JD

JUSTIS- OG BEREDSKAPSDEPARTEMENTET

Høringsnotat

Politiavdelingen
Dato: 21. desember 2023
Saksnr: 23/5535
Høringsfrist: 8. februar 2024

Forslag til endringer i grenseloven, SIS-loven, utlendingsloven, politiloven og forslag til tilhørende forskriftsbestemmelser for gjennomføring av EUs forordninger om interoperabilitet mellom felleseuropeiske informasjonssystemer m.m.

Innhold

1 Høringsnotatets hovedinnhold

Justis- og beredskapsdepartementet sender med dette på høring forslag til nye lov- og forskriftsbestemmelser for gjennomføring av EUs to forordninger om interoperabilitet (driftskompatibilitet) mellom felleseuropeiske informasjonssystemer: Forordning (EU) 2019/817 om opprettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer for grenser og visum, og forordning (EU) 2019/818 om opprettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer for politisamarbeid og rettslig samarbeid, asyl og migrasjon.

Forordningene inneholder i det vesentlige likelydende bestemmelser. For enkelhets skyld vil de følgende henvisningene til artikler referer seg til artikkelnummereringen i forordning (EU) 2019/817. En nærmere redegjørelse for bakgrunnen for og innholdet i forordningene gis i punkt 2 og 3 nedenfor. Uoffisielle norske oversettelser av forordningene følger vedlagt.

Forordningene foreslås gjennomført ved inkorporasjon i grenseloven § 8 første ledd nye nr. 4 og 5, se høringsnotatet punkt 4.1 og lovforslaget.

Fordi forordningene gjør endringer i en rekke andre forordninger som allerede er inkorporert i norsk rett, foreslås også endringer i grenseloven § 8 første ledd nr. 1 og 2, SIS-loven § 1 nr. 1 og 2 og utlendingsloven § 9a og 102 som innarbeider endringene. I tillegg foreslå noen språklige justeringer i disse inkorporasjonsbestemmelsene, se punkt 4.2.

Med hjemmel i grenseloven § 25 nr. 12 og ny nr. 13 foreslås en ny forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for grensepassering, utlendingsforvaltning og politisamarbeid, se høringsnotatet punkt 4.3. I forskriften foreslås angitt hvilke informasjonssystemer Norge er tilsluttet og hvem som har behandlingsansvar for de ulike systemene. Det foreslås i tillegg en bestemmelse som gjennomfører den valgfrie adgangen i forordningene artikkel 20 til å gi politiet rett til å søke i det felles identitetsregisteret for identifikasjonsformål, se punkt 4.4.

Videre foreslås det to nye hjemler i politiloven for opptak av biometriske opplysninger i forbindelse med identitetskontroll, samt enkelte endringer i reglene i utlendingsloven om opptak av biometriske opplysninger, se punkt 5. Disse forslagene er ikke nødvendig for å gjennomføre forordningene. Departementet har ikke tatt stilling til om det bør innføres en hjemmel som skissert i politiloven ny § 10 a, og ber særskilt om innspill fra høringsinstansene til denne bestemmelsen.

2 Bakgrunnen for forordningene

Etter terrorangrepene i Paris i november 2015 og i Brussel i mars 2016 publiserte Europakommisjonen i april 2016 en meddelelse om sterkere og smartere informasjonssystemer for grenser og sikkerhet (KOM (2016) 205). Meddelelsen omhandlet svakhetene i de felleseuropeiske informasjonssystemene for grensekontroll, migrasjonsforvaltning og kriminalitetsbekjempelse, og tiltak for mer effektiv beskyttelse av Schengens yttergrenser og indre sikkerhet. Mer helhetlig informasjonsforvaltning og mer effektiv utnyttelse av eksisterende informasjon ble ansett som sentrale tiltak. I tilknytning til dette ble det identifisert et behov for å lette berørte aktørers tilgang til nødvendig informasjon gjennom utvikling av multifunksjonelle løsninger og enhetlig regulering. Ved å få informasjonssystemene til å kommunisere med hverandre, såkalt interoperabilitet, mente Kommisjonen at informasjonen kunne utnyttes bedre, at kvaliteten på den kunne heves og kostnadene reduseres.

Forordning (EU) 2019/817 om opprettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer for grenser og visum og forordning (EU) 2019/818 om opprettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer for politisamarbeid og rettslig samarbeid, asyl og migrasjon ble vedtatt samtidig og inneholder i det vesentlige likelydende bestemmelser. Inndelingen i to forordninger skyldes at man på denne måten kan ivareta hensynet til at noen av EUs medlemsstater står utenfor Schengen-samarbeidet, mens andre har egne avtaler knyttet til politisamarbeidet.

Forordningene tar sikte på å legge til rette for en mer effektiv utnyttelse av EU-informasjonssystemene som understøtter forvaltningen av grense-, migrasjons- og sikkerhetsområdet. Dette gjøres ved at det opprettes en portal som gjør det mulig for medlemslandenes systemer å søke i flere EU-systemer samtidig. Tilgangen til biografiske og biometriske opplysninger som i dag lagres i enkeltdatabaser, samles, og det etableres muligheter for å identifisere personer som er registrert i

flere systemer. Dette vil også styrke muligheten for å oppdage personer som er registrert med ulike identiteter eller som bruker en annens identitet.

Interoperabilitetsforordningene er senere endret ved europarlaments- og rådsforordningene (EU) 2021/1133 og (EU) 2021/1134 om endringer i VIS-forordningen, begge av 7. juli 2021. Det vises til departementets høringsnotat 7. juni 2023 (saksnummer 23/2710) om endringer i visuminformasjonssystemet (VIS) og tilkobling av VIS til andre europeiske informasjonssystemer for omtale av betydningen av disse endringene.

3 Innholdet i forordningene

3.1 Kort om interoperabilitetsløsningen

Interoperabilitetsløsningen etablerer felles funksjoner og infrastruktur for ulike informasjonssystemer. Med «interoperabilitet» forstås IT-systemers evne til å utveksle data og dele informasjon og kunnskap. Interoperabilitet mellom systemene innebærer ikke at flere personer blir registrert eller at noen må oppgi flere opplysninger om seg selv.

Informasjonssystemene som ligger under interoperabilitetsløsningen er fremreisesystemet (EES), visuminformasjonssystemet (VIS), det europeiske systemet for reiseinformasjon og reisetillatelse (ETIAS), Eurodac, Schengen informasjonssystem (SIS) og det europeiske strafferegistreringssystemet for tredjelandsborgere (ECRIS-TCN). Rettsaktene forutsetter også at det skal kunne søkes mot Europol og Interpolbaser.

EES, VIS, ETIAS, Eurodac og SIS er gjennomført i Norge og regulerer hvilke opplysninger som registreres om den enkelte. Norge er ikke tilknyttet ECRIS-TCN. At det kommer en forordning som regulerer funksjoner som er felles for disse systemene innebærer ikke at flere personer blir registrert eller at noen må gi flere opplysninger om seg selv enn hva som allerede fremkommer av rettsaktene som regulerer de underliggende systemene.

Interoperabilitetsløsningen skal sikre at sluttbrukerne av de ulike systemene gis rask og enkel tilgang til informasjonen i de underliggende systemene. En persons identitet skal kunne klarlegges ved bruk av eksisterende biometrisk informasjon for å sikre at en person identifiseres korrekt, samt hindre misbruk av identitet.

For å nå disse målsettingene foreskriver forordningene en interoperabilitetsløsning bestående av fire komponenter.

1. Felles søkeportal (European search portal - ESP)
2. Felles biometrisk sammenligningstjeneste (shared Biometric Matching Service - sBMS)
3. Felles identitetsregister (Common Identity Repository - CIR)
4. Fleridentitetsdetektor (Multiple-Identity Detector - MID)

Den felles søkeportalen (ESP) vil være en felles inngang til systemene som omfattes av løsningen. Portalen vil gjøre det mulig å foreta søk i flere systemer samtidig og få et samlet svar tilbake. Myndigheten som foretar slike søk vil ikke få tilgang til mer informasjon enn det som følger av brukertilgangen til de

underliggende EU-systemene. ESP er regulert i forordningenes kapittel II, jf. punkt 2.4.2 under.

