de nationella myndigheternas behandling av personuppgifter i interoperabilitetssyfte inom ramen för denna förordning, förutom om behandlingen görs av medlemsstaternas utsedda myndigheter eller centrala kontaktpunkter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

(54) Direktiv (EU) 2016/680 är tillämpligt i de fall medlemsstaternas behandling av personuppgifter utförs av de behöriga myndigheterna i interoperabilitetssyfte i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

(55) Förordning (EU) 2016/679 förordning (EU) 2018/1725 eller, i tillämpliga fall, direktiv (EU) 2016/680 tillämpas på överföringar av personuppgifter till tredjeländer eller internationella organisationer som utförs enligt den här förordningen. Utan att det påverkar grunderna för överföring enligt kapitel V i förordning (EU) 2016/679 eller, i tillämpliga fall, direktiv (EU) 2016/680, bör en dom i en domstol eller ett beslut av en administrativ myndighet i ett tredjeland som kräver att en personuppgiftsansvarig eller ett personuppgiftsbiträde ska överföra eller offentliggöra personuppgifter erkännas eller verkställas på något sätt endast om domen eller beslutet grundar sig på ett internationellt avtal som är i kraft mellan det begärande tredjelandet och unionen eller en medlemsstat.

(56) De särskilda bestämmelserna om dataskydd i Europaparlamentets och rådets förordning (EU) 2018/1862 och Europaparlamentets och rådets förordning (EU) 2019/816 ([11]) är tillämpliga på behandlingen av personuppgifter i de system som regleras genom dessa förordningar.

(57) Förordning (EU) 2018/1725 är tillämplig på behandling av personuppgifter som utförs av eu-Lisa och unionens andra institutioner och organ när de fullgör sina skyldigheter enligt den här förordningen, utan att det påverkar tillämpningen av förordning (EU) 2016/794, som är tillämplig på Europols behandling av personuppgifter.

(58) De tillsynsmyndigheter som avses i förordning (EU) 2016/679 eller direktiv (EU) 2016/680 bör övervaka lagligheten i medlemsstaternas behandling av personuppgifter. Europeiska datatillsynsmannen, bör övervaka unionsinstitutionernas och unionsorganens behandling av personuppgifter. Europeiska datatillsynsmannen och tillsynsmyndigheterna bör samarbeta med varandra vid övervakningen av interoperabilitetkomponenternas behandling av personuppgifter. För att Europeiska datatillsynsmannen ska kunna utföra sina uppgifter enligt den här förordningen krävs tillräckliga både personella och ekonomiska resurser.

(59) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ([12]) och avgav ett yttrande den 16 april 2018 ([13]).

(60) Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (artikel 29-gruppen) avgav ett yttrande den 11 april 2018.

(61) Både medlemsstaterna och eu-Lisa bör ha säkerhetsplaner för att underlätta genomförandet av säkerhetsskyldigheterna och bör samarbeta med varandra för att hantera säkerhetsproblem. eu-Lisa bör också se till att man fortlöpande utnyttjar den senaste tekniska utvecklingen för att säkerställa dataintegritet i fråga om utveckling, utformning och förvaltning av interoperabilitetskomponenterna. eu-Lisas skyldigheter i detta avseende bör

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

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

([13]) EUT C 233, 4.7.2018, s. 12.

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

(62) Till stöd för statistik och rapportering är det nödvändigt att bevilja bemyndigad personal vid de behöriga myndigheter, unionsinstitutioner och unionsbyråer som avses i denna förordning åtkomst till vissa uppgifter som rör vissa interoperabilitetskomponenter utan att möjliggöra identifiering av enskilda personer.

(63) För att medlemsstaternas myndigheter och unionsbyråerna ska kunna anpassa sig till de nya kraven beträffande användningen av ESP är det nödvändigt att föreskriva en övergångsperiod. Likaledes bör övergångsåtgärder fastställas för driftsättningen av MID för att den ska fungera konsekvent och optimalt.

(64) Eftersom målet för denna förordning, nämligen att inrätta en ram för interoperabilitet mellan EU-informationssystem, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(65) Det återstående beloppet i den budget som öronmärkts för smarta gränser i Europaparlamentets och rådets förordning (EU) nr 515/2014 ([15]) bör omfördelas till den här förordningen, i enlighet med artikel 5.5 b i förordning (EU) nr 515/2014, för att täcka kostnaderna för utveckling av interoperabilitetskomponenterna.

(66) För att komplettera vissa detaljerade tekniska aspekter i denna förordning bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) delegeras till kommissionen med avseende på

— förlängning av övergångsperioden för användning av ESP,

— förlängning av övergångsperioden för spårning av multipla identiteter som utförs av Etias centralenhet,

— förfarandena för att fastställa de fall där identitetsuppgifterna kan betraktas som desamma eller liknande samt

— reglerna för driften av CRRS, däribland särskilda skyddsåtgärder för behandling av personuppgifter och säkerhetsregler tillämpliga på databasen,

— samt närmare regler om driften av webbportalen.

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

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

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

([15]) Europaparlamentets och rådets förordning (EU) nr 515/2014 av den 16 april 2014 om inrättande, som en del av fonden för inre säkerhet, av ett instrument för ekonomiskt stöd för yttre gränser och visering och om upphävande av beslut nr 574/2007/EG (EUT L 150, 20.5.2014, s. 143).

([16]) EUT L 123, 12.5.2016, s. 1.

(68) Kommissionen bör även tilldelas genomförandebefogenheter med avseende på antagande av närmare bestämmelser om tekniska detaljer i användarprofilerna för ESP, specifikationer för den tekniska lösningen som gör det möjligt att utföra sökningar i EU-informationssystemen, Europoluppgifter och Interpols databaser genom ESP samt formatet för svaren från ESP, tekniska regler för att skapa länkar i MID mellan uppgifter från olika EU-informationssystem, innehållet i och utformningen av det formulär som ska användas för att informera den registrerade när en röd länk skapas, prestandakrav och prestandaövervakning för den gemensamma biometriska matchningstjänsten, mekanismer, förfaranden och indikatorer för automatiserad kontroll av uppgiftskvalitet, utveckling av UMF-standarden, det samarbetsförfarande som ska användas i händelse av säkerhetsincidenter, samt specifikationerna för den tekniska lösningen för medlemsstaternas hantering av åtkomstbegäranden från användare. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([17]).

(69) Eftersom interoperabilitetskomponenterna kommer att medföra behandling av betydande mängder känsliga personuppgifter är det viktigt att personer vars uppgifter behandlas genom dessa komponenter i praktiken kan utöva sina rättigheter som registrerade i enlighet med förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725. De registrerade bör få tillgång till en webbportal som gör det lättare för dem att utöva sin rätt till åtkomst till och rättelse, radering och begränsning av behandlingen av deras personuppgifter. eu-Lisa bör inrätta och förvalta en sådan webbportal.

(70) En av huvudprinciperna i samband med dataskydd är uppgiftsminimering. Enligt artikel 5.1 c i förordning (EU) 2016/679 ska de personuppgifter som behandlas vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Interoperabilitetskomponenterna bör därför inte lagra några nya personuppgifter, med undantag för de länkar som kommer att lagras i MID och som utgör det minimum som krävs för tillämpningen av den här förordningen.

(71) Denna förordning bör innehålla tydliga bestämmelser om ansvar och rätten till ersättning vid otillåten behandling av personuppgifter och vid någon annan åtgärd som är oförenlig med den. Sådana bestämmelser bör inte påverka rätten till ersättning från samt ansvaret för den personuppgiftsansvarige eller personuppgiftsbiträdet enligt förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725. eu-Lisa bör vara ansvarig för skada som den orsakat i sin egenskap av personuppgiftsbiträde om byrån inte har fullgjort de skyldigheter som den specifikt har ålagts enligt den här förordningen eller om den har agerat utanför eller i strid med lagenliga instruktioner från den medlemsstat som är personuppgiftsansvarig.

(72) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2004/38/EG ([18]).

(73) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, deltar Danmark inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Danmark. Eftersom denna förordning, i den utsträckning som dess bestämmelser rör SIS såsom det regleras genom förordning (EU) 2018/1862, är en utveckling av Schengenregelverket ska Danmark, i enlighet med artikel 4 i det protokollet, inom sex månader efter det att rådet har beslutat i fråga om den här förordningen, besluta huruvida landet ska genomföra den i sin nationella rätt.

(74) I den utsträckning som dess bestämmelser rör SIS såsom det regleras genom förordning (EU) 2018/1862, deltar Förenade kungariket i den här förordningen, i enlighet med artikel 5.1 i protokoll nr 19 om Schengenregelverket införlivat inom Europeiska unionens ramar, fogat till EU-fördraget och EUF-fördraget och artikel 8.2 i rådets beslut 2000/365/EG ([19]). I den utsträckning som dess bestämmelser rör Eurodac och Ecris-TCN i enlighet med artikel 3 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och till EUF-fördraget, har Förenade kungariket dessutom genom en skrivelse av den 16 maj 2018 meddelat att det önskar delta i antagandet och tillämpningen av denna förordning.

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

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

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

(75) I den utsträckning som dess bestämmelser rör SIS såsom det regleras genom förordning (EU) 2018/1862, kunde Irland i princip delta i denna förordning i enlighet med artikel 5.1 i protokoll nr 19 om Schengenregelverket införlivat inom Europeiska unionens ramar, fogat till EU-fördraget och EUF-fördraget, och artikel 6.2 i rådets beslut 2002/192/EG ([20]). I den utsträckning som dess bestämmelser rör Eurodac och Ecris-TCN, i enlighet med artiklarna 1 och 2 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och till EUF-fördraget, och utan att det påverkar tillämpningen av artikel 4 i det protokollet, deltar Irland inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Irland. Eftersom det under dessa omständigheter inte är möjligt att säkerställa att denna förordning i alla delar är tillämplig på Irland, såsom krävs enligt artikel 288 i EUF-fördraget, deltar Irland inte i antagandet av denna förordning, utan att det påverkar Irlands rättigheter enligt protokollen nr 19 och nr 21.

(76) När det gäller Island och Norge utgör denna förordning, i den utsträckning den rör SIS såsom det regleras genom förordning (EU) 2018/1862, i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([21]), en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1 G i rådets beslut 1999/437/EG ([22]).

(77) När det gäller Schweiz utgör denna förordning, i den utsträckning den rör SIS såsom det regleras genom förordning (EU) 2018/1862, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([23]), en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1 G i rådets beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2008/149/RIF ([24]).

(78) När det gäller Liechtenstein utgör denna förordning, i den utsträckning den rör SIS såsom det regleras genom förordning (EU) 2018/1862, i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Lichtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([25]), en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1 G i rådets beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2011/350/EU ([26]).

(79) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns i synnerhet i Europeiska unionens stadga om de grundläggande rättigheterna, och bör tillämpas i enlighet med dessa rättigheter och principer.

(80) För att denna förordning ska passa in i den befintliga rättsliga ramen bör Europaparlamentets och rådets förordningar (EU) 2018/1726 ([27]), (EU) 2018/1862 och (EU) 2019/816 ändras i enlighet med detta.