Den felles biometriske sammenligningstjenesten (sBMS) skal ha en sentral infrastruktur hvor biometriske maler samles og lagres, og skal erstatte de sentrale systemene for biometriske opplysninger i EES, VIS, SIS, Eurodac (EUs fingeravtrykksdatabase) og ECRIS-TCN (det europeiske strafferegisterinformasjonssystemet for tredjestatsborgere). En biometrisk mal er en kodebasert representasjon av materialet, i stedet for en hel gjengivelse med alle detaljer. Lagring av maler fremfor fullt bilde anses mindre inngripende for personvernet og er godt egnet for elektronisk behandling. Reglene om sBMS er inntatt i forordningenes kapittel III, jf. punkt 2.4.3 under.

Felles identitetsregister (CIR) skal inneholde biografiske data (navn, fødselsdato, nasjonalitet mv.) og biometriske opplysninger (ansiktsfoto, fingeravtrykk) som er registrert på en person i Eurodac, VIS, EES, ETIAS og ECRIS-TCN. Hovedformålet med registeret er å sikre at en person blir riktig identifisert uansett hvilket system eller systemer det søkes i. De biografiske opplysningene vil bli lagret i det felles identitetsregisteret i individuelle saksmapper for hver registrerte person, men opplysningene skal fortsatt tilhøre de enkelte underliggende systemene. CIR er regulert i forordningenes kapittel IV, jf. punkt 2.4.4 under.

Opprettelsen av CIR gir i utgangspunktet ingen utvidet rett til eller mulighet for søk utover det som følger av myndighetens tilgang til de underliggende informasjonssystemene. Søk gjennom CIR avgrenser treff til de registrene enheten har tilgang til etter underliggende rettsgrunnlag, og til de formål tilgangsretten gjelder. Et unntak er hvis et søk gir treff på liknende identitetsopplysninger i et annet register. I slike tilfeller vil myndigheten med ansvar for manuell kontroll av treff ha tilgang til identitetsopplysninger i alle registrene med mulig treff. Personinformasjon registrert i SIS inngår ikke i CIR.

For å forenkle identitetskontroller og bekjempe identitetsbedrageri opprettes en teknisk komponent kalt fleridentitetsdetektor (MID) som skal kunne påvise flere identiteter. Når en person er registrert i flere registre blir det opprettet en lenke mellom identitetsopplysningene. Det opprettes en gul lenke dersom opplysningene er delvis like, men ulike nok til at de må verifiseres manuelt. Lenkene gis deretter manuelt en farge som angir hvorvidt det dreier seg om samme person, om det er behov for nærmere undersøkelser rundt identitet, eller om det er mistanke om misbruk av identitet.

Myndigheten som har ansvaret for å avgjøre hva slags lenke som skal opprettes mellom identitetsopplysningene i ulike registre, har tilgang til de ulike registrene for dette formål. Når det er lenker mellom ulike registre, opprettes en identitetsbekreftelsesmappe hvor det blant annet skal være en henvisning til hvilke av registrene de lenkede opplysningene tilhører.

3.2 Personvernregler og behandlingsansvar

Forordning (EU) 2016/679 (General Data Protection Regulation - personvernforordningen) – heretter GDPR – gjelder for myndighetenes behandling av opplysninger etter forordningene, med mindre behandlingen foretas av rettshåndhevende myndigheter med sikte på å forebygge, avsløre eller etterforske terrorhandlinger eller andre alvorlige straffbare forhold. I disse tilfellene kommer

(EU) 2016/680 (Law Enforcement Directive) – heretter LED – til anvendelse. I Norge er disse rettsaktene gjennomført i henholdsvis personopplysningsloven og politiregisterloven, som da vil gjelde når norske myndigheter behandler opplysninger i henhold til interoperabilitetsforordningene.

Personopplysningene det gis tilgang til gjennom interoperabilitetsløsningen er innhentet med grunnlag i de rettsaktene som regulerer de enkelte informasjonssystemene. Interoperabilitetsforordningene angir hvem som vil være behandlingsansvarlig ved behandling av opplysninger gjennom interoperabilitetsforordningens nye tekniske komponenter, og fordeler dette ansvaret mellom ulike nasjonale myndigheter og EU-organer avhengig av bruk.

Forordningenes bestemmelser om vern av personopplysninger og behandlingsansvar omtales nærmere i punkt 3.3.7 under.

3.3 Nærmere om de enkelte kapitlene i forordningene

3.3.1 Kapittel I – Alminnelige bestemmelser

Kapittelet gir alminnelige bestemmelser om formål, mål, virkeområde og definisjoner.

Formålet er å opprette en ramme for å sikre interoperabilitet mellom informasjonssystemene.

Rammeløsningen omfatter en søkeportal (ESP), en felles biometrisk sammenligningstjeneste (sBMS), et felles identitetsregister (CIR) og en fleridentitetsdetektor (MID). Forordningene om interoperabilitet har til mål å forbedre inn- og utreisekontroll ved de ytre grensene, forebygge og bekjempe ulovlig innvandring, bidra til et høyt sikkerhetsnivå, forbedre gjennomføringen av felles visumpolitikk, bistå ved gjennomgåelsen av søknad om beskyttelse, bidra til å forebygge, avsløre og etterforske terrorhandlinger og andre alvorlige straffbare forhold, samt å gjøre det enklere å identifisere ukjente personer etter naturkatastrofer, ulykker og terrorangrep. Målene skal oppnås ved blant annet å sikre korrekt identifisering av personer og bidra til å bekjempe identitetsbedrageri.

3.3.2 Kapittel II – Den europeiske søkeportal

Kapittelet omhandler Den europeiske søkeportal (ESP). Portalen skal gjøre det mulig å søke samtidig i EES, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN, samt i Europol-opplysninger og Interpol-databasene. Bruken av ESP skal forbeholdes medlemsstatene og byråene som har tilgang til minst ett av EU-informasjonssystemene. Det skal opprettes ulike profiler for brukertilgang til ESP for hver kategori av brukere av portalen. De ulike profilene vil fastsettes ut fra hvordan retten til å søke er avgrenset til ulike systemer og opplysninger. Svarene på søkene kan bare inneholde opplysningene brukeren har tilgang til. Det er eu-LISA – Den europeiske unions byrå for driftsforvaltning av store IT-systemer innenfor området frihet, sikkerhet og rettferdighet – som skal føre logg over all behandling av opplysninger i ESP. Loggen skal vise hvilen medlemsstat eller unionsbyrå som innledet søket og hvilke systemer det ble foretatt søk i. Den enkelte medlemsstat skal på sin side selv føre logg over søk foretatt av personale hos deres myndigheter.

3.3.3 Kapittel III – Felles biometrisk sammenligningstjeneste

Kapittelet omhandler felles biometrisk sammenligningstjeneste. Den skal bestå av en sentral infrastruktur som skal erstatte de sentrale systemene for registrering av data i henholdsvis EES, VIS, Eurodac og ECRIS-TCN og muliggjøre søk i disse registrene med biometriske opplysninger.

Hovedformålet med tjenesten for sammenligning av biometriske opplysninger er å forenkle identifiseringen av en person som er registrert i flere databaser ved bruk av en felles teknologisk sammenligningsløsning.

3.3.4 Kapittel IV – Felles identitetsregister

Kapittelet gir regler om det felles identitetsregisteret (CIR). Dette skal bestå av individuelle saksmapper på personer som er registrert i de underliggende systemene, med unntak av SIS. CIR erstatter dermed de sentrale systemene i EES, VIS, ETIAS, Eurodac og ECRIS-TCN. Den individuelle saksmappen kan bare lagres i CIR så lenge de tilsvarende opplysningene lagres i minst ett av EU-informasjonssystemene.

Interoperabilitetsforordningene artikkel 20 til 22 angir hvem som kan søke i CIR og vilkårene for søk.

Den mest sentrale bestemmelsen er artikkel 21, som gir myndighetene med ansvar for manuell verifisering av forskjellige identiteter tilgang til CIR for behandling av røde og gule lenker, se punkt 3.3.5. Overført til norske forhold vil det være grense- og utlendingsmyndighetene som kan søke i CIR når det oppstår tvil om den registrertes identitet. Departementet finner i denne sammenheng også grunn til å nevne at politiet i Norge er grensemyndighet og en del av utlendingsmyndigheten. I denne egenskap vil dermed også politiet kunne søke i CIR. Derimot vil politiet som politimyndighet ikke kunne søke i CIR i medhold av artikkel 21.

Derimot vil politiet som politimyndighet og påtalemyndigheten kunne søke i CIR etter artikkel 22, der formålet med søk er å forebygge, avsløre eller etterforske terrorhandlinger eller andre alvorlige straffbare forhold. Politiet har allerede i dag tilgang til EES, VIS, ETIAS og Eurodac for å bekjempe kriminalitet i henhold til disse informasjonssystemenes respektive rettslige grunnlag. Artikkel 22 er ment å forenkle politimyndighetens tilgang ved at de gjennom søk i CIR raskt kan gis svar på om det finnes informasjon i noen av de underliggende systemene.

Artikkel 20 åpner for at politimyndigheter på nærmere angitte vilkår kan søke i CIR for identifiseringsformål. Bestemmelsen skiller seg fra artikkel 21 og 22 ved at anvendelsen av bestemmelsen forutsetter særskilt forankring i nasjonal lovgivning. Departementet foreslår at artikkel 20 forankres i norsk rett, jf. nærmere om dette i punkt 4.4 under.

Artikkel 24 omhandler føring av logger. Nr. 1 til 4 pålegger eu-LISA å føre logg over all behandling etter artikkel 20 til 22, og bestemmelsen gir en detaljert opplisting av hvilke forhold som skal logges. Nr. 5 pålegger også medlemslandene å føre logg over søk som myndigheter og personale utfører i samsvar med artikkel 20 til 22.

3.3.5 Kapittel V – Fleridentitetsdetektor

Kapittel V omhandler fleridentitetsdetektoren (MID). Denne skal opprette og lagre identitetsbekreftelsesmapper som inneholder lenker mellom opplysninger i EU-informasjonssystemene som inngår i CIR og SIS og som gjør det mulig å påvise flere identiteter, både for å forenkle identitetskontroller og bekjempe identitetsmisbruk.

Prosessen innledes ved opprettelse eller ajourføring av individuelle saksmapper gjennom EES, VIS, ETIAS, Eurodac eller SIS. Dersom innføring av nye opplysninger i et av informasjonssystemene ved sammenligning gir treff mot opplysninger som allerede er registrert i CIR eller SIS, skal det automatisk opprettes en hvit eller gul lenke mellom opplysningene som har ført til treffet.

Det opereres med fire farger på lenkene: hvit – gul – grønn – rød.

Hvite lenker genereres automatisk eller opprettes manuelt hvis identitetsopplysningene fra to eller flere informasjonssystemer bekrefter at man står overfor samme person. Dette omfatter også tilfeller hvor biometriske opplysninger viser til ulike biografiske opplysninger hvor denne forskjellen er begrunnet, for eksempel ved at en person har endret navn i forbindelse med ekteskapsinngåelse.

En *gul* lenke opprettes når det er behov for manuell kontroll av opplysningene i ulike registre. Dette vil være tilfellet når det er ulikhet mellom biografiske eller biometriske opplysninger eller opplysninger om reisedokumenter, eksempelvis hvor like biometriske opplysninger peker til forskjellige identitetsopplysninger. En *grønn* lenke skal etableres når koblingen mellom opplysningene er kontrollert og det viser seg at opplysningene gjelder forskjellige personer. Dette kan eksempelvis forekomme ved navnelikhet. En *rød* lenke skal etableres hvis like biometriske opplysninger peker mot ulike biografiske opplysninger og disse henviser til samme person på en ubegrunnet måte. Røde lenker etableres også når flere biometriske opplysninger peker mot samme biografiske opplysninger uten at dette er begrunnet eller hvor forskjellige identitetsopplysninger peker mot samme reisedokumentopplysninger uten at dette er begrunnet.

Den nærmere beskrivelsen av hvilke situasjoner de ulike lenkene skal dekke fremgår i artiklene 30 til 33.

Identitetsbekreftelsene skal kun lagres i MID så lenge de lenkede opplysningene er lagret i to eller flere EU-informasjonssystemer. Det gis nærmere opplysninger om hvilke myndigheter som skal foreta manuell kontroll av identiteter og hvilke registre de har tilgang til for dette formål.

3.3.6 Kapittel VI – Tiltak til støtte for interoperabilitet

Kapittelet omhandler tiltak til støtte for interoperabilitet, blant annet krav til kvaliteten på de opplysninger som registreres. Det gis også regler om meldingsformatet som skal brukes (UMF-standarden) og om etablering av et sentralt register for rapportering og statistikk.

3.3.7 Kapittel VII – Vern av personopplysninger

Kapittelet omhandler vern av personopplysninger, den registrertes rettigheter og tilsynsmyndighetens oppgaver.

Som nevnt i punkt 3.2 legges det i interoperabilitetsforordningene til grunn at GDPR og LED kommer til anvendelse, i norsk rett gjennomført i henholdsvis personopplysningsloven og politiregisterloven. Flere av bestemmelsene viser således også til disse rettsaktene, men enkelte ganger er det gitt regler som enten presiserer eller i noen grad avviker fra de tilsvarende reglene i de nevnte personvernrettsaktene.

Artikkel 40 regulerer behandlingsansvaret for komponentene sBMS, CIR og MID. Etter bestemmelsens nr. 1 og 2 skal de myndighetene som har behandlingsansvaret for de underliggende systemene også ha behandlingsansvaret når de behandler opplysninger i sBMS og CIR.

Når det gjelder MID fremgår det av bestemmelsens nr. 3 a at det er Det europeiske grense- og kystvaktbyrå (Frontex) som skal være behandlingsansvarlig for behandlingen av personopplysninger som utføres av Den sentrale ETIAS-enheten. Dette vil i all hovedsak dreie seg om lenker som er håndtert under MIDs overgangsperiode etter artikkel 65. Videre skal myndigheter som tilføyer og endrer opplysninger i identitetsbekreftelsesmappen ha ansvar for behandlingen av disse personopplysninger i MID, jf. nr. 3 b. Dette vil i praksis være ansvarlig myndighet for å foreta manuell kontroll av identiteter.

I artikkel 41 utpekes eu-LISA som databehandler for iBMS, CIR og MID.

Artikkel 42 omhandler informasjonssikkerhet, men her vises det ikke til de tilsvarende bestemmelsene i GDPR og LED. I stedet gis det en detaljert opplisting av hvilke tiltak, rutiner og rapportering eu-LISA skal utføre for å sikre informasjonssikkerhet knyttet til interoperabilitetsordningen.

Artikkel 43 omhandler brudd på personopplysningssikkerheten, og også her gis det detaljerte regler om hvilke prosedyrer som skal følges og hvilke organer som skal underrettes om slike brudd.

Artikkel 44 regulerer internkontroll. Den behandlingsansvarlige skal påse at behandlingen av opplysninger skjer i samsvar med forordningene, herunder gjennom hyppig kontroll av loggene.

Etter artikkel 45 skal medlemsstatene påse at misbruk av opplysninger eller behandling eller utveksling av opplysninger i strid med forordningen sanksjoneres i samsvar med nasjonal rett. Slike regler finner man i henholdsvis personopplysningsloven § 29 og politiregisterloven § 60 siste ledd, hvoretter Datatilsynet kan ilegge den behandlingsansvarlige tvangsmulkt dersom disse ikke etterkommer tilsynets pålegg.

Artikkel 46 regulerer erstatningsansvar. Både den registrerte og medlemsstatene kan kreve erstatning dersom de er påført skade som følge av ulovlig behandling av opplysninger. Erstatningsansvaret omfatter både økonomisk og ikke-økonomisk skade. Retten til erstatning gjelder uavhengig av retten til erstatning etter GDPR og LED.

Artikkel 47 regulerer informasjonsplikt. For opplysninger som lagres i sBMS, CIR eller MID gjelder artiklene 12 og 13 i GDPR. Personer som er registrert i EES, VIS eller ETIAS, skal underrettes i samsvar med bestemmelsene i forordningene om henholdsvis EES, VIS og ETIAS.

I artikkel 48 er det gitt regler om innsyn, retting og sletting og hvilke frister som gjelder for begjæringer om innsyn, retting og sletting. Det skal opprettes en

nettportal for å forenkle utøvelsen av rettighetene om innsyn, retting, sletting og begrensning av behandlingen, jf. artikkel 49.

Artikkel 51 regulerer tilsynsmyndighetenes tilsyn. I Norge fører Datatilsynet tilsyn med opplysningene som behandles etter personopplysningsloven og politiregisterloven. Etter nr. 3 skal tilsynet påse at det minst hvert fjerde år utføres en revisjon, i samsvar med relevante internasjonale revisjonsstandarder, av behandlingen av personopplysninger i henhold til interoperabilitetsforordningene. Videre skal tilsynet hvert år offentliggjøre antallet anmodninger til tilsynet om retting, sletting eller begrensning av behandling av personopplysninger, tiltak som er iverksatt som følge av dette, og antallet rettinger, slettinger eller begrensninger av behandling som er utført som følge av anmodninger fra berørte personer.