([20]) Rådets beslut 2002/192/EG av den 28 februari 2002 om Irlands begäran om att få delta i vissa bestämmelser i Schengenregelverket (EGT L 64, 7.3.2002, s. 20).
([21]) EGT L 176, 10.7.1999, s. 36.
([22]) Rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtal som har ingåtts mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EGT L 176, 10.7.1999, s. 31).
([23]) EUT L 53, 27.2.2008, s. 52.
([24]) Rådets beslut 2008/149/RIF av den 28 januari 2008 om ingående på Europeiska unionens vägnar av avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 53, 27.2.2008, s. 50).
([25]) EUT L 160, 18.6.2011, s. 21.
([26]) Rådets beslut 2011/350/EU av den 7 mars 2011 om ingående på Europeiska unionens vägnar av protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, om avskaffande av kontroller vid de inre gränserna och om personers rörlighet (EUT L 160, 18.6.2011, s. 19).
([27]) Europaparlamentets och rådets förordning (EU) 2018/1726 av den 14 november 2018 om Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-Lisa), om ändring av förordning (EG) nr 1987/2006 och rådets beslut 2007/533/RIF och om upphävande av förordning (EU) nr 1077/2011 (EUT L 295, 21.11.2018, s. 99).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. Genom denna förordning tillsammans med Europaparlamentets och rådets förordning (EU) 2019/817 ([28]) inrättas en ram för att säkerställa interoperabilitet mellan in- och utresesystemet, Informationssystemet för viseringar (VIS), EU-systemet för reseuppgifter och resetillstånd (Etias), Eurodac, Schengens informationssystem (SIS) och Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN).

2. Denna ram ska omfatta följande interoperabilitetskomponenter:

a) En europeisk sökportal (ESP).

b) En gemensam biometrisk matchningstjänst.

c) En gemensam databas för identitetsuppgifter (CIR).

d) En detektor för multipla identiteter (MID).

3. Denna förordning innehåller också bestämmelser om kraven på uppgifternas kvalitet, ett universellt meddelandeformat (UMF), en central databas för rapporter och statistik (CRRS) och om ansvarsområden för medlemsstaterna och Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-Lisa) vad gäller utformningen, utvecklingen och driften av interoperabilitetskomponenterna.

4. Genom denna förordning anpassas också förfarandena och villkoren för att de utsedda myndigheterna och Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) ska få åtkomst till in- och utresesystemet, VIS, Etias och Eurodac i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

5. I denna förordning fastställs också ramar för verifiering av personers identitet och för identifiering av personer.

Artikel 2

Mål

1. Genom att säkerställa interoperabilitet har denna förordning följande mål:

a) Förbättra ändamålsenligheten och effektiviteten hos in- och utresekontrollerna vid de yttre gränserna.

b) Bidra till att förebygga och bekämpa olaglig invandring.

c) Bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen, bland annat att bevara allmän säkerhet och allmän ordning och trygga säkerheten på medlemsstaternas territorier.

d) Förbättra genomförandet av den gemensamma viseringspolitiken.

e) Bistå vid prövningen av en ansökan om internationellt skydd.

f) Bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott och andra grova brott.

g) Underlätta identifieringen av okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor vid en naturkatastrof, olycka eller ett terrordåd.

2. De mål som avses i punkt 1 ska uppnås genom att:

a) säkerställa en korrekt identifiering av personer,

b) bidra till kampen mot identitetsbedrägerier,

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

c) förbättra uppgiftskvaliteten och harmonisera kvalitetskraven på uppgifter som lagras i EU-informationssystemen, samtidigt som kraven avseende uppgiftsbehandling i de rättsliga instrument som reglerar de enskilda systemen samt normerna och principerna för dataskydd respekteras,

d) underlätta och stödja medlemsstaternas tekniska implementering och operativa drift av EU-informationssystem,

e) skärpa och förenkla de villkor för datasäkerhet och dataskydd som reglerar de respektive EU-informationssystemen och göra dem mer enhetliga, utan att det påverkar det särskilda skyddet och de särskilda skyddsåtgärderna för vissa kategorier av uppgifter,

f) rationalisera villkoren för utsedda myndigheters åtkomst till in- och utresesystemet, VIS, Etias och Eurodac, samtidigt som nödvändiga och proportionella villkor för denna åtkomst säkerställs,

g) stödja syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

Artikel 3

Tillämpningsområde

1. Denna förordning ska tillämpas på Eurodac, SIS och Ecris-TCN.

2. Denna förordning ska också tillämpas på Europoluppgifter i en utsträckning som gör det möjligt att söka i dem samtidigt som i de EU-informationssystem som avses i punkt 1.

3. Denna förordning ska tillämpas på personer vars personuppgifter får behandlas i de EU-informationssystem som avses i punkt 1 och i de Europoluppgifter som avses i punkt 2.

Artikel 4

Definitioner

I denna förordning avses med

1. *yttre gränser*: yttre gränser enligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2016/399 ([29]),

2. *in- och utresekontroller*: in- och utresekontroller enligt definitionen i artikel 2.11 i förordning (EU) 2016/399,

3. *gränsmyndighet*: den gränskontrolltjänsteman som i enlighet med nationell rätt tilldelats uppgiften att genomföra in- och utresekontroller,

4. *tillsynsmyndigheter*: den tillsynsmyndighet som avses i artikel 51.1 i förordning (EU) 2016/679 och den tillsynsmyndighet som avses i artikel 41.1 i direktiv (EU) 2016/680,

5. *verifiering*: förfarandet att jämföra en uppsättning uppgifter med en annan för att fastställa om en påstådd identitet är riktig (*one-to-one-check*),

6. *identifiering*: förfarandet att fastställa en persons identitet genom en databassökning mot flera grupper av uppgifter (*one-to-many-check*),

7. *alfanumeriska uppgifter*: uppgifter som återges med bokstäver, siffror, specialtecken, mellanslag och skiljetecken,

8. *identitetsuppgifter*: de uppgifter som avses i artikel 27.3 a–e,

9. *fingeravtrycksuppgifter*: bilder av fingeravtryck och bilder av fingeravtrycksspår som på grund av sin unika karaktär och de referenspunkter som de innefattar möjliggör exakta och entydiga jämförelser för att fastställa en persons identitet,

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

10. *ansiktsbild*: digitala bilder av en persons ansikte,

11. *biometriska uppgifter*: fingeravtrycksuppgifter eller ansiktsbilder, eller båda,

12. *biometrisk mall*: en matematisk representation som erhålls genom särdragsextraktion från biometriska uppgifter och som är begränsad till de egenskaper som är nödvändiga för att utföra identifikationer och verifieringar,

13. *resehandling*: pass eller motsvarande handling som ger innehavaren rätt att passera de yttre gränserna och i vilken en visering kan föras in,

14. *resehandlingsuppgifter*: resehandlingens typ, nummer och utfärdandeland samt sista giltighetsdag och koden på tre bokstäver för det land som utfärdat resehandlingen,

15. *EU-informationssystem*: in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN,

16. *Europoluppgifter*: de personuppgifter som behandlas av Europol för det syfte som avses i artikel 18.2 a, b och c i förordning (EU) 2016/794,

17. *Interpols databaser*: Interpols databas över stulna och förkomna resehandlingar (SLTD-databasen) och Interpols databas för resehandlingar som är föremål för ett meddelande (TDAWN-databasen),

18. *träff*: förekomsten av en motsvarighet till följd av en automatisk jämförelse mellan personuppgifter som har registrerats eller håller på att registreras i ett informationssystem eller en databas,

19. *polismyndighet*: behörig myndighet enligt definitionen i artikel 3.7 i direktiv (EU) 2016/680,

20. *utsedda myndigheter*: medlemsstaternas utsedda myndigheter enligt definitionen i artikel 3.1.26 i Europaparlamentets och rådets förordning (EU) 2017/2226 ([30]), artikel 2.1 e i rådets beslut 2008/633/RIF ([31]) och artikel 3.1.21 i Europaparlamentets och rådets förordning (EU) 2018/1240 ([32]),

21. *terroristbrott*: ett brott enligt nationell rätt som motsvarar eller är likvärdigt med ett av de brott som avses i Europaparlamentets och rådets direktiv (EU) 2017/541 ([33]),

22. *grovt brott*: ett brott som motsvarar eller är likvärdigt med ett av de brott som avses i artikel 2.2 i rådets rambeslut 2002/584/RIF ([34]) om det enligt nationell rätt kan leda till fängelse eller annan frihetsberövande åtgärd under en maximal tidsperiod på minst tre år,

23. *in- och utresesystemet*: det in- och utresesystem som inrättats genom förordning (EU) 2017/2226,

24. *Informationssystemet för viseringar* eller *VIS*: det informationssystem för viseringar som inrättats genom Europaparlamentets och rådets förordning (EG) nr 767/2008 ([35]),

25. *EU-systemet för reseuppgifter och resetillstånd* eller *Etias*: det EU-system för reseuppgifter och resetillstånd som inrättats genom förordning (EU) 2018/1240,

---

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

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

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

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

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

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

26. *Eurodac*: Eurodac som inrättats genom Europaparlamentets och rådets förordning (EU) nr 603/2013 ([36]),

27. *Schengens informationssystem* eller *SIS*: Schengens informationssystem som inrättats genom Europaparlamentets och rådets förordning (EU) 2018/1860, (EU) 2018/1861 och (EU) 2018/1862,

28. *Ecris-TCN*: det centraliserade system för identifiering av medlemsstater som innehar uppgifter ur kriminalregister avseende tredjelandsmedborgare och statslösa personer som inrättats genom förordning (EU) 2019/816.

Artikel 5

Icke-diskriminering och grundläggande rättigheter

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

KAPITEL II

Den europeiska sökportalen

Artikel 6

Den europeiska sökportalen

1. En europeisk sökportal (ESP) ska inrättas för att underlätta medlemsstaternas myndigheters och unionsbyråernas möjligheter att få snabb, kontinuerlig, effektiv, systematisk och kontrollerad åtkomst till EU-informationssystemen, Europoluppgifter och Interpols databaser som krävs för att de ska kunna utföra sina uppgifter, i enlighet med sina åtkomsträttigheter och målen för och syftena med in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

2. ESP ska bestå av följande:

a) En central infrastruktur, inbegripet en sökportal som gör det möjligt att samtidigt söka i in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN samt i Europoluppgifter och Interpols databaser.

b) En säker kommunikationskanal mellan ESP, medlemsstaterna och de unionsbyråer som har rätt att använda sökportalen.

c) En säker kommunikationsinfrastruktur mellan ESP och in- och utresesystemet, VIS, Etias, Eurodac, centrala SIS, Ecris-TCN, Europoluppgifter och Interpols databaser samt mellan ESP och de centrala infrastrukturerna för CIR och MID.

3. eu-Lisa ska utveckla ESP och säkerställa dess tekniska förvaltning.

Artikel 7

Användning av den europeiska sökportalen

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

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

([36]) Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 180, 29.6.2013, s. 1).

2. De myndigheter i medlemsstaterna och de unionsbyråer som avses i punkt 1 ska använda ESP för att söka uppgifter om personer eller deras resehandlingar i Eurodacs och Ecris-TCN:s centrala system i enlighet med sina åtkomsträttigheter enligt de rättsliga instrument som reglerar dessa EU-informationssystem och nationell rätt. De ska också använda ESP för att söka i CIR i enlighet med sina åtkomsträttigheter enligt denna förordning för de syften som avses i artiklarna 20, 21 och 22.

3. De myndigheter i medlemsstaterna som avses i punkt 1 får använda ESP för att söka på uppgifter om personer eller deras resehandlingar i det centrala SIS som avses i förordningarna (EU) 2018/1860 och (EU) 2018/1861.

4. När så föreskrivs enligt unionsrätten ska de unionsbyråer som avses i punkt 1 använda ESP för att söka på uppgifter om personer eller deras resehandlingar i centrala SIS.

5. De myndigheter i medlemsstaterna och de unionsbyråer som avses i punkt 1 får använda ESP för att söka på uppgifter om personer eller deras resehandlingar i Europoluppgifter i enlighet med sina åtkomsträttigheter enligt unionsrätten och nationell rätt.