Artikkel 53 pålegger nasjonale tilsynsmyndigheter og EUs datatilsyn å aktivt samarbeide for å sikre et samordnet tilsyn med bruken av interoperabilitetskomponentene. Annethvert år skal Det europeiske Personvernrådet (EDPB) utarbeide en felles rapport som skal inneholde et kapittel om hver medlemsstat, utarbeidet av den berørte medlemsstatens tilsynsmyndighet.

3.3.8 Kapittel VIII, IX og X – Ansvar, endring av andre rettsakter og sluttbestemmelser

Kapittel VIII gir nærmere bestemmelser om ansvaret til eu-LISA, nasjonale myndigheter og Den sentrale ETIAS-enheten etter forordningen. Eu-LISA har ansvar for den tekniske infrastrukturen og driften av de sentrale systemene, mens medlemsstatene har ansvar for integrasjon av de eksisterende nasjonale systemene og infrastrukturene med ESP, CIR og MID.

Kapittel IX omhandler endringer i rettsaktene som regulerer de underliggende systemene for å tilpasse disse til etableringen av CIR, sBMS og MID. Dette gjelder VIS (forordning (EU) 767/2008), grenseforordningen (forordning (EU) 2016/399), EES (forordning (EU) 2017/2226), ETIAS (forordning (EU) 2018/1240), eu-LISA (forordning (EU) 2018/1726), SIS innen grensekontroll (forordning (EU) 2018/1861), VIS (forordning (EU) 2004/512/EF), samt rådsbeslutning 2008/633/JIS om rettshåndhevende myndigheters og Europols tilgang til VIS.

Kapittel X gir sluttbestemmelser. Det gis blant annet overgangsbestemmelser i forbindelse med innfasingen av interoperabilitetsløsningen. Det åpnes for at bruken av ESP vil være frivillig i en toårsperiode fra løsningen er satt i drift. CIR vil brukes når løsningen settes i drift, mens den sentrale ETIAS-enheten blir første bruker av MID i en ettårsperiode før løsningen settes i ordinær drift. Kapitelet regulerer fordelingen av kostnader mellom henholdsvis EU med ulike byråer og medlemsstatene, og det fremgår at medlemsstatene skal underrette eu-LISA om hvilke myndigheter som kan bruke eller ha tilgang til henholdsvis ESP, CIR og MID. Interoperabilitetsforordningene gir Europakommisjonen fullmakt til å fastsette gjennomføringsrettsakter for å angi tekniske detaljer og fremgangsmåter etter ulike bestemmelser, herunder standardskjema for behandling av hvite og røde lenker.

4 Gjennomføring av forordningene i norsk rett

4.1 Forslag til inkorporasjon av interoperabilitetsforordningene i grenseloven

Departementet foreslår at forordningene gjennomføres i norsk rett ved inkorporasjon, i form av en henvisningsbestemmelse som gjør forordningene til norsk lov uten omskrivninger.

En slik henvisningsbestemmelsene kan enten inntas i en eksisterende lov eller nedfelles i en egen lov. Departementet finner det ikke hensiktsmessig at det gis en egen lov om interoperabilitet. Det har samtidig vist seg noe vanskelig å innpasse gjennomføring av forordningene i en eksisterende lov. Utfordringen er at interoperabilitetsforordningene etablerer et felles teknisk system til bruk på tvers innen utlendingsforvaltning, grensekontroll og politisamarbeid, og at de underliggende systemene i Norge er regulert i ulike lover. VIS, ETIAS og Eurodac er i dag gjennomført i utlendingsloven. EES er gjennomført i grenseloven, og SIS i SIS-loven.

Etter en samlet vurdering foreslås interoperabilitetsforordningene gjennomført i grenseloven ved en tilføyelse av rettsaktene til listen over gjennomførte rettsakter i § 8 første ledd.

Rammeløsningen for interoperabilitet omfatter også informasjonssystemet ECRIS-TCN, som ikke omfattes av Schengen-samarbeidet og som Norge heller ikke er tilknyttet gjennom egen avtale. Departementet har vurdert om det i inkorporasjonsbestemmelsen er nødvendig å presisere at bestemmelser som omhandler dette informasjonssystemet, ikke vil gjelde for Norge. Gitt interoperabilitetsforordningenes oppbygning er vurderingen at en slik presisering ikke er nødvendig. Interoperabilitetsforordningene oppstiller kun reglene for de tekniske komponentene, og regulerer ikke tilgangen til de underliggende systemene. Gjennomføring av interoperabilitetsforordningene i norsk rett etablerer ikke tilgang til ECRIS-TCN for norske myndigheter. Heller ikke henvisninger til annet regelverk som Norge ikke er bundet av gjør slikt regelverk bindende for Norge. Tilsvarende gjelder Europol-opplysninger. Norge er tilknyttet Europol gjennom en egen samarbeidsavtale, men har, i motsetning til EU-landene, ikke direkte tilgang til Europols opplysninger.

Det følger av artikkel 5 i tilknytningsavtalen mellom Schengen-landene og Norge at avtalen ikke gjelder for Svalbard, men for Jan Mayen. Interoperabilitetsforordningene vil få samme virkeområde når disse inkorporeres i grenseloven, jf. grenseloven §§ 3 og 25 nr. 1, jf. grenseforskriften § 1-2, dvs. at de vil gjelde på Jan Mayen, men ikke på Svalbard.

4.2 Forslag til inkorporasjon av endringsforordninger

Etableringen av en teknisk ramme for interoperabilitet har nødvendiggjort endringer i en rekke andre rettsakter. Interoperabilitetsforordningene gjør endringer i forordning (EF) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726, (EU) 2018/1861, (EU) 2018/1862, (EU) 2019/816, rådsvedtak 2004/512/EF og rådsbeslutning 2008/633/JIS. De opplistede rettsaktene regulerer de underliggende informasjonssystemene som inngår i

rammen for interoperabilitet, og de fleste av disse rettsaktene er gjort til norsk lov ved inkorporasjon.

For å gjennomføre interoperabilitetsforordningenes endringer i disse rettsaktene, foreslås det endringer i deres respektive inkorporasjonsbestemmelser i grenseloven § 8 første ledd nr. 1 og 2, SIS-loven § 1 nr. 1 og 2 og utlendingsloven § 9a og 102. Forslagene tar utgangspunkt i og bygger videre på allerede foreslåtte endringer i de samme lovene i departementets høringsnotat 7. juni 2023 om nødvendige endringer som følge av gjennomføring av forordning (EU) 2021/1133 og (EU) 2021/1134 i norsk rett.

4.3 Forslag til forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning

Med hjemmel i grenseloven § 25 nr. 12 og ny nr. 13 foreslås en egen forskrift med utfyllende regler om gjennomføringen av interoperabilitetsforordningene i norsk rett.

Av informasjonshensyn foreslås at det i forskriften § 1 angis hvilke av informasjonssystemene i rammeløsningen Norge er tilknyttet.

I forskriften § 2 foreslås hjemmel for politiets søk identitetsregisteret (CIR) til identifiseringsformål på visse vilkår. Forslaget omtales i punkt 4.4 under.

Departementet ser også behov for nærmere regulering av behandlingsansvaret etter forordningene, se §§ 3 til 6 i forslaget til forskrift.

Interoperabilitetsforordningene artikkel 40 regulerer behandlingsansvaret for behandling av opplysninger i sBMS, CIR og MID. Som nevnt under punkt 3.3.7, legger forordningene opp til at den behandlingsansvarlige for det underliggende systemet, også skal være behandlingsansvarlig for opplysninger som behandles i sBMS og CIR. Ansvarlig myndigheter som tilføyer eller endrer opplysninger i identitetsbekreftelsesmappen i MID, skal være behandlingsansvarlig for behandlingen i denne tekniske komponenten.

I gjeldende rett er behandlingsansvaret for EES, VIS, SIS, Eurodac og ETIAS regulert ulikt. For de fleste systemene er behandlingsansvaret regulert i lov og forskrift, mens behandlingsansvaret for ETIAS og EES er regulert i instruks. Departementet foreslår at også behandlingsansvaret for ETIAS og EES forskriftsreguleres, se forslag til ny § 1-6 i grenseforskriften og ny § 3-3 b i utlendingsforskriften. Forskriftsfestingen innebærer ingen realitetsendring.

For å fastsette hvem som er behandlingsansvarlig etter interoperabilitetsforordningene artikkel 40, må det altså sees hen til hvem som er behandlingsansvarlig for de underliggende systemene. I forskriften § 3 foreslås en henvisningsbestemmelse som lister opp hvem som er behandlingsansvarlig for personopplysninger i EES, VIS, SIS, Eurodac og ETIAS i Norge, med en henvisning til hvor behandlingsansvaret er fastsatt i norsk rett. For å angi behandlingsansvarlig i sBMS og CIR, henvises det i forskriften §§ 4 og 5 tilbake til oversikten i forskriften § 3. Behandlingsansvaret for MID foreslås regulert i forskriften § 6, og følger i hovedsak samme systematikk.

4.4 Forslag til hjemmel for politiets søk i felles identitetsregister (CIR) for identifiseringsformål

4.4.1 Nærmere om artikkel 20

Politimyndigheter kan i henhold til artikkel 20 nr. 1 gis adgang til å søke i CIR for identifiseringsformål når

- politimyndigheten ikke kan identifisere en person fordi vedkommende mangler identifikasjonspapirer
- det er tvil om identitetsopplysningene som en person har framlagt
- det er tvil om ektheten av det reisedokumentet eller et annet troverdig dokument som en person har framlagt
- det er tvil om identiteten til innehaveren av et reisedokument eller et annet troverdig dokument
- personen ikke kan eller vil samarbeide

Bruk av søkeadgangen forutsetter hjemmel i medlemslandenes nasjonale lovgivning. En eventuell nasjonal regulering skal være utformet slik at tredjelandsborgere ikke forskjellsbehandles og skal angi til hvilke av formålene angitt i forordningene artikkel 2 nr. 1 bokstav b og c, søk i CIR tillates gjennomført, jf. art. 20 nr. 5. Det følger av artikkel 2 nr.1 bokstav b og c at identifiseringssøk skal kunne gjennomføres for å forebygge og bekjempe ulovlig innvandring og for å opprettholde offentlig sikkerhet og orden og ivareta sikkerheten på medlemsstatenes territorier. Kompetent politimyndighet skal utpekes, og fremgangsmåter, vilkår og kriterier for slike kontroller skal fastsettes i de nasjonale bestemmelsene om søkeadgang.

Forutsetningen for politimyndighetenes søk med biometriske opplysninger er at det skjer ved bruk av biometriske opplysninger som er opptatt under en identitetskontroll, og forutsatt at prosedyren er innledet i personens nærvær, jf. artikkel 20 nr. 2. Fortalens punkt 28 angir at fingeravtrykk bør opptas med teknikker for direkteskanning. Dersom personens biometriske opplysninger ikke kan brukes eller søket med disse opplysningene mislykkes, skal søket utføres med vedkommende sine identitetsopplysninger i kombinasjon med reisedokumentopplysninger eller identitetsopplysningene som personen har gitt.

Søk er ikke tillatt for identifisering av barn under 12 år, med mindre det er til barnets beste.

Søk i henhold til artikkel 20 gir tilgang til slike data som nevnt i artikkel 18 nr. 1, herunder navn, statsborgerskap, fødselsdato, kjønn, reisedokumentdetaljer, ansiktsbilder og fingeravtrykk. Det gis informasjon om hvilket underliggende system informasjonen stammer fra, men det gis ikke tilgang til ytterligere informasjon registrert i det eller de aktuelle EU-informasjonssystemet/-ene, jf. artikkel 18 nr. 2.

Etter artikkel 20 nr. 4 og 6 kan politimyndigheter også gis søkeadgang for å identifisere ukjente personer som er ute av stand til å legitimere seg og uidentifiserte menneskelige levninger etter naturkatastrofer, ulykker eller terrorangrep.

«Politimyndigheter» defineres i forordningene artikkel 4 nr. 19 ved henvisning til definisjonen i LED artikkel 3 nr. 7, som også omfatter påtalemyndigheten.

4.4.2 Departementets vurdering

Departementet foreslår at politiet gis hjemmel til å foreta identifiseringssøk mot CIR, slik artikkel 20 i interoperabilitetsforordningene åpner for, til de formål som er nevnt i bestemmelsen nr. 1 til 4. Søkeadgangen foreslås som nevnt hjemlet i forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning § 2, jf. grenseloven § 25 ny nr. 13.

Et av hovedformålene med interoperabilitetsforordningene er å bedre muligheten til å fastsette en persons identitet. Det å ha kjennskap til en persons reelle identitet er en grunnleggende forutsetning for at myndigheter kan utføre sine lovpålagte oppgaver. Søk i CIR etter artikkel 20 vil, på lik linje med undersøkelser etter artikkel 21 og 22, bedre politiets mulighet til å fastsette personers identitet. Departementet mener derfor at det bør åpnes for søk i CIR i de situasjoner artikkel 20 åpner for. Departementet legger vekt på at Politidirektoratet mener det er behov for en slik hjemmel, og en kan heller ikke se at det er vektige grunner som tilsier at politiet ikke skulle få denne adgangen.

Forslaget gir ikke i seg selv hjemmel for å oppta biometriske opplysninger, kun for at biometriske opplysninger kan benyttes til søk mot CIR for identifiseringsformål. Hjemmelen vil isolert sett ha begrensede personvernkonsekvenser, men disse må sees i sammenheng med forslaget om å gi politiet utvidede muligheter til å oppta biometriske opplysninger. Nytteverdien for politiet av en adgang til å søke i CIR etter artikkel 20 nr. 1 til 3 med biometriske opplysninger antas nemlig å ville være relativt begrenset dersom politiet ikke også gis hjemmel for opptak av biometriske opplysninger i forbindelse med identitetskontroll. Dette drøftes nærmere i punkt 5.1.3. Det vises til at nr. 2 forutsetter at søk med biometriske opplysninger bare kan finne sted dersom slike opplysninger er opptatt direkte under en identitetskontroll, og forutsatt at prosedyren er innledet i den berørte persons nærvær.

Etter gjeldende rett er det grenseloven § 22, utlendingsloven § 100 og straffeprosessloven § 160 som hjemler opptak av biometriske opplysninger.

Utlendingsloven § 100 gir hjemmel for å oppta og behandle biometriske opplysninger i form av ansiktsfoto og fingeravtrykk av en utlending som ikke kan dokumentere sin identitet, eller som det er grunn til å mistenke at oppgir uriktig identitet. Etter grenseloven § 22 tredje ledd kan biometrisk personinformasjon (ansiktsfoto og fingeravtrykk) innhentes elektronisk av alle som passerer grensekontroll eller annet kontrollsted for kontroll av reisedokumenter. Ingen av disse gir grunnlag for å oppta biometriske opplysninger for slike søk som artikkel 20 omhandler, siden bestemmelsene kun hjemler opptak av opplysninger som politiet innhenter henholdsvis grensemyndighet og utlendingsmyndighet. Politiet som grensekontrollmyndighet og utlendingsmyndighet vil kunne gjøre bruk av CIR, men da er tilgangen hjemlet i artikkel 21.

Det er kun straffeprosessloven § 160 som vil kunne være hjemmel for politiet for søk med biometriske opplysninger i CIR for de formål som artikkel 20 omfatter, og forutsatt at opptak etter denne bestemmelsen finner sted under identitetskontrollen. Straffeprosessloven § 160 åpner for at det kan tas fingeravtrykk og fotografi av personer som mistenkes eller er dømt for en handling som etter loven kan medføre frihetsstraff, og disse opplysningene lagres i politiets foto- og fingeravtrykkregister, jf. politiregisterloven § 13. Nærmere bestemmelser

er gitt i påtaleinstruksen kapittel 11. Etter § 11-1 kan det opptas fingeravtrykk og fotografi av enhver som er mistenkt i saken når det anses nødvendig for å oppklare en straffesak som kan medføre frihetsstraff. Departementet foreslår at politiet i ny forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning § 2 første ledd gis adgang til å gjennomføre søk i CIR dersom vilkårene i straffeprosessloven § 160 anses å være oppfylt under identitetskontrollen. Dersom personens biometriske opplysninger ikke kan brukes eller søket med disse opplysningene mislykkes, vil politiet kunne søke i CIR i henhold til artikkel 20 nr. 3 annet avsnitt, hvoretter søk kan finne sted med vedkommendes identitetsopplysninger kombinert med reisedokumentopplysninger.

Departementet antar samtidig at § 160 sjelden vil være aktuell i forbindelse med politiets identitetskontroll fordi den forutsetter at vedkommende kan mistenkes for lovbrudd som kan medføre frihetsstraff. Som det fremgår nedenfor vurderer departementet etter innspill fra Politidirektoratet å innføre to nye hjemler for opptak av biometriske opplysninger i politiloven §§ ny 10 a og 12 nytt sjette ledd, jf. nærmere om dette i punkt 5.1.