Artikel 8

Profiler för användarna av ESP

1. För att det ska vara möjligt att använda ESP ska eu-Lisa i samarbete med medlemsstaterna skapa en profil för varje kategori av ESP användare och på, det syfte som de har med sökningarna, i enlighet med de tekniska detaljer och åtkomsträttigheter som avses i punkt 2. Varje profil ska, i enlighet med unionsrätten och nationell rätt, inbegripa följande information:

a) De uppgiftsfält som ska användas vid sökningar.

b) De EU-informationssystem, Europoluppgifter och Interpols databaser som ska vara föremål för sökningar, de som kan vara föremål för sökningar och de som ska tillhandahålla användaren ett svar.

c) De specifika uppgifter i EU-informationssystemen, Europoluppgifterna och Interpols databaser som får vara föremål för sökningar.

d) De kategorier av uppgifter som får tillhandahållas i varje svar.

2. Kommissionen ska anta genomförandeakter för att närmare ange de tekniska detaljerna för de profiler som avses i punkt 1 ESP i enlighet med ESP-användarnas åtkomsträttigheter enligt de rättsliga instrument som reglerar EU-informationssystemen och nationell rätt. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

3. De profiler som avses i punkt 1 ska regelbundet ses över av eu-Lisa i samarbete med medlemsstaterna, minst en gång om året, och vid behov uppdateras.

Artikel 9

Sökningar

1. Användarna av ESP ska inleda en sökning genom att mata in alfanumeriska eller biometriska uppgifter i ESP. När en sökning har inletts ska ESP samtidigt söka i in- och utresesystemet, Etias, VIS, SIS, Eurodac, Ecris-TCN och CIR samt i Europoluppgifter och Interpols databaser med de uppgifter som användaren matat in och i enlighet med användarprofilen.

2. De kategorier av uppgifter som används för att inleda en sökning via ESP ska motsvara de kategorier av uppgifter i fråga om personer eller resehandlingar som kan användas för att söka i de olika EU-informationssystemen, Europoluppgifter och Interpols databaser i enlighet med de rättsliga instrument som reglerar dem.

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

4. När en sökning inleds av en ESP-användare ska in- och utresesystemet, Etias, VIS, SIS, Eurodac, Ecris-TCN, CIR och MID samt Europoluppgifter och Interpols databaser som svar på sökningen tillhandahålla uppgifter som de innehåller.

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

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

5. Alla sökningar i Interpols databaser genom ESP ska göras på ett sådant sätt att ingen information röjs för ägaren av Interpolregistreringen.

6. ESP ska så snart som uppgifter finns tillgängliga tillhandahålla användaren svar från något av EU-informationssystemen, Europoluppgifterna eller Interpols databaser. Dessa svar får endast innehålla de uppgifter som användaren har åtkomst till enligt unionsrätten och nationell rätt.

7. Kommissionen ska anta en genomförandeakt för att specificera det tekniska förfarandet för ESP:s sökningar i EU-informationssystemen, Europoluppgifterna och Interpols databaser och formatet för ESP:s svar. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 10

Registerföring av loggar

1. Utan att det påverkar tillämpningen av artiklarna 12 och 18 i förordning (EU) 2018/1862, artikel 29 i förordning (EU) 2019/816 och artikel 40 i förordning (EU) 2016/794, ska eu-Lisa föra logg över all uppgiftsbehandling i ESP. Dessa loggar ska innehålla följande:

a) Den medlemsstat eller unionsbyrå som inlett sökningen och den ESP-profil som används.

b) Datum och tidpunkt för sökningen.

c) De EU-informationssystem och Europoluppgifter som varit föremål för sökning.

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

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

Artikel 11

Reservförfaranden om det är tekniskt omöjligt att använda den europeiska sökportalen

1. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera av de EU-informationssystem eller i CIR, på grund av ett fel i ESP, ska ESP:s användare automatiskt underrättas av eu-Lisa.

2. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera EU-informationssystem eller i CIR, på grund av ett fel i en medlemsstats nationella infrastruktur, ska den medlemsstaten automatiskt underrätta eu-Lisa och kommissionen.

3. I de fall som avses i punkterna 1 och 2 i denna artikel och till dess att det tekniska felet har åtgärdats ska den skyldighet som avses i artikel 7.2 och 7.4 inte tillämpas och medlemsstaterna ska ha åtkomst till EU-informationssystem eller till CIR direkt när så krävs enligt unionsrätten eller nationell rätt.

4. Om det är tekniskt omöjligt att använda ESP för att söka i ett eller flera EU-informationssystem eller i CIR, på grund av ett fel i en unionsbyrås infrastruktur, ska den byrån automatiskt underrätta eu-Lisa och kommissionen.

KAPITEL III

En gemensam biometrisk matchningstjänst

Artikel 12

En gemensam biometrisk matchningstjänst

1. Det ska inrättas en gemensam biometrisk matchningstjänst för lagring av biometriska mallar som erhållits från de biometriska uppgifter som avses i artikel 13, vilka är lagrade i CIR och SIS, och för möjliggörande av sökningar med biometriska uppgifter i flera EU-informationssystem för att stödja CIR och MID och målen för in- och utresesystemet, VIS, Eurodac, SIS och Ecris-TCN.

2. Den gemensamma biometriska matchningstjänsten ska bestå av följande:

a) En central infrastruktur som ska ersätta de centrala systemen för in- och utresesystemet, VIS, SIS, Eurodac respektive Ecris-TCN i den mån den ska lagra biometriska mallar och möjliggöra sökning med biometriska uppgifter.

b) En säker kommunikationsinfrastruktur mellan den gemensamma biometriska matchningstjänsten, centrala SIS och CIR.

3. eu-Lisa ska utveckla den gemensamma biometriska matchningstjänsten och säkerställa den tekniska förvaltningen.

Artikel 13

Lagring av biometriska mallar i den gemensamma biometriska matchningstjänsten

1. Den gemensamma biometriska matchningstjänsten ska lagra de biometriska mallar som den ska få från följande biometriska uppgifter:

a) de uppgifter som avses i artikel 20.3 w och y i förordning (EU) 2018/1862, med undantag för uppgifter om handavtryck.

b) de uppgifter som avses i artikel 5.1 b och 5.2 i förordning (EU) 2019/816.

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

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

3. Biometriska mallar ska registreras i den gemensamma biometriska matchningstjänsten endast efter en automatisk kvalitetskontroll av de biometriska uppgifter som läggs in i ett av EU-informationssystemen, vilken utförs av den gemensamma biometriska matchningstjänsten för att säkerställa att en minimistandard för uppgifternas kvalitet uppfylls.

4. Lagringen av de uppgifter som avses i punkt 1 ska uppfylla de kvalitetsstandarder som avses i artikel 37.2.

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

Artikel 14

Sökning på biometriska uppgifter med den gemensamma biometriska matchningstjänsten

För att söka på de biometriska uppgifter som lagrats i CIR och SIS ska CIR och SIS använda de biometriska mallar som lagrats i den gemensamma biometriska matchningstjänsten. Sökningar med biometriska uppgifter ska äga rum i enlighet med de syften som anges i denna förordning och i förordningarna (EG) nr 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 och (EU) 2019/816.

Artikel 15

Lagring av uppgifter i den gemensamma biometriska matchningstjänsten

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

Artikel 16

Registerföring av loggar

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

a) Den medlemsstat eller unionsbyrå som inlett sökningen.

b) Historiken för skapandet och lagringen av biometriska mallar.

c) De EU-informationssystem som varit föremål för sökning med de biometriska mallar som lagrats i den gemensamma biometriska matchningstjänsten.

d) Datum och tidpunkt för sökningen.

e) Den typ av biometriska uppgifter som används för att inleda sökningen.

f) Resultaten av sökningen och datum och tidpunkt för resultatet.

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

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

KAPITEL IV

En gemensam databas för identitetsuppgifter

Artikel 17

En gemensam databas för identitetsuppgifter

1. Det ska inrättas en gemensam databas för identitetsuppgifter (CIR), varigenom det skapas en personakt för varje person som är registrerad i in- och utresesystemet, VIS, Etias, Eurodac eller Ecris-TCN och som innehåller de uppgifter som avses i artikel 18, för att underlätta och bistå vid en korrekt identifiering av personer som är registrerade i in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN i enlighet med artikel 20, stödja funktionen av MID i enlighet med artikel 21 och underlätta och rationalisera de utsedda myndigheternas och Europols åtkomst till in- och utresesystemet, VIS, Etias och Eurodac, om det är nödvändigt för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott i enlighet med artikel 22.

2. CIR ska bestå av följande:

a) En central infrastruktur som ska ersätta de centrala systemen för in- och utresesystemet, VIS, Etias, Eurodac respektive Ecris-TCN i den mån den ska lagra de uppgifter som avses i artikel 18.

b) En säker kommunikationskanal mellan CIR, medlemsstaterna och de unionsbyråer som har rätt att använda CIR i enlighet med unionsrätten och nationell rätt.

c) En säker kommunikationsinfrastruktur mellan CIR och in- och utresesystemet, VIS, Etias, Eurodac och Ecris-TCN samt de centrala infrastrukturerna för ESP, den gemensamma biometriska matchningstjänsten och MID.

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

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

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

Artikel 18

Uppgifter i den gemensamma databasen för identitetsuppgifter

1. CIR ska lagra följande uppgifter, logiskt åtskilda enligt det informationssystem från vilket uppgifterna härrör: De uppgifter som avses i artikel 5.1 b och 5.2 och följande uppgifter i artikel 5.1 a i förordning (EU) 2019/816: efternamn, förnamn, födelsedatum, födelseort (ort och land), medborgarskap (ett eller flera), kön, tidigare namn, i förekommande fall, pseudonymer eller alias samt, i förekommande fall, information om resehandlingar.

2. För varje uppsättning uppgifter som avses i punkt 1 ska CIR innehålla en hänvisning till de EU-informationssystem som uppgifterna tillhör.

3. De myndigheter som har åtkomst till CIR ska handla i enlighet med sina åtkomsträttigheter enligt de rättsliga instrument som reglerar EU-informationssystemen och enligt nationell rätt och i enlighet med sina åtkomsträttigheter enligt denna förordning för de syften som avses i artiklarna 20, 21 och 22.

4. För varje uppsättning uppgifter som avses i punkt 1 ska CIR innehålla en hänvisning till den konkreta post i EU-informationssystemen som uppgifterna tillhör.

5. Lagringen av de uppgifter som avses i punkt 1 ska uppfylla de kvalitetsstandarder som avses i artikel 37.2.

Artikel 19

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

1. Om uppgifter läggs till, ändras eller raderas i Eurodac eller Ecris-TCN ska de uppgifter som avses i artikel 18 vilka lagras i personakten i CIR automatiskt läggas till, ändras eller raderas.

2. Om en vit eller en röd länk skapas i MID i enlighet med artikel 32 eller 33 mellan uppgifter i två eller flera av EU-informationssystemen som utgör CIR, ska CIR i stället för att skapa en ny personakt lägga till de nya uppgifterna i den personakt som innehåller de länkade uppgifterna.

Artikel 20

Åtkomst till den gemensamma databasen för identitetsuppgifter i identifieringssyfte

1. Sökningar i CIR får utföras av en polismyndighet i enlighet med punkterna 2 och 5 endast under följande omständigheter:

a) Om en polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet.

b) Om det föreligger tvivel om de identitetsuppgifter som lämnats av en person.

c) Om det föreligger tvivel om äktheten i den resehandling eller en annan trovärdig handling som lämnats av en person.

d) Om det föreligger tvivel om identiteten på innehavaren av en resehandling eller en annan trovärdig handling.

e) Om en person inte kan eller vägrar att samarbeta.

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

2. Om någon av de omständigheter som förtecknas i punkt 1 uppstår och en polismyndighet har bemyndigats genom de nationella lagstiftningsåtgärder som avses i punkt 5, får myndigheten, endast i syfte att identifiera en person, söka i CIR med den personens biometriska uppgifter som tagits direkt under en identitetskontroll, förutsatt att förfarandet inletts i den berörda personens närvaro.

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

Om personens biometriska uppgifter inte kan användas eller om sökningen med dessa uppgifter misslyckas, ska sökningen utföras med vederbörandes identitetsuppgifter i kombination med resehandlingsuppgifter eller med de identitetsuppgifter som tillhandahållits av personen.

4. Om en polismyndighet har bemyndigats genom de nationella lagstiftningsåtgärder som avses i punkt 6, får den, i händelse av en naturkatastrof, en olycka eller ett terrordåd och endast i syfte att identifiera okända personer som inte kan identifiera sig eller oidentifierade mänskliga kvarlevor, söka i CIR med dessa personers biometriska uppgifter.

5. Medlemsstater som vill utnyttja den möjlighet som anges i punkt 2 ska anta nationella lagstiftningsåtgärder. När medlemsstaterna gör detta ska de ta hänsyn till att ingen diskriminering av tredjelandsmedborgare får förekomma. I sådana lagstiftningsåtgärder ska de exakta syftena med identifieringen anges inom ramen för de mål som avses i artikel 2.1 b och c. De behöriga polismyndigheterna ska utses, och förfaranden, villkor och kriterier för sådana kontroller ska fastställas i dessa lagstiftningsåtgärder.

6. Medlemsstater som vill utnyttja den möjlighet som anges i punkt 4 ska anta nationella lagstiftningsåtgärder som fastställer förfarandena, villkoren och kriterierna.

Artikel 21

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

1. Om en sökning i CIR resulterar i en gul länk i enlighet med artikel 28.4, ska den myndighet som ansvarar för den manuella verifieringen av olika identiteter i enlighet med artikel 29 enbart i verifieringssyfte ha åtkomst till de uppgifter som avses i artikel 18.1 och 18.2, som lagrats i CIR och som är kopplade genom en gul länk.

2. Om en sökning i CIR ger upphov till en röd länk i enlighet med artikel 32, ska de myndigheter som avses i artikel 26.2 enbart i syfte att bekämpa identitetsbedrägerier ha åtkomst till de uppgifter som avses i artikel 18.1 och 18.2, som lagrats i CIR och som är kopplade genom en röd länk.

Artikel 22

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

1. Om det i ett specifikt fall finns rimliga skäl att anta att en sökning i EU-informationssystem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, särskilt om det finns misstankar om att en person som misstänks för, har begått eller utsatts för ett terroristbrott eller ett annat grovt brott är en person vars uppgifter lagras i Eurodac, får de utsedda myndigheterna och Europol söka i CIR för att få information om huruvida det finns uppgifter om en viss person i Eurodac.

2. Om ett svar på en sökning i CIR visar att det finns uppgifter om den personen i Eurodac ska CIR tillhandahålla de utsedda myndigheterna och Europol ett svar i form av en hänvisning som avses i artikel 18.2 som anger att Eurodac innehåller motsvarande uppgifter. CIR ska svara på ett sådant sätt att uppgifternas säkerhet inte äventyras.

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

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

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

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

Artikel 23

Lagring av uppgifter i den gemensamma databasen för identitetsuppgifter

1. De uppgifter som avses i artikel 18.1, 18.2 och 18.4 ska automatiskt raderas från CIR i enlighet med bestämmelserna om lagring av uppgifter i förordning (EU) 2019/816.

2. Personakten ska lagras i CIR endast så länge de motsvarande uppgifterna lagras i minst ett av de EU-informationssystem vars uppgifter finns i CIR. Skapandet av en länk ska inte påverka lagringsperioden för varje post av de länkade uppgifterna.

Artikel 24

Registerföring av loggar

1. Utan att det påverkar tillämpningen av artikel 29 i förordning (EU) 2019/816 ska eu-Lisa föra logg över all uppgiftsbehandling i CIR i enlighet med punkterna 2, 3 och 4 i den här artikeln.

2. eu-Lisa ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 20 i CIR. Dessa loggar ska omfatta följande:

a) Den medlemsstat eller den unionsbyrå som inlett sökningen.

b) Syftet med användarens åtkomst för att söka via CIR.

c) Datum och tidpunkt för sökningen.

d) Den typ av uppgifter som används för att inleda sökningen.

e) Sökningens resultat.

3. eu-Lisa ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 21 i CIR. Dessa loggar ska omfatta följande:

a) Den medlemsstat eller den unionsbyrå som inlett sökningen.

a) Syftet med användarens åtkomst för att söka via CIR.

b) Datum och tidpunkt för sökningen.

c) I fall där en länk skapas, de uppgifter som används för att inleda sökningen, och sökningens resultat med angivelse av det EU-informationssystem som uppgifterna erhållits från.

4. eu-Lisa ska föra logg över all uppgiftsbehandling som sker i enlighet med artikel 22 i CIR. Dessa loggar ska omfatta följande:

a) Datum och tidpunkt för sökningen.

b) De uppgifter som används för att inleda sökningen.

c) Sökningens resultat.

d) Den medlemsstat eller den unionsbyrå som söker i CIR.

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

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

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

a) Referensnummer för den nationella akten.

b) Syftet med åtkomsten.

c) I enlighet med nationella regler, den unika användaridentitet som anger vilken tjänsteman som utförde sökningen och vilken tjänsteman som beordrade sökningen.

6. I enlighet med förordning (EU) 2016/794 ska Europol för all åtkomst till CIR i enlighet med artikel 22 i den här förordningen föra logg över den unika användaridentitet som anger vilken tjänsteman som utförde sökningen och vilken tjänsteman som beordrade sökningen.

7. De loggar som avses i punkterna 2–6 får endast användas för övervakning av dataskyddet, inbegripet för kontroll av om en sökning är tillåten och om uppgifter har behandlats på ett lagligt sätt samt för att säkerställa datasäkerhet och dataintegritet. Dessa loggar ska på lämpligt sätt skyddas mot obehörig åtkomst och ska raderas ett år efter det att de skapats. För det fall de behövs för övervakningsförfaranden som redan har inletts, ska de emellertid raderas så snart loggarna i fråga inte längre behövs för övervakningsförfarandena.

8. eu-Lisa ska lagra loggarna över historiken avseende uppgifterna s i personakterna. eu-Lisa ska automatiskt radera sådana loggar så snart uppgifterna har raderats.

KAPITEL V

Detektorn för multipla identiteter

Artikel 25

Detektorn för multipla identiteter

1. Det ska inrättas en detektor för multipla identiteter (MID) som skapar och lagrar akter med identitetsbekräftelse som avses i artikel 34, som innehåller länkar mellan uppgifter i de EU-informationssystem som ingår i CIR och SIS och som gör det möjligt att spåra multipla identiteter, med det dubbla syftet att underlätta identitetskontroller och bekämpa identitetsbedrägerier, för att stödja CIR:s funktion och målen för in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN.

2. MID ska bestå av följande:

a) En central infrastruktur som lagrar länkar och hänvisningar till EU-informationssystem.

b) En säker kommunikationsinfrastruktur som kopplar MID till SIS och ESP:s och CIR:s centrala infrastrukturer.

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

Artikel 26

Åtkomst till detektorn för multipla identiteter

1. För den manuella verifiering av olika identiteter som avses i artikel 29 ska åtkomst till de uppgifter som avses i artikel 34 och som är lagrade i MID beviljas

a) Sirenekontoret i den medlemsstat som skapar eller uppdaterar en registrering i enlighet med förordning (EU) 2018/1862,

b) de centrala myndigheterna i den dömande medlemsstaten vid registrering eller ändring av uppgifter i Ecris-TCN i enlighet med artikel 5 eller 9 i förordning (EU) 2019/816.

2. De myndigheter i medlemsstaterna och de unionsbyråer som har åtkomst till minst ett av de EU-informationssystem som ingår i CIR eller till SIS ska ha åtkomst till de uppgifter som avses i artikel 34 a och b vad gäller samtliga röda länkar som avses i artikel 32.

3. Myndigheterna i medlemsstaterna och unionsbyråerna ska ha åtkomst till de vita länkar som avses i artikel 33 om de har åtkomst till de två EU-informationssystem som innehåller uppgifter mellan vilka den vita länken skapats.

4. Myndigheterna i medlemsstaterna och unionsbyråerna ska ha åtkomst till de gröna länkar som avses i artikel 31 om de har åtkomst till de två EU-informationssystem som innehåller uppgifter mellan vilka den gröna länken skapats och en sökning i dessa informationssystem gett en träff med de två uppsättningarna länkade uppgifter.

Artikel 27

Spårning av multipla identiteter

1. Spårning av multipla identiteter ska i följande fall inledas i CIR och i SIS:

a) En registrering om en person skapas eller uppdateras i SIS i enlighet med kapitlen VI–IX i förordning (EU) 2018/1862.

b) En datapost skapas eller ändras i Ecris-TCN i enlighet med artikel 5 eller 9 i förordning (EU) 2019/816.

2. Om de uppgifter i ett EU-informationssystem som avses i punkt 1 innehåller biometriska uppgifter ska CIR och centrala SIS använda den gemensamma biometriska matchningstjänsten för att utföra en spårning av multipla identiteter. Den gemensamma biometriska matchningstjänsten ska jämföra de biometriska mallar som erhållits från nya biometriska uppgifter med de biometriska mallar som redan finns i den gemensamma biometriska matchningstjänsten i syfte att verifiera huruvida uppgifter som tillhör samma person redan finns lagrade i CIR eller i centrala SIS.

3. Utöver det förfarande som avses i punkt 2 ska CIR och centrala SIS använda ESP för att söka i uppgifter som lagrats i centrala SIS respektive CIR med hjälp av följande uppgifter:

a) Efternamn, förnamn, namn vid födelsen, tidigare använda namn och alias, födelseort, födelsedatum, kön och samtliga medborgarskap enligt artikel 20.3 i förordning (EU) 2018/1862.

b) Efternamn, förnamn, födelsedatum, födelseort (ort och land), medborgarskap (ett eller flera) och kön enligt artikel 5.1 a i förordning (EU) 2019/816.

4. Utöver det förfarande som avses i punkterna 2 och 3 ska CIR och centrala SIS använda ESP för att söka i uppgifter som lagrats i centrala SIS respektive CIR med hjälp av resehandlingsuppgifter.

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

Artikel 28

Resultat av en spårning av multipla identiteter

1. Om de sökningar som avses i artikel 27.2, 27.3 och 27.4 inte ger någon träff ska de förfaranden som avses i artikel 27.1 fortsätta i enlighet med respektive de rättsliga instrument genom vilka de regleras.

2. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 ger en eller flera träffar ska CIR och, i förekommande fall, SIS skapa en länk mellan de uppgifter som används för att inleda sökningen och de uppgifter som gett upphov till träffen.

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

3. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är desamma eller liknande, ska en vit länk skapas i enlighet med artikel 33.

4. Om den sökning som avses i artikel 27.2, 27.3 och 27.4 ger en eller flera träffar och identitetsuppgifterna i de länkade akterna inte kan anses vara liknande, ska en gul länk skapas i enlighet med artikel 30 och det förfarande som avses i artikel 29 ska tillämpas.

5. Kommissionen ska anta delegerade akter i enlighet med artikel 69 för att fastställa förfarandena för att avgöra ärenden där identitetsuppgifter kan anses vara desamma eller liknande.