I forslaget til ny forskrift § 2 legges det opp til at det kun er politiet som skal ha adgang til å foreta søk etter forordningene artikkel 20. Forordningenes definisjon av politimyndigheter favner også påtalemyndigheten. Departementet legger til grunn at det ikke er behov for, ei heller hensiktsmessig, at påtalemyndigheten gis tilsvarende søketilgang.

Etter kystvaktloven § 21 har Kystvaktens tjenestemenn begrenset politimyndighet og kan foreta etterforsking på nærmere bestemte vilkår. Det legges ikke i forslaget opp til at Kystvakten skal gis tilgang til å søke i CIR for identifiseringsformål. Det bes om innspill til om det er behov for slik adgang også for Kystvakten.

Forordningene krever at det nasjonale rettsgrunnlaget, i tillegg til å utpeke kompetent myndighet, også fastsetter vilkår, fremgangsmåter og kriterier for identifiseringssøk. Departementet foreslår at kravet til regulering av formål, kriterier og fremgangsmåter ivaretas med en henvisning til vilkårene som følger av artikkel 20, at identifiseringssøk kun kan gjøres for formål nevnt i forordningene artikkel 2 nr. 1 bokstav b og c, og med henvisning til de aktuelle rettsgrunnlagene for opptak av biometriske opplysninger etter norsk rett.

5 Forslag til lovendringer som ikke er en nødvendig for gjennomføring av forordningene

5.1 Forslag til endringer i politiloven

5.1.1 Innledning

Som nevnt i punkt 4.4.2 har Politidirektoratet bedt departementet vurdere behovet for nye hjemler for opptak av biometriske opplysninger i politiloven for at politiet i større grad skal kunne benytte seg av de mulighetene for søk i CIR som artikkel 20 åpner for. Dette gjelder både adgang til opptak av biometriske opplysninger i situasjoner som beskrevet i forordningene artikkel 20 nr. 4, for identifisering av (1) ukjente personer ute av stand til å legitimere seg og (2) menneskelige levninger etter en naturkatastrofe, ulykke eller terrorangrep, og ved brudd på

identifikasjonsplikten overfor politiet. I de sistnevnte tilfellene er forutsetningen at opptaket er basert på samtykke.

De nye hjemlene foreslås inntatt i henholdsvis politiloven § 12 nytt sjette ledd og ny § 10 a. Disse forslagene er ikke nødvendig for å gjennomføre interoperabilitetsforordningene, men er i praksis en forutsetning for at politiet skal kunne nyttiggjøre seg søkeadgangen som artikkel 20 åpner for.

Med forslaget vil adgangen til opptak av biometriske opplysninger utvides utover hva som følger av straffeprosessloven § 160. I forslaget til forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning er det i § 2 også inntatt en henvisning til politiloven §§ 10 a og 12 sjette ledd.

5.1.2 Opptak av biometriske opplysninger ved naturkatastrofer, ulykker og terrorhandlinger

I forslaget til politiloven § 12 nytt sjette ledd foreslås en hjemmel for opptak av biometriske opplysninger til bruk for identifisering ved naturkatastrofer, ulykker og terrorhandlinger, jf. interoperabilitetsforordningene artikkel 20 nr. 4.

Politiloven § 12 har overskriften «Hjelp til syke mv.» og hjemler i annet til siste ledd ulike inngrep overfor syke, tilskadekomne og andre personer som ikke er i stand til å ta vare på seg selv, samt personer som er eller må antas å være omkommet. Femte og siste ledd gjelder politiets arbeid med identifisering. I femte ledd lovfestes politiets rett til å foreta visitasjon for å fastslå identiteten til personer som tas hånd om etter paragrafens tredje ledd. Samme ledd pålegger enhver å la politiet få adgang til materiale som kan brukes til identifikasjon av bortkomne, syke, tilskadekomne eller andre som ikke kan ta vare på seg selv, samt døde, jf. Ot.prp. nr. 22 (1994–1995) s. 64.

I forslaget til nytt sjette ledd gis det hjemmel for å oppta biometriske opplysninger for å identifisere ukjente personer ute av stand til å legitimere seg og uidentifiserte menneskelige levninger. Departementet mener at politiet i slike ekstreme situasjoner bør har muligheten for opptak av biometriske opplysninger for å kunne identifisere vedkommende. Det understrekes at den nye bestemmelsen ikke gir hjemmel for lagring av opplysningene, som derfor skal slettes så snart søket er gjennomført.

Det foreslås i ny forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning § 2 fastsatt at også biometriske opplysninger opptatt med hjemmel i politiloven § 12 nytt sjette ledd kan benyttes til søk mot CIR.

5.1.3 Opptak av biometriske opplysninger ved brudd på identifikasjonsplikten

Politiet kan forlange at personer oppgir navn, fødselsdato, fødselsår, stilling og bopel. Ved brudd eller mistanke om brudd på denne identifikasjonsplikten, kan politiet innbringe personen med hjemmel i politiloven § 8 første ledd nr. 3. Hverken identifikasjonsplikten eller politiets innbringelsesadgang er betinget av at det foreligger eller har foreligget en ordensforstyrrelse. Det kreves kun at identifisering er nødvendig for tjenesteutførelsen.

Adgangen til innbringelse til et polititjenestested gir mulighet til å gjennomføre visitasjon og søk i ulike registre, men innbringelse gir ikke i seg selv grunnlag for opptak av biometriske opplysninger. For at politiet skal kunne oppta biometriske opplysninger etter gjeldende rett, må det være grunnlag for dette i medhold av straffeprosessloven § 160.

Politidirektoratet har spilt inn at politiet har behov for å kunne ta opp biometri og søke i CIR i tilfeller hvor personer ikke oppfyller identifikasjonsplikten. Direktoratet har overfor departementet begrunnet behovet for den nye hjemmelen med at den vil kunne bidra til å effektivisere politipatruljenes identifiseringsarbeid og øke nytteverdien av personkontroll for patruljen. Ved å gjennomføre søk i CIR med sikre faktorer som fingeravtrykk og bilde, vil politiet i forbindelse med en hendelse raskere kunne fastsette korrekt identitet. Det vil da heller ikke være nødvendig å innbringe personen, noe som må antas å være i vedkommendes interesse. Direktoratet har også fremhevet er at man med den nye hjemmelen vil kunne unngå å bli beskyldt for diskriminering av utlendinger. Eksisterende lovhjemler i utlendingsloven § 100 gir kun grunnlag for opptak av biometriske opplysninger fra utlendinger eller personer som antas å være utlendinger. Det kan resultere i forskjellsbehandling hvis politiet (i egenskap av utlendingsmyndighet) påtreffer en større gruppe personer som ikke kan identifisere seg, og der hudfarge vil være eneste grunn til å anta at vedkommende er utlending. Med en slik ny hjemmel som foreslås vil politiet i medhold av politiloven kunne oppta biometriske opplysninger av alle tilstedeværende som ikke oppfyller identifikasjonsplikten.

Departementet vurderer at hensynet til å unngå diskriminering – eller beskyldninger om eller opplevelsen av det – ikke i seg selv er tilstrekkelig for å innføre en ny hjemmel for å oppta biometriske opplysninger. En ser imidlertid at opptak av biometriske opplysninger i slike tilfeller vil kunne bidra til å effektivisere politiets arbeid og unngå unødvendige innbringelser. En slik vil være forenlig med de formål som artikkel 20 nr. 5 oppstiller for å tillate søk i CIR til identifiseringsformål, nemlig å «bidra til å forebygge og bekjempe ulovlig innvandring», og å «opprettholde den offentlige sikkerhet og den offentlige orden og ivareta sikkerheten på medlemsstatenes territorier», jf. art. 2 nr. 1 bokstav b og c.

Departementet er samtidig noe i tvil om den reelle nytteverdien av en slik bestemmelse. En har derfor ikke konkludert med om en slik hjemmel bør innføres. Ved søk mot CIR, vil politiet kunne få treff mot tredjelandsborgere som er registrert med biometriske opplysninger i de underliggende EU-informasjonssystemer Norge er tilknyttet.