6. Länkarna ska lagras i den akt med identitetsbekräftelse som avses i artikel 34.

7. Kommissionen ska, i samarbete med eu-Lisa, fastställa de tekniska reglerna för att skapa länkar mellan uppgifter från olika EU-informationssystem genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 29

Manuell verifiering av olika identiteter och ansvariga myndigheter

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

a) Sirenekontoret i medlemsstaten för träffar som uppstår när en registrering i SIS skapas eller uppdateras i enlighet med förordning (EU) 2018/1862.

b) De centrala myndigheterna i den dömande medlemsstaten för träffar som uppstår vid registrering eller ändring av uppgifter i Ecris-TCN i enlighet med artikel 5 eller 9 i förordning (EU) 2019/816.

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

2. Den myndighet som ansvarar för den manuella verifieringen av olika identiteter i akten med identitetsbekräftelse ska vara Sirenekontoret i den medlemsstat som skapade registreringen om det skapas en länk till uppgifterna i en registrering om

a) personer som är efterlysta för att gripas och överlämnas eller för att utlämnas enligt artikel 26 i förordning (EU) 2018/1862,

b) försvunna eller sårbara personer enligt artikel 32 i förordning (EU) 2018/1862,

c) personer som söks för att delta i ett rättsligt förfarande enligt artikel 34 i förordning (EU) 2018/1862,

d) personer för diskreta kontroller, undersökningskontroller eller särskilda kontroller enligt artikel 36 i förordning (EU) 2018/1862.

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

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

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

Artikel 30

Gul länk

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

a) De länkade uppgifterna innehåller samma biometriska uppgifter men har liknande eller olika identitetsuppgifter.

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

c) De länkade uppgifterna innehåller samma identitetsuppgifter men har olika biometriska uppgifter.

d) De länkade uppgifterna har liknande eller olika identitetsuppgifter, och innehåller samma resehandlingsuppgifter men har olika biometriska uppgifter.

2. Om en länk klassificeras som gul i enlighet med punkt 1 ska förfarandet i artikel 29 tillämpas.

Artikel 31

Grön länk

1. En länk mellan uppgifter från två eller flera EU-informationssystem ska klassificeras som grön om

a) de länkade uppgifterna har olika biometriska uppgifter men innehåller samma identitetsuppgifter och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer,

b) de länkade uppgifterna har olika biometriska uppgifter, har liknande eller olika identitetsuppgifter, innehåller samma resehandlingsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer,

c) de länkade uppgifterna har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter, minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer.

2. Om en sökning görs i CIR eller SIS och om det finns en grön länk mellan två eller fler av EU-informationssystemen, ska MID ange att identitetsuppgifterna i de länkade uppgifterna inte gäller samma person.

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

Artikel 32

Röd länk

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

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

b) De länkade uppgifterna har samma, liknande eller olika identitetsuppgifter och har samma resehandlingsuppgifter men olika biometriska uppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer, av vilka åtminstone en person använder en och samma resehandling på ett oberättigat sätt.

c) De länkade uppgifterna innehåller samma identitetsuppgifter men har olika biometriska uppgifter och olika eller inga resehandlingsuppgifter, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till två olika personer på ett oberättigat sätt.

d) De länkade uppgifterna har olika identitetsuppgifter men innehåller samma resehandlingsuppgifter, minst ett av EU-informationssystemen saknar biometriska uppgifter om den berörda personen, och den myndighet som ansvarar för den manuella verifieringen av olika identiteter har konstaterat att de länkade uppgifterna hänvisar till en och samma person på ett oberättigat sätt.

2. Om CIR eller SIS är föremål för sökning och om det finns en röd länk mellan uppgifter i två eller fler av EU-informationssystemen, ska MID ange de uppgifter som avses i artikel 34. En uppföljning av en röd länk ska ske i enlighet med unionsrätten och nationell rätt, och eventuella rättsliga följder för den berörda personen ska bygga uteslutande på de relevanta uppgifterna om personen i fråga. Inga rättsliga följder för den berörda personen ska uppstå enbart till följd av att det finns en röd länk.

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

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

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

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

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

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

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

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

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

Artikel 33

Vit länk

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

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

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

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

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

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

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

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

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

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

Artikel 34

Akt med identitetsbekräftelse

Akten med identitetsbekräftelse ska innehålla följande uppgifter:

a) De länkar som avses i artiklarna 30–33.

b) En hänvisning till de EU-informationssystem i vilka de länkade uppgifterna finns.

c) Ett enda identifikationsnummer som gör det möjligt att hämta de länkade uppgifterna från de motsvarande EU-informationssystemen.

d) Den myndighet som ansvarar för den manuella av olika identiteter.

e) Datum för skapande av länken eller uppdatering därav.

Artikel 35

Lagring av uppgifter i detektorn för multipla identiteter

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

Artikel 36

Registerföring av loggar

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

a) Den medlemsstat som inlett sökningen.

b) Syftet med användarens åtkomst.

c) Datum och tidpunkt för sökningen.

d) Den typ av uppgifter som används för att inleda sökningen.

e) Hänvisning till de länkade uppgifterna.

f) Historik tillhörande akten med identitetsbekräftelse.

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

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

KAPITEL VI

Åtgärder till stöd för interoperabilitet

Artikel 37

Uppgifternas kvalitet

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

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

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

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

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

5. Ett år efter inrättandet av de automatiska mekanismerna och förfarandena för kontroll av uppgifternas kvalitet, de gemensamma indikatorerna för uppgifternas kvalitet samt minimikvalitetsstandarderna för uppgifter, och varje år därefter, ska kommissionen utvärdera medlemsstaternas genomförande av uppgifters kvalitet och lämna nödvändiga rekommendationer. Medlemsstaterna ska förse kommissionen med en handlingsplan för att avhjälpa de brister som konstaterats i utvärderingsrapporten och, i synnerhet, problem med uppgiftskvalitet vilka härrör från felaktiga uppgifter i EU-informationssystem. Medlemsstaterna ska regelbundet rapportera till kommissionen om vilka framsteg som har gjorts med denna handlingsplan till dess att den genomförts fullt ut.

Kommissionen ska överlämna utvärderingsrapporten till Europaparlamentet, rådet, Europeiska datatillsynsmannen, Europeiska dataskyddsstyrelsen och Europeiska unionens byrå för grundläggande rättigheter, som inrättades genom rådets förordning (EG) nr 168/2007 ([37]).

Artikel 38

Universellt meddelandeformat

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

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

2. UMF-standarden ska användas vid utvecklingen av Eurodac, Ecris-TCN, ESP, CIR, MID och, när så är lämpligt, eu-Lisas eller andra unionsbyråers utveckling av nya modeller för informationsutbyte och informationssystem på området rättsliga och inrikes frågor.

3. Kommissionen ska anta en genomförandeakt för att fastställa och utveckla den UMF-standard som avses i punkt 1 i denna artikel. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 39

Den centrala databasen för rapporter och statistik

1. Det ska inrättas en central databas för rapporter och statistik (CRRS) för att stödja målen för SIS, Eurodac och Ecris-TCN, i enlighet med de respektive rättsliga instrument som reglerar de systemen, och för att tillhandahålla systemöverskridande statistiska uppgifter och analysrapporter för politiska och operativa syften samt för uppgiftskvaliteten.

2. eu-Lisa ska inrätta, implementera och hysa i sina tekniska anläggningar CRRS som innehåller de uppgifter och den statistik som avses i artikel 74 i förordning (EU) 2018/1862 och artikel 32 i förordning (EU) 2019/816, logiskt åtskilda per EU-informationssystem. Åtkomst till CRRS ska beviljas via kontrollerad, säkrad åtkomst och specifika användarprofiler enbart för rapportering och statistik, till de myndigheter som avses i artikel 74 i förordning (EU) 2018/1862 och artikel 32 i förordning (EU) 2019/816

3. eu-Lisa ska anonymisera uppgifterna och registrera de anonymiserade uppgifterna i CRRS. Förfarandet för att anonymisera uppgifterna ska vara automatiskt.

Uppgifterna i CRRS ska inte möjliggöra identifiering av enskilda personer.

4. CRRS ska bestå av följande:

a) De verktyg som är nödvändiga för anonymisering av uppgifter.

b) En central infrastruktur som består av en databas med anonymiserade uppgifter.

c) En säker kommunikationsinfrastruktur för att ansluta CRRS till SIS, Eurodac och Ecris-TCN samt de centrala infrastrukturerna för den gemensamma biometriska matchningstjänsten, CIR och MID.

5. Kommissionen ska anta en delegerad akt i enlighet med artikel 69 för att fastställa detaljerade bestämmelser om driften av CRRS, inbegripet särskilda skyddsåtgärder för behandlingen av personuppgifter enligt punkterna 2 och 3 i den här artikeln och de säkerhetsregler som är tillämpliga på databasen.

KAPITEL VII

Dataskydd

Artikel 40

Personuppgiftsansvarig

1. När det gäller behandling av uppgifter i den gemensamma biometriska matchningstjänsten ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för Eurodac, SIS respektive Ecris-TCN vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 avseende de biometriska mallar som erhållits från de uppgifter som avses i artikel 13 i den här förordningen och som de för in i de underliggande systemen och ska ansvara för behandlingen av de biometriska mallarna i den gemensamma biometriska matchningstjänsten.

2. När det gäller behandling av uppgifter i CIR ska de av medlemsstaternas myndigheter som är personuppgiftsansvariga för Eurodac respektive Ecris-TCN vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 avseende de uppgifter som avses i artikel 18 i den här förordningen och som de för in i de underliggande systemen och ska ansvara för behandlingen av de personuppgifterna i CIR.

3. När det gäller behandling av uppgifter i MID gäller följande:

a) Europeiska gräns- och kustbevakningsbyrån ska vara personuppgiftsansvarig i den mening som avses i artikel 3.8 i förordning (EU) 2018/1725 när det gäller den behandling av personuppgifter som utförs av Etias centralenhet.

b) De av medlemsstaternas myndigheter som lägger till eller ändrar uppgifter i akten med identitetsbekräftelse ska vara personuppgiftsansvariga i enlighet med artikel 4.7 i förordning (EU) 2016/679 eller artikel 3.8 i direktiv (EU) 2016/680 och ska ansvara för behandlingen av personuppgifter i MID.

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

Artikel 41

Personuppgiftsbiträde

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

Artikel 42

Säkerhet vid behandling

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

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

3. eu-Lisa ska i synnerhet vidta nödvändiga åtgärder, inbegripet en säkerhetsplan, en kontinuitetsplan och en katastrofplan, i syfte att

a) fysiskt skydda uppgifter, bland annat genom att utarbeta beredskapsplaner för skydd av kritisk infrastruktur,

b) hindra obehöriga från åtkomst till utrustning eller anläggningar för uppgiftsbehandling,

c) förhindra obehörig läsning, kopiering, ändring eller obehörigt avlägsnande av datamedier,

d) hindra obehörigt inmatning av uppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter,

e) förhindra obehörig behandling av uppgifter och obehörig kopiering, ändring eller radering av uppgifter,

f) hindra obehöriga från att med hjälp av datakommunikationsutrustning använda automatiserade system för uppgiftsbehandling,

g) säkerställa att personer som har åtkomstbehörighet till interoperabilitetskomponenterna har åtkomst endast till de uppgifter för vilka de är behöriga och endast genom individuella användaridentiteter och skyddade åtkomstmetoder,

h) säkerställa att det finns möjlighet att kontrollera och fastställa till vilka organ personuppgifter får överföras med hjälp av datakommunikationsutrustning,

i) säkerställa att det finns möjlighet att kontrollera och fastställa vilka uppgifter som har behandlats i interoperabilitetskomponenterna, när detta har gjorts, av vem och i vilket syfte,

j) hindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av personuppgifter till eller från interoperabilitetskomponenterna eller under transport av datamedier, särskilt med hjälp av lämplig krypteringsteknik,

k) säkerställa att installerade system i händelse av driftavbrott kan återställas till normal drift,

l) säkerställa driftsäkerhet genom att se till att eventuella driftfel hos interoperabilitetskomponenterna rapporteras på korrekt sätt,

m) övervaka att de säkerhetsåtgärder som avses i denna punkt är verksamma och vidta nödvändiga organisatoriska åtgärder i fråga om intern övervakning för att säkerställa att denna förordning efterlevs och för att bedöma dessa säkerhetsåtgärder mot bakgrund av utvecklingen av ny teknik.

4. Medlemsstaterna, Europol och Etias centralenhet ska vidta åtgärder som är likvärdiga med de som avses i punkt 3 vad gäller säkerheten vid behandling av personuppgifter som utförs av de myndigheter som har rätt till åtkomst till någon av interoperabilitetskomponenterna.

Artikel 43

Säkerhetstillbud

1. Alla händelser som har eller kan ha inverkan på interoperabilitetskomponenternas säkerhet och som kan orsaka skada på eller förlust av uppgifter lagrade i dem ska betraktas som säkerhetstillbud, särskilt om obehörig åtkomst till uppgifter kan ha inträffat eller om uppgifters tillgänglighet, integritet och konfidentialitet har äventyrats eller kan ha äventyrats.

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

3. Utan att det påverkar anmälan av och information om personuppgiftsincidenter i enlighet med artikel 33 i förordning (EU) 2016/679, artikel 30 i direktiv (EU) 2016/680, eller båda, ska medlemsstaterna utan dröjsmål underrätta kommissionen, eu-Lisa, de behöriga tillsynsmyndigheterna och Europeiska datatillsynsmannen om alla säkerhetstillbud.

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

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

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

5. De berörda medlemsstaterna, Etias centralenhet, Europol och eu-Lisa ska samarbeta om ett säkerhetstillbud inträffar. Kommissionen ska fastställa specifikationer för detta samarbete genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 70.2.

Artikel 44

Egenkontroll

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

De personuppgiftsansvariga som avses i artikel 40 ska vidta nödvändiga åtgärder för att övervaka att uppgiftsbehandlingen sker i enlighet med denna förordning, inklusive genom frekventa kontroller av de loggar som avses i artiklarna 10, 16, 24 och 36, och vid behov samarbeta med tillsynsmyndigheterna och med Europeiska datatillsynsmannen.

Artikel 45

Sanktioner

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

Artikel 46

Skadeståndsansvar

1. Utan att det påverkar rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet, eller dessas skadeståndsansvar i enlighet med förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EU) 2018/1725, ska följande gälla:

a) Varje person eller medlemsstat som har lidit materiell eller immateriell skada till följd av en otillåten behandling av personuppgifter eller av någon annan åtgärd från en medlemsstats sida som är oförenlig med denna förordning ska ha rätt till ersättning från den berörda medlemsstaten.

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

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

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

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

Artikel 47

Rätt till information

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

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

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

Artikel 48

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

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

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

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

4. Om en begäran om rättelse eller radering av personuppgifter ställs till en medlemsstat där Etias centralenhet ansvarade för den manuella verifieringen av olika identiteter, ska den medlemsstat till vilken begäran ställdes kontakta Etias centralenhet inom sju dagar och begära att den avger ett yttrande. Etias centralenhet ska avge sitt yttrande utan otillbörligt dröjsmål, dock senast inom 30 dagar efter det att den kontaktades. Denna period får vid behov förlängas med ytterligare 15 dagar, med beaktande av hur komplicerade och hur många begärandena är. Den berörda personen ska informeras om det fortsatta förfarandet av den medlemsstat som kontaktade Etias centralenhet.

5. Om det, efter en prövning, visar sig att de uppgifter som lagrades i MID är oriktiga eller har registrerats på ett olagligt sätt, ska den medlemsstat som ansvarade för den manuella verifieringen av olika identiteter eller – om det inte fanns någon medlemsstat som ansvarade för den manuella verifieringen av olika identiteter eller om Etias centralenhet ansvarade för den manuella verifieringen av olika identiteter – den medlemsstat till vilken begäran har ställts utan otillbörligt dröjsmål rätta eller radera dessa uppgifter. Den berörda personen ska informeras skriftligen om att hans eller hennes uppgifter har rättats eller raderats.

6. Om uppgifter som lagras i MID ändras av en medlemsstat under lagringsperioden, ska den medlemsstaten utföra den behandling som avses i artikel 27 och, i förekommande fall, artikel 29 för att avgöra huruvida de ändrade uppgifterna ska länkas. Om behandlingen inte ger någon träff ska den medlemsstaten radera uppgifterna från akten med identitetsbekräftelse. Om den automatiska behandlingen ger en eller flera träffar ska den medlemsstaten skapa eller uppdatera den relevanta länken i enlighet med de relevanta bestämmelserna i denna förordning.

7. Om den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts inte instämmer i att uppgifter som lagras i MID är oriktiga eller har registrerats på ett olagligt sätt, ska den medlemsstaten utan dröjsmål anta ett administrativt beslut med en skriftlig förklaring till den berörda personen om varför den inte är beredd att rätta eller radera uppgifter som rör honom eller henne.

8. Det beslut som avses i punkt 7 ska även ge den berörda personen information om möjligheten att invända mot det beslut som fattats med avseende på begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter och, i tillämpliga fall, information om hur talan kan väckas vid eller klagomål inges till behöriga myndigheter eller domstolar samt möjligheterna till bistånd, även från tillsynsmyndigheterna.

9. En begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter ska innehålla den information som behövs för att den berörda personen ska kunna identifieras. Denna information ska användas uteslutande för att de rättigheter som avses i denna artikel ska kunna utövas och ska sedan omedelbart raderas.

10. Den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter eller, i tillämpliga fall, den medlemsstat till vilken begäran har ställts ska spara skriftlig dokumentation av att en begäran om åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter har gjorts och hur den behandlats, och ska utan dröjsmål tillhandahålla tillsynsmyndigheterna denna dokumentation.

11. Denna artikel påverkar inte begränsningar och inskränkningar av de rättigheter som anges i denna artikel i enlighet med förordning (EU) 2016/679 och direktiv (EU) 2016/680.

Artikel 49

Webbportal

1. En webbportal inrättas för att underlätta utövandet av rätten till åtkomst till, rättelse, radering eller begränsning av behandling av personuppgifter.

2. Webbportalen ska innehålla information om de rättigheter och förfaranden som avses i artiklarna 47 och 48 och ett användargränssnitt som gör det möjligt för personer vars uppgifter behandlas i MID och som underrättats om förekomsten av en röd länk i enlighet med artikel 32.4 att få kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter.

3. För att få kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter bör den person vars uppgifter behandlas i MID uppge referensen för den myndighet som ansvarar för den manuella verifieringen av olika identiteter enligt vad som avses i artikel 34 d. Webbportalen ska använda denna referens för att hämta kontaktuppgifterna till den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter. Webbportalen ska också inkludera en mall för ett e-postmeddelande för att underlätta kommunikationen mellan portalanvändaren och den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter. Detta e-postmeddelande ska innehålla ett fält för det enda identifikationsnummer som avses i artikel 34 c, så att den behöriga myndigheten i den medlemsstat som ansvarar för den manuella verifieringen av olika identiteter kan identifiera de berörda uppgifterna.

4. Medlemsstaterna ska ge eu-Lisa kontaktuppgifter till alla myndigheter som är behöriga att pröva och besvara varje sådan begäran som avses i artiklarna 47 och 48 och ska regelbundet se över huruvida dessa kontaktuppgifter är aktuella.

5. eu-Lisa ska utveckla webbportalen och säkerställa dess tekniska förvaltning.

6. Kommissionen ska anta en delegerad akt i enlighet med artikel 69 för att fastställa närmare bestämmelser om driften av webbportalen, inklusive användargränssnittet, de språk på vilka webbportalen ska finnas tillgänglig och e-postmallen.

Artikel 50

Överföring av personuppgifter till tredjeländer, internationella organisationer och privata parter

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

Artikel 51

Tillsynsmyndigheternas övervakning

1. Varje medlemsstat ska se till att tillsynsmyndigheterna på ett oberoende sätt övervakar lagligheten i den berörda medlemsstatens behandling av personuppgifter enligt den här förordningen, inklusive överföringen av dem till och från interoperabilitetskomponenterna.

2. Varje medlemsstat ska se till att de nationella lagar, föreskrifter och administrativa bestämmelser som antas i enlighet med direktiv (EU) 2016/680 vid behov är tillämpliga också på polismyndigheters och utsedda myndigheters åtkomst till interoperabilitetskomponenterna, även med avseende på rättigheterna för de personer vars uppgifter åtkomsten gäller.

3. Tillsynsmyndigheterna ska säkerställa att en revision av den behandling av personuppgifter som utförs av de ansvariga nationella myndigheterna vid tillämpningen av denna förordning genomförs i enlighet med relevanta internationella revisionsstandarder minst vart fjärde år.

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

4. Medlemsstaterna ska se till att deras tillsynsmyndigheter har de resurser och den expertis som krävs för att fullgöra de uppgifter som de åläggs enligt denna förordning.

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

Artikel 52

Europeiska datatillsynsmannens revisioner

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

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

Artikel 53

Samarbete mellan tillsynsmyndigheterna och Europeiska datatillsynsmannen

1. Tillsynsmyndigheterna och Europeiska datatillsynsmannen ska, var och en inom ramen för sina respektive befogenheter, aktivt samarbeta inom ramen för sina respektive ansvarsområden och säkerställa en samordnad tillsyn av användningen av interoperabilitetskomponenterna och tillämpningen av övriga bestämmelser i denna förordning, i synnerhet om Europeiska datatillsynsmannen eller en tillsynsmyndighet upptäcker stora skillnader mellan praxis i medlemsstaterna eller upptäcker eventuellt olagliga överföringar genom interoperabilitetskomponenternas kommunikationskanaler.

2. I de fall som avses i punkt 1 i den här artikeln ska en samordnad tillsyn säkerställas i enlighet med artikel 62 i förordning (EU) 2018/1725.

3. Europeiska dataskyddsstyrelsen ska senast den 12 juni 2021, och därefter vartannat år, skicka en gemensam rapport om sina aktiviteter enligt denna artikel till Europaparlamentet, rådet, kommissionen, Europol, Europeiska gräns- och kustbevakningsbyrån och eu-Lisa. Denna rapport ska innehålla ett kapitel om varje medlemsstat som utarbetats av den berörda medlemsstatens tillsynsmyndighet.

KAPITEL VIII

Ansvarsområden

Artikel 54

eu-Lisas ansvarsområden under utformnings- och utvecklingsfasen

1. eu-Lisa ska säkerställa att interoperabilitetskomponenternas centrala infrastrukturer drivs i enlighet med denna förordning.

2. Interoperabilitetskomponenterna ska hysas av eu-Lisa vid dess tekniska anläggningar och ska tillhandahålla de funktioner som fastställs i denna förordning i enlighet med de krav på säkerhet, tillgänglighet, kvalitet och prestanda som anges i artikel 55.1.

3. eu-Lisa ska ansvara för interoperabilitetskomponenternas utveckling, för de anpassningar som krävs för att upprätta interoperabilitet mellan de centrala systemen för in- och utresesystemet, VIS, Etias, SIS, Eurodac och Ecris-TCN, ESP, den gemensamma biometriska matchningstjänsten, CIR, MID och CRRS.

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

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

eu-Lisa ska utveckla och implementera interoperabilitetskomponenterna så snart som möjligt efter ikraftträdandet av denna förordning och kommissionens antagande av de åtgärder som föreskrivs i artiklarna 8.2, 9.7, 28.5 och 28.7, 37.4, 38.3, 39.5, 43.5 och 74.10.