Søk mot CIR vil ikke gi treff dersom personen er norsk statsborger eller EØS-borger. Departementet foreslår imidlertid også å åpne for søk i foto- og fingeravtrykkregisteret, jf. politiregisterloven § 13 og politiregisterforskriften kapittel 46, til de samme formål og på de samme vilkår som for søk i CIR. Dette gjør at politiet i tillegg vil kunne få treff på personer som er blitt registrert i forbindelse med etterforsking av straffesaker og fullbyrdelse av straffereaksjoner, i utvisningssaker og i saker om utlevering til annen stat, jf. politiregisterforskriften § 46-5.

Når departementet likevel har kommet til å sende forslag til ny hjemmel for opptak i politiloven § 10 a på høring, er dette først og fremst begrunnet i at politiet i de

aktuelle situasjonene uansett har hjemmel til å innbringe vedkommende etter politiloven § 8 nr. 3. Ved innbringelse kan personen som nevnt visiteres, og personen kan holdes tilbake i inntil 4 timer, jf. politiloven § 8 annet ledd. I de tilfellene der opptak av biometriske opplysninger vil føre til identifikasjon, vil opptak på stedet basert på samtykke kunne være et atskillig mindre inngrep for vedkommende enn innbringelse. Det må også kunne legges til grunn at opptak på stedet i disse situasjonene vil være i den registrertes interesse. Opptak er etter forslaget betinget av at personen samtykker.

Når politiet behandler opplysninger i medhold av politiloven, kommer politiregisterlovgivningen til anvendelse. Av politiregisterforskriften § 6-2 om behandling av opplysninger på grunnlag av samtykke følger at et samtykke skal være frivillig og uttrykkelig, og samtykkeerklæringen skal være skriftlig og undertegnet av den som gir samtykke. Et eventuelt muntlig samtykke skal nedtegnes av politiet på stedet. Politiet må videre gi tilstrekkelig informasjon om hva samtykket innebærer.

Forslaget åpner for behandling av biometriske opplysninger med det formål å entydig identifisere en person, og innebærer dermed behandling av særlige kategorier av opplysninger. Slik behandling er normalt regnet som særlig inngripende. I dette tilfellet er behandlingen av opplysningene begrenset til opptak og søk mot konkret angitte registre og systemer for identifiseringsformål. Den biometriske informasjonen skal slettes straks etter at søket er gjennomført.

Opptak er begrenset til situasjoner der personen kan innbringes etter politiloven § 8 nr. 3, og er videre betinget av et informert samtykke. Departementet erkjenner at det kan stilles spørsmål ved hvor frivillig samtykket er i en situasjon der alternativet er å bli innbrakt. Samtidig mener departementet at det ikke er aktuelt å åpne for å oppta biometriske opplysninger uten samtykke eller ved bruk av tvang. Selv om den enkelte kan oppleve at det er vanskelig å nekte samtykke, er det et reelt alternativ å heller bli innbrakt i tråd med politiloven § 8 nr. 3. For personen det gjelder vil innbringelse, der man kan bli tilbakeholdt i inntil fire timer, normalt oppleves som mer inngripende enn å avgi biometri som skal slettes straks det er gjennomført søk. Departementet vurderer derfor at personvernkonsekvensene av forslaget samlet sett vil være begrenset.

5.2 Forslag til endringer i utlendingsloven

5.2.1 Opptak av biometriske opplysninger ved manglende samarbeid om identitetsavklaring

Utlendingsloven § 100 første ledd hjemler opptak av biometrisk personinformasjon i form av ansiktsfoto og fingeravtrykk av en utlending blant annet dersom vedkommende ikke kan dokumentere sin identitet eller mistenkes for å oppgi uriktig identitet (bokstav a). Det forslås en endring i bokstav a for eksplisitt å dekke også tilfeller der vedkommende ikke medvirker til å klarlegge sin identitet i samsvar med §§ 21 og 83. Utlendingsloven § 21 er hjemmelen for alminnelig utlendingskontroll og pålegger utlendingen å vise legitimasjon og gi identifiserende opplysninger, mens § 83 omhandler en utlendings møte- og opplysningsplikt for å medvirke til avklaring av identitet.

Det vurderes i tillegg at bestemmelsen ikke tydelig nok reflekterer at hjemmelen for opptak av biometriske opplysninger også gjelder når det ikke kan stadfestes om personen det gjelder er utenlandsk statsborger grunnet personens manglende evne eller vilje til å identifisere seg. Departementet foreslår et nytt annet ledd i utlendingsloven § 100 hvor det presiseres at første ledd bokstav a også gjelder når det er usikkert om personen er utlending. Endringen er bare en klargjøring av gjeldende regelverk, og er ikke ment å innebære noen utvidelse av adgangen til å oppta biometriske opplysninger.

5.2.2 Bruk av biometriske opplysninger ved søk mot EES

Departementet foreslår videre en endring i utlendingsloven § 100 femte ledd for at biometriske opplysninger opptatt med hjemmel i bestemmelsen også skal kunne brukes til søk mot EES-systemet i tråd med EES-forordningen (forordning (EU) 2017/2226) artikkel 26, 27 og 35. Forordningen er i sin helhet tatt inn og gjort gjeldende som norsk lov gjennom grenseloven § 8 første ledd nr. 2. Forslaget innebærer ingen utvidelse av adgangen til å oppta biometriske opplysninger, men innebærer en viss utvidelsen av bruken av opplysningene.

Som ledd i personkontroll for å verifisere identitet og lovlig innreise og opphold i Norge, kan innvandringsmyndighetene foreta et søk med biometriske opplysninger etter artikkel 26 i EES-forordningen. Grensemyndighetene eller innvandringsmyndighetene kan i tillegg foreta søk med biometriske opplysninger for å identifisere en person som kan ha vært registrert med en annen identitet tidligere eller som ikke lenger fyller vilkårene for innreise eller opphold på medlemsstatenes territorium, jf. artikkel 27.

Det følger videre av slettereglene i EES-forordningen artikkel 35 nr. 6 at en persons individuelle saksmappe, de tilknyttede inn- og utreiseregistreringer og eventuelle tilknyttede registreringer om nektet innreise skal slettes fra inn- og utreisesystemet umiddelbart og under alle omstendigheter senest fem virkedager regnet fra den datoen tredjelandsborgeren er innvilget langtidsvisum, oppholdstillatelse eller statsborgerskap i en medlemsstat. Sletteplikten etter artikkel 35 innebærer at det i de nevnte tilfeller vil måtte foretas systematiske søk mot EES. Utlendingsmyndighetene vil ikke ha kjennskap til hvorvidt en tredjelandsborger har opplysninger registeret i EES uten å foreta systematiske søk i EES ved innvilgelse av søknader i saker som nevnt over.

Plikten til å slette opplysningene innen fem virkedager tilsier at sletteprosessen automatiseres. Det følger også av EES-håndboken at det skal foretas en automatisk sletting av opplysninger.

For å sikre korrekt sletting av opplysninger tilknyttet riktig person ved hjelp av automatiserte løsninger, anses det nødvendig å gjøre søk med alfanumeriske og biometriske opplysninger.

GDPR artikkel 6 nr. 4 gir et snevert handlingsrom for bruk av biometriske opplysninger utover det umiddelbare formålet de er innsamlet for. Biometriske opplysninger opptatt med hjemmel i utlendingsloven § 100 er samlet inn for identifisering og verifisering av identitet ved søknad om oppholdstillatelse og utlendingskontroll. Formålet er i så måte sammenfallende med EES-forordningen artikkel 26 og 27, og etter GDPR kreves det derfor ingen særlig hjemmel for å

gjennomføre slike søk etter artikkel 26 og 27 med biometriske opplysninger opptatt etter utlendingsloven § 100.

Derimot har bruk av opplysningene for å søke og slette opplysninger i EES etter artikkel 35 et noe annet – men etter departementets syn beslektet – formål enn det opprinnelige formålet de ble innhentet for etter utlendingsloven § 100. Hensynet til å ivareta EES-forordningens sletteregler, som i seg selv ivaretar personvernformål, er imidlertid legitimt og tungtveiende. Departementet mener derfor det er behov for en hjemmel for bruk av biometriske opplysninger i forbindelse med søk i EES for å oppfylle slettefristene i EES-forordningen art. 35 nr. 6.

Det kan i sammenheng med lovforslagene nevnes at utlendingsloven § 100 femte ledd nylig ble endret for å gi en uttrykkelig hjemmel for bruk av biometriske opplysninger for behandling i SIS-registeret. Endringen trådte i kraft 7. mars 2023. I proposisjonen, Prop. 226 L (2020-2021) s. 21, uttalte departementet at «[s]elv om ordlyden i utlendingsforskriften § 17-7 a kan tolkes slik at den gir hjemmel for at innsamlede opplysninger i utlendingssakene kan gjenbrukes for registrering i SIS, finner departementet det mest hensiktsmessig å forankre en tydelig hjemmel for slik gjenbruk av biometriske opplysninger i nytt fjerde ledd i utlendingsloven § 100».