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

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

5. Förvaltningsgruppen för programmet ska sammanträda regelbundet och minst tre gånger i kvartalet. Den ska säkerställa en lämplig hantering av interoperabilitetskomponenternas utformnings- och utvecklingsfas.

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

6. eu-Lisas styrelse ska fastställa arbetsordningen för förvaltningsgruppen för programmet, vilken i synnerhet ska innehålla bestämmelser om följande:

a) Ordförandeskap.

b) Mötesplatser.

c) Mötesförberedelser.

d) Tillträde för experter till mötena.

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

Ordförandeskapet ska innehas av en medlemsstat som enligt unionsrätten fullt ut omfattas av de rättsliga instrument som reglerar utveckling, inrättande, drift och användning av samtliga EU-informationssystem och som kommer att delta i interoperabilitetskomponenterna.

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

Den rådgivande grupp för interoperabilitet som avses i artikel 71 ska sammanträda regelbundet till dess att interoperabilitetskomponenterna tas i drift. Den ska rapportera till förvaltningsgruppen för programmet efter varje möte. Den ska tillhandahålla teknisk expertis till stöd för förvaltningsgruppens uppgifter och följa upp medlemsstaternas förberedelser.

Artikel 55

eu-Lisas ansvarsområden före och efter idrifttagandet

1. Efter det att respektive interoperabilitetskomponent tagits i drift ska eu-Lisa ansvara för den tekniska förvaltningen av den centrala infrastrukturen för interoperabilitetskomponenterna, inbegripet underhållet av dem och den tekniska utvecklingen. I samarbete med medlemsstaterna ska byrån se till att bästa tillgängliga teknik används, med förbehåll för en kostnads-nyttoanalys. eu-Lisa ska också ansvara för den tekniska förvaltningen av den kommunikationsinfrastruktur som avses i artiklarna 6, 12, 17, 25 och 39.

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

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

2. Utan att det påverkar tillämpningen av artikel 17 i tjänsteföreskrifterna för tjänstemän vid Europeiska unionen ska eu-Lisa tillämpa lämpliga regler avseende tystnadsplikt eller motsvarande konfidentialitetskrav på all personal som arbetar med uppgifter som lagras i interoperabilitetskomponenterna. Denna skyldighet ska gälla även efter det att den anställda i fråga lämnat sin tjänst eller anställning eller upphört med sin verksamhet.

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

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

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

Artikel 56

Medlemsstaternas ansvarsområden

1. Varje medlemsstat ska ansvara för följande:

a) Anslutning av till ESP:s och CIR:s kommunikationsinfrastruktur.

b) Integration av de befintliga nationella systemen och infrastrukturerna med ESP, CIR och MID.

c) Organisation, förvaltning, drift och underhåll av den befintliga nationella infrastrukturen och dess anslutning till interoperabilitetskomponenterna.

d) Förvaltning av och föreskrifter för åtkomst för vederbörligen bemyndigad personal vid de behöriga nationella myndigheterna till ESP, CIR och MID i enlighet med denna förordning och upprättande och regelbunden uppdatering av en förteckning över denna personal och deras profiler.

e) Antagande av de lagstiftningsåtgärder som avses i artikel 20.5 och 20.6 för att få åtkomst till CIR i identifieringssyfte.

f) Den manuella verifiering av olika identiteter som avses i artikel 29.

g) Efterlevnad av de krav på uppgiftskvalitet som fastställs i unionsrätten.

h) Efterlevnad av reglerna i varje EU-informationssystem beträffande personuppgifternas säkerhet och integritet.

i) Avhjälpande av eventuella brister som konstaterats i kommissionens utvärderingsrapport om uppgifternas kvalitet som avses i artikel 37.5.

2. Varje medlemsstat ska ansluta sina utsedda myndigheter till CIR.

Artikel 57

Europols ansvarsområden

1. Europol ska säkerställa att ESP behandlar sökningarna i Europoluppgifter. Europol ska i enlighet med detta anpassa sitt gränssnitt Querying Europol Systems (QUEST) till uppgifter med en grundläggande skyddsnivå.

2. Europol ska ansvara för förvaltningen av, och arrangemangen för, dess vederbörligen bemyndigade personals användning av och åtkomst till ESP och CIR enligt denna förordning samt upprättandet och regelbunden uppdatering av en förteckning över denna personal och deras profiler.

Artikel 58

Etias centralenhets ansvarsområden

Etias centralenhet ska ansvara för följande:

a) Den manuella verifieringen av olika identiteter i enlighet med artikel 29.

b) Genomförande av en spårning av multipla identiteter bland de uppgifter som lagras i in- och utresesystemet, VIS, Eurodac och SIS enligt vad som avses i artikel 65.

KAPITEL IX

Ändringar av andra unionsinstrument

Artikel 59

Ändringar av förordning (EU) 2018/1726

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

1. Artikel 12 ska ersättas med följande:

"*Artikel 12*

Uppgifternas kvalitet

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

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

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

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

2. Artikel 19.1 ska ändras på följande sätt:

a) Följande led ska införas:

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

b) Led ff ska ersättas med följande:

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

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

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

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

c) Led hh ska ersättas med följande:

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

d) Led mm ska ersättas med följande:

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

3. Artikel 22.4 ska ersättas med följande:

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

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

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

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

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

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

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

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

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

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

5. Artikel 27 ska ändras på följande sätt:

a) I punkt 1 ska följande led införas:

"da) Den rådgivande gruppen för interoperabilitet."

b) Punkt 3 ska ersättas med följande:

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

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

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

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

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

Artikel 60

Ändringar av förordning (EU) 2018/1862

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

1. I artikel 3 ska följande led läggas till:

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

19. *den gemensamma biometriska matchningstjänsten*: den gemensamma biometriska matchningstjänst som inrättas genom artikel 12.1 i förordning (EU) 2019/818,

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

21. *MID*: den detektor för multipla identiteter som inrättas genom artikel 25.1 i förordning (EU) 2019/818,

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

2. Artikel 4 ska ändras på följande sätt:

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

"b) Ett nationellt system (nedan kallat *N.SIS*) i var och en av medlemsstaterna, bestående av de nationella datasystem som står i förbindelse med det centrala SIS, inklusive minst en nationell eller gemensam backup av N.SIS.

c) En kommunikationsinfrastruktur som förenar CS-SIS och dess backup samt NI-SIS (nedan kallad *kommunikationsinfrastrukturen*) och som tillhandahåller ett krypterat virtuellt nätverk särskilt avsett för SIS-uppgifter och utbytet av uppgifter mellan Sirenekontoren i enlighet med vad som avses i artikel 7.2.

d) En säker kommunikationsinfrastruktur mellan CS-SIS och de centrala infrastrukturerna för ESP, den gemensamma biometriska matchningstjänsten och MID."

b) Följande punkter ska läggas till:

"8. Utan att det påverkar tillämpningen av punkterna 1–5 får sökningar i SIS-uppgifter om personer och identitetshandlingar göras också via ESP.

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

3. I artikel 7 ska följande punkt införas:

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

4. I artikel 12.1 ska följande stycke läggas till:

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

5. I artikel 44.1 ska följande led läggas till:

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

6. Artikel 74.7 ska ersättas med följande:

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

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

Artikel 61

Ändringar av förordning (EU) 2019/816

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

1. I artikel 1 ska följande led läggas till:

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

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

2. Artikel 2 ska ersättas med följande:

"*Artikel 2*

Tillämpningsområde

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

3. Artikel 3 ska ändras på följande sätt:

a) Led 8 utgår.

b) Följande led ska läggas till:

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

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

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

4. Artikel 4.1 ska ändras på följande sätt:

a) Led a ska ersättas med följande:

"a) ett centralt system,".

b) Följande led ska införas:

"aa) CIR,".

c) Följande led ska läggas till:

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

5. Artikel 5 ska ändras på följande sätt:

a) I punkt 1 ska inledningen ersättas med följande:

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

b) Följande punkt ska införas:

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

6. Artikel 8 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

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

b) Punkt 2 ska ersättas med följande:

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

7. Artikel 9 ska ändras på följande sätt:

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

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

8. I artikel 10.1 ska led j utgå.

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

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

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

12. Artikel 24 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

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

b) Följande punkt ska läggas till:

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

13. Artikel 32 ska ersättas med följande:

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

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

15. Artikel 41.2 ska ersättas med följande:

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

a) Alfanumeriska uppgifter ska föras in i det centrala systemet och CIR senast vid utgången av den period som avses i artikel 35.2.

b) Uppgifter om fingeravtryck ska föras in i det centrala systemet och CIR inom två år från driftstarten i enlighet med artikel 35.4."

KAPITEL IX

Slutbestämmelser

Artikel 62

Rapportering och statistik

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

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

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

a) Antalet sökningar för de syften som avses i artiklarna 20, 21 och 22.

b) Personens medborgarskap, kön och födelseår.

c) Typ av resehandling och trebokstavskoden för det utfärdande landet.

d) Antalet sökningar som utförts med och utan biometriska uppgifter.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

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

a) Antalet sökningar som utförts med och utan biometriska uppgifter.

b) Antalet länkar per typ och de EU-informationssystem som innehåller de länkade uppgifterna.

c) Den tidsperiod under vilken en gul och en röd länk har blivit kvar i systemet.

Uppgifterna får inte möjliggöra identifiering av enskilda personer.

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

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

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

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

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

Artikel 63

Övergångsperiod för användning av den europeiska sökportalen

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

2. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 69 för att ändra denna förordning genom att förlänga den period som avses i punkt 1 i den här artikeln en gång med högst ett år, om en bedömning av genomförandet av ESP visar att en sådan förlängning är nödvändig, särskilt mot bakgrund av de konsekvenser som idrifttagandet av ESP skulle ha för organisationen och varaktigheten av in- och utresekontroller.

Artikel 64

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

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

Artikel 65

Övergångsperiod för spårning av multipla identiteter

1. Under en ettårsperiod efter det att eu-Lisa har anmält slutförandet av det test av MID som avses i artikel 68.4 b och innan MID tas i drift ska Etias centralenhet ansvara för att utföra spårning av multipla identiteter med användning av de uppgifter som lagras i in- och utresesystemet, VIS, Eurodac och SIS. Spårningarna av multipla identiteter ska utföras med hjälp av enbart biometriska.

2. Om sökningen ger en eller flera träffar och identitetsuppgifterna i de länkade akterna är desamma eller liknande, ska en vit länk skapas i enlighet med artikel 33.

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

Vid flera träffar ska en länk skapas mellan alla uppgifter som gett upphov till träffen.

3. Om en gul länk skapas ska MID bevilja Etias centralenhet åtkomst till de identitetsuppgifter som finns i de olika EU-informationssystemen.

4. Om det skapas en länk till en registrering i SIS, utom en registrering som skapats enligt artikel 3 i förordning (EU) 2018/1860, artiklarna 24 och 25 i förordning (EU) 2018/1861 eller artikel 38 i förordning (EU) 2018/1862, ska MID bevilja Sirenekontoret i den medlemsstat som skapade registreringen åtkomst till de identitetsuppgifter som finns i de olika informationssystemen.

5. Etias centralenhet eller, i de fall som avses i punkt 4 i denna artikel, Sirenekontoret i den medlemsstat som skapade registreringen ska ha åtkomst till de uppgifter som finns i akten med identitetsbekräftelse och ska bedöma de olika identiteterna samt uppdatera länken i enlighet med artiklarna 31, 32 och 33 och lägga till den i akten med identitetsbekräftelse.

6. Etias centralenhet ska underrätta kommissionen i enlighet med artikel 67.3 först efter det alla gula länkar har verifierats manuellt och deras status uppdaterats till antingen gröna, vita eller röda länkar.