I motsetning til registering i SIS, vil ikke søkene mot EES innebære at biometriske opplysninger opptatt i medhold av utlendingsloven § 100 første ledd registreres i EES. Det er imidlertid ikke helt klart i hvilken grad utlendingsforskriften § 17-7 a dekker behandling av biometriske opplysninger som beskrevet i tilfellene over.

Departementet mener den foreslåtte hjemmelen er forenlig med GDPR artikkel 9 nr. 2 bokstav g, som tillater behandling av biometriske opplysninger med det formål å entydig identifisere en fysisk person når behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av medlemsstatenes nasjonale rett. De personvernrettslige hensynene sletteregelen i EES-forordningen 35 skal ivareta, utgjør etter departementets syn en viktig allmenn interesse som kan begrunne behandling av biometriske opplysninger. Departementet vurderer i tillegg at behandlingen står i et rimelig forhold til det mål som søkes oppnådd, da formålet med søket nettopp er å sikre at opplysninger om rett person slettes fra EES. Videre vurderes det at kravet til at behandlingen skal være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser, er oppfylt. Som nevnt innebærer ikke forslaget at opplysningene vil bli registrert i EES. Bruk av allerede registrerte biometriske opplysninger for å sikre at personen slettes i EES vil være en fordel for den registrerte, og departementet kan ikke se at slik bruk har noen personvernmessige ulemper.

Departementet foreslår etter dette en uttrykkelig hjemmel for bruk av biometriske opplysninger opptatt med hjemmel i utlendingsloven § 100 for behandling av opplysninger etter EES-forordningen.

6 Økonomiske og administrative konsekvenser

Interoperabilitetsforordningene medfører at politiet og utlendingsmyndighetene må gjennomføre vesentlige tekniske systemendringer for å kunne knytte seg til den systemoverbyggende løsningen for interoperabilitet mellom de ulike

felleseuropeiske informasjonssystemene som er omfattet. Interoperabilitetsløsningen innebærer blant annet nasjonal tilrettelegging for etableringen av en felles søkeportal (ESP), en felles biometrisk sammenligningstjeneste (sBMS), et felles identitetsregister (CIR) og et system for varsler ved mistanke om at en person har flere eller falske identiteter (MID).

For dette arbeidet har EU fastsatt en felles fremdriftsplan med felles milepæler, med krav til samtidig implementering for alle Schengen-medlemslandene. Etterlevelse av rettsaktene krever at en rekke løsninger i dagens systemer i politier og utlendingsforvaltningen må tilpasses og videreutvikles.

Innføring og utvikling av interoperabilitetssystemet vil påvirke arbeidsprosessene for flere ulike aktører på tvers av politiet og utlendingsforvaltningen. Endringene medfører blant annet at det ved kontroll av dokumenter og personer skal utføres automatiske søk som gjør oppslag i EU-systemene via en felles søkeportal, i tillegg til systemstøtten for å fange opp forsøk på bruk av falske identiteter og misbruk av ekte identiteter (impostere). Det er for gjennomføringen lagt til grunn at det ikke gjennomføres tiltak utover det som er strengt nødvendig for å innfri Norges EU/Schengen-forpliktelser.

Stortinget vedtok i forbindelse med behandlingen av Prop. 1 S (2022-2023) en felles kostnadsramme for Schengen IKT-systemene Interoperabilitet, SIS, VIS og Eurodac i politiet og UDI, hvor også kostnader til etterlevelse av interoperabilitetsforordningene inngår. Kostnadsrammen for prosjektporteføljen er 2 187 millioner kroner inkl. mva. (P85, 2023-kroner). Den forventede kostnaden for politiets og UDIs implementering er på hhv. 728 mill. kroner ekskl. mva. over perioden 2022-2025 for politiet, og 69,4 mill. kroner ekskl. mva. over perioden 2022-2024 for UDI (P50, 2023-kroner). Varige driftskostnader for interoperabilitetssystemet er for politiet anslått til om lag 91 mill. kroner ekskl. mva. fra og med 2026 (2023-kroner) og om lag 20 mill. kroner fra og med 2025 for UDI. Driftskostnadene er hovedsakelig knyttet til behov for opplæring, økte i ressurser for å håndtere en økt arbeidsmengde, og drift av IT-løsningene.

Det forventes at Norge kan benytte midler som mottas gjennom EUs grenseforvaltnings- og visumfinansieringsordning (BMVI-fondet) til utvikling av interoperabilitetssystemet. Størrelsen på bevilgningene fra fondet er p.t. uavklart.

Forslag fra regjeringen som krever budsjettendringer vil bli fremmet for Stortinget i de årlige budsjettfremleggene.

I tillegg pålegges Datatilsynet, som kompetent tilsynsmyndighet etter LED og GDPR, visse plikter etter interoperabilitetsforordningene. Departementet viser til pkt. 3.3.7 for omtale av tilsynsmyndighetenes tilsyns- og samarbeidsplikter etter artikkel 51 og 53. I tillegg skal Datatilsynet etter artikkel 24 nr. 4 som tilsynsmyndighet etter LED regelmessig, og senest hver sjette måned, kontrollere logger fra søk i CIR etter artikkel 22 for å forebygge, avsløre eller etterforske terrorhandlinger eller andre alvorlige straffbare forhold. Kontrollen er begrenset til å kontrollere om fremgangsmåten og vilkårene i artikkel 22 nr. 1 og 2 er oppfylt. Det er usikkert hvor omfattende tilsynsoppgaven etter forordningene i praksis vil vise seg å være. De økonomiske og administrative konsekvensene for Datatilsynet vil utredes nærmere.

7 Forslag til lov- og forskriftsendringer

7.1 Endringer i grenseloven

I lov 20. april 2018 nr. 8 om grensetilsyn og grensekontroll av personer (grenseloven) gjøres følgende endringer:

§ 8 første ledd skal lyde:

Følgende rettsakter gjelder som lov:

1. *Forordning* (EU) 2016/399 om bevegelsen av personer over grenser (grenseforordningen), som endret ved *forordning* (EU) 2017/2225, *forordning* (EU) 2017/458*, forordning* (EU) 2018/1240 artikkel 80, *forordning (EU) 2019/817 og (EU) 2021/1134*
2. *Forordning* (EU) 2017/2226 om etableringen av inn- og utreisesystemet (EES-forordningen), *som endret ved forordning (EU) 2019/817 og (EU) 2021/1134*
3. Rådsdirektiv 2004/82/EF om transportselskapers plikt til å fremsende opplysninger om passasjerer (API-direktivet)
4. *Forordning (EU) 2019/817 om opprettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer for grenser og visum og om endring av Europaparlaments- og rådsforordning (EF) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 og (EU) 2018/1861, Rådsvedtak 2004/512/EF og Rådsbeslutning 2008/633/JIS*
5. *Forordning (EU) 2019/818 om opprettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer for politisamarbeid og rettslig samarbeid, asyl og migrasjon, og om endring av forordning (EU) 2018/1726, (EU) 2018/1862 og (EU) 2019/816, som endret ved forordning (EU) 2021/1133.*

§ 25 nr. 11, 12 og ny 13 skal lyde:

11. bruk av teknisk overvåkingsutstyr, jf. § *23,*
12. gjennomføringen av rettsakter som nevnt i § 8 første ledd, blant annet om behandling av *opplysninger,*

13. gjennomføringen av forordning (EU) 2019/817 artikkel 20 og forordning (EU) 2019/818 artikkel 20.

7.2 Endringer i SIS-loven

I lov 17. juli 1999 nr. 66 om Schengen informasjonssystem (SIS) (SIS-loven) gjøres følgende endringer:

§ 1 skal lyde:

§ 1 *Gjennomføring av forordninger om Schengen informasjonssystem (SIS)*

Følgende forordninger gjelder som lov:

1. *Forordning* (EU) 2018/1862 om opprettelse, drift og bruk av Schengen-informasjonssystem (SIS) innenfor politisamarbeid og strafferettslig samarbeid, om endring og oppheving av rådsbeslutning 2007/533/JIS og om oppheving av europaparlaments- og rådsforordning (EF) nr. 1986/2006 og kommisjonsbeslutning 2010/261/EU (politisamarbeidsforordningen)*, som endret ved forordning (EU) 2019/818, (EU) 2021/1133 art. 