7. Medlemsstaterna ska vid behov bistå Etias centralenhet med att utföra spårning av multipla identiteter enligt denna artikel.

8. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 69 för att ändra denna förordning genom att förlänga den period som avses i punkt 1 i den här artikeln med sex månader, vilken kan förlängas två gånger med sex månader i taget. En sådan förlängning ska beviljas endast efter en bedömning av den uppskattade tiden för slutförande av spårning av multipla identiteter enligt denna artikel som visar att spårningen av multipla identiteter inte kan slutföras före utgången av den period som återstår antingen enligt punkt 1 i den här artikeln eller av en pågående förlängning, av skäl som ligger utanför Etias centralenhets kontroll, och att inga avhjälpande åtgärder kan tillämpas. Bedömningen ska genomföras senast tre månader före utgången av en sådan period eller av en pågående förlängning.,

Artikel 66

Kostnader

1. Kostnaderna i samband med inrättandet och driften av ESP, den gemensamma biometriska matchningstjänsten, CIR och MID ska belasta unionens allmänna budget.

2. Kostnaderna i samband med integreringen av befintliga nationella infrastrukturer och deras anslutning till de enhetliga nationella gränssnitten samt i samband med förvaltandet av de enhetliga nationella gränssnitten ska belasta unionens allmänna budget.

Följande kostnader ska vara undantagna:

a) Medlemsstaternas projektledningskontor (möten, tjänsteresor, kontor).

b) Hysande av nationella it-system (lokaler, implementering, elektricitet, kylning).

c) Drift av nationella it-system (operatörs- och supportavtal).

d) Utformning, utveckling, implementering, drift och underhåll av nationella kommunikationsnätverk.

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

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

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

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

Artikel 67

Underrättelser

1. Medlemsstaterna ska underrätta eu-Lisa om de myndigheter som avses i artiklarna 7, 20, 21 och 26 och som får använda eller ha åtkomst till ESP, CIR respektive MID.

En konsoliderad förteckning över dessa myndigheter ska offentliggöras i *Europeiska unionens officiella tidning* inom tre månader efter den dag då respektive interoperabilitetskomponent togs i drift i enlighet med artikel 68. Om förteckningen ändras ska eu-Lisa en gång om året offentliggöra en uppdaterad konsoliderad förteckning.

2. eu-Lisa ska underrätta kommissionen om att det test som avses i artikel 68.1 b, 68.2 b, 68.3 b, 68.4 b, 68.5 b och 68.6 b har slutförts på ett framgångsrikt sätt.

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

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

Artikel 68

Driftsstart

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

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

b) eu-Lisa har förklarat att ett övergripande test av ESP, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter och de unionsbyråer som får använda ESP, har slutförts på ett framgångsrikt sätt.

c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 8.1 och har anmält dessa till kommissionen.

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

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

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

a) De åtgärder som avses i artiklarna 13.5 och 43.5 har antagits.

b) eu-Lisa har förklarat att ett övergripande test av den gemensamma biometriska matchningstjänsten, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.

c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 13 och har anmält dessa till kommissionen.

d) eu-Lisa har förklarat att det test som avses i punkt 5 b har slutförts på ett framgångsrikt sätt.

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

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

a) De åtgärder som avses i artiklarna 43.5 och 74.10 har antagits.

b) eu-Lisa har förklarat att ett övergripande test av CIR, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.

c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 18 och har anmält dessa till kommissionen.

d) eu-Lisa har förklarat att det test som avses i punkt 5 b har slutförts på ett framgångsrikt sätt.

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

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

a) De åtgärder som avses i artiklarna 28.5 och 28.7, 32.5, 33.6, 43.5 och 49.6 har antagits.

b) eu-Lisa har förklarat att ett övergripande test av MID, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter och Etias centralenhet, har slutförts på ett framgångsrikt sätt.

c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 34 och har anmält dessa till kommissionen.

d) Etias centralenhet har underrättat kommissionen i enlighet med artikel 67.3.

e) eu-Lisa har förklarat att de tester som avses i punkterna 1 b, 2 b, 3 b och 5 b har slutförts på ett framgångsrikt sätt.

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

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

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

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

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

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

a) De åtgärder som avses i artiklarna 39.5 och 43.5 har antagits.

b) eu-Lisa har förklarat att ett övergripande test av CRRS, vilket ska utföras av eu-Lisa i samarbete med medlemsstaternas myndigheter, har slutförts på ett framgångsrikt sätt.

c) eu-Lisa har godkänt de tekniska och rättsliga arrangemangen för insamling och överföring av de uppgifter som avses i artikel 39 och har anmält dessa till kommissionen.

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

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

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

Artikel 69

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 28.5, 39.5, 49.6, 63.2 och 65.8 ska ges till kommissionen för en period på fem år från och med den 11 juni 2019. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av femårsperioden. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i artiklarna 28.5, 39.5, 49.6, 63.2 och 65.8 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning* eller vid ett senare datum som anges i beslutet. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 28.5, 39.5, 49.6, 63.2 och 65.8 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på [två månader] från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 70

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

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

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

Artikel 71

Rådgivande grupp

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

Artikel 72

Utbildning

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

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

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

Artikel 73

Handbok

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

Artikel 74

Övervakning och utvärdering

1. eu-Lisa ska säkerställa att det finns förfaranden för att övervaka utvecklingen av interoperabilitetskomponenterna och deras anslutning till det enhetliga nationella gränssnittet mot bakgrund av målen för planering och kostnader samt för att övervaka interoperabilitetskomponenternas funktion mot bakgrund av målen för tekniska resultat, kostnadseffektivitet, säkerhet och tjänsternas kvalitet.

2. Senast den 12 december 2019 och därefter var sjätte månad under interoperabilitetskomponenternas utvecklingsfas ska eu-Lisa lämna en rapport till Europaparlamentet och rådet om hur utvecklingen av interoperabilitetskomponenterna och deras anslutning till det enhetliga nationella gränssnittet fortskrider. Så snart utvecklingsarbetet har slutförts ska en rapport lämnas till Europaparlamentet och rådet med en ingående redogörelse för hur målen för framför allt planering och kostnader har uppfyllts samt vad eventuella avvikelser beror på.

3. Fyra år efter det att respektive interoperabilitetskomponent i enlighet med artikel 68 har tagits i drift, och därefter vart fjärde år, ska eu-Lisa rapportera till Europaparlamentet, rådet och kommissionen om interoperabilitetskomponenternas tekniska funktion, inbegripet ur säkerhetssynpunkt.

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

a) En bedömning av tillämpningen av denna förordning.

b) En granskning av uppnådda resultat i relation till denna förordnings mål och dess inverkan på de grundläggande rättigheterna, inbegripet i synnerhet en bedömning av påverkan av interoperabilitetskomponenterna på rätten till icke-diskriminering.

c) En bedömning av hur webbportalen fungerar, inklusive sifferuppgifter om användningen av webbportalen och antalet tillgodosedda begäranden.

d) En bedömning av huruvida de förutsättningar som ligger till grund för interoperabilitetskomponenterna fortfarande är giltiga.

e) En bedömning av säkerheten i interoperabilitetskomponenterna.

f) En bedömning av användningen av CIR för identifiering.

g) En bedömning av användningen av CIR för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.

h) En bedömning av eventuella konsekvenser, inbegripet eventuell oproportionellt stor inverkan på trafikflödet vid gränsövergångsställena, samt budgetkonsekvenser för unionens allmänna budget.

i) En bedömning av sökningar i Interpols databaser via ESP, inbegripet information om antalet träffar i Interpols databaser samt information om eventuella problem som uppstått.

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

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

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

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

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

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

a) de exakta syftena med sökningarna, däribland vilken typ av terroristbrott eller andra grova brott det gällt,

b) de välgrundade skälen att tro att en person som misstänks för, har begått eller utsatts för ett brott omfattas av förordning (EU) nr 603/2013,

c) antalet begäranden om åtkomst till CIR i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott,

d) antalet och den typ av ärenden som har lett till identifieringar,

e) behovet och utnyttjandet av möjligheten att åberopa brådskande undantagsfall, inklusive de fall där brådska inte godtogs som skäl vid den kontroll i efterhand som genomfördes av den centrala åtkomstpunkten.

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

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

Artikel 75

Ikraftträdande och tillämplighet

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

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

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

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

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

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

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

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

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

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

Utfärdad i Bryssel den 20 maj 2019.

På Europaparlamentets vägnar	*På rådets vägnar*
A. TAJANI	G. CIAMBA
Ordförande	*Ordförande*

Departementsserien 2022

Kronologisk förteckning

1. Viktigt meddelande till allmänheten – en översyn av VMA-systemet. Ju.
2. UTGÅR.
3. Garantitillägg i bostadstillägget. S.
4. Ökade möjligheter till användning av välfärdsteknik inom äldreomsorgen. S.
5. En effektivare upphandlingstillsyn. Fi.
6. Straff för deltagande i en terroristorganisation. Ju.
7. Ett försämrat säkerhetspolitiskt läge – konsekvenser för Sverige. UD.
8. Deterioration of the security environment – implications for Sweden. UD.
9. Ett utvidgat utreseförbud för barn. S.
10. Ett flexiblare karensvillkor i arbetslöshetsförsäkringen. A.
11. Arlanda flygplats – en plan för framtiden. I.
12. Vistelseförbud för barn. S.
13. Utökat informationsutbyte. Fi.
14. Ett hållbart mediestöd för hela landet. Ku.
15. Regler om privata sjukvårdsförsäkringar inom den offentligt finansierade hälso- och sjukvården. S.
16. Ledarhundar. S.
17. Inordnande av Statens medieråd i Myndigheten för press, radio och tv. Ku.
18. Straffansvar för pyskiskt våld. Ju.
19. Sweden's Ninth National Report under the Convention on Nuclear Safety. Sweden's Implementation of the Obligations of the Convention. M.
20. Återkallelse av sändningstillstånd med hänsyn till Sveriges säkerhet. Ku.
21. Anpassningar av svensk rätt till EU:s förordningar om interoperabilitet. Ju.

Departementsserien 2022

Systematisk förteckning

Arbetsmarknadsdepartementet

Ett flexiblare karensvillkor i arbetslöshetsförsäkringen. [10]

Finansdepartementet

UTGÅR. [2]

En effektivare upphandlingstillsyn. [5]

Utökat informationsutbyte. [13]

Infrastrukturdepartementet

Arlanda flygplats – en plan för framtiden. [11]

Justitiedepartementet

Viktigt meddelande till allmänheten – en översyn av VMA-systemet. [1]

Straff för deltagande i en terroristorganisation. [6]

Straffansvar för psykiskt våld. [18]

Anpassningar av svensk rätt till EU:s förordningar om interoperabilitet. [21]

Kulturdepartementet

Ett hållbart mediestöd för hela landet. [14]

Inordnande av Statens medieråd i Myndigheten för press, radio och tv. [17]

Återkallelse av sändningstillstånd med hänsyn till Sveriges säkerhet. [20]

Miljödepartementet

Sweden's Ninth National Report under the Convention on Nuclear Safety. Sweden's Implementation of the Obligations of the Convention. [19]

Socialdepartementet

Garantitillägg i bostadstillägget. [3]

Ökade möjligheter till användning av välfärdsteknik inom äldreomsorgen. [4]

Ett utvidgat utreseförbud för barn. [9]

Vistelseförbud för barn. [12]

Regler om privata sjukvårdsförsäkringar inom den offentligt finansierade hälso- och sjukvården. [15]

Ledarhundar. [16]

Utrikesdepartementet

Ett försämrat säkerhetspolitiskt läge – konsekvenser för Sverige. [7]

Deterioration of the security environment – implications for Sweden. [8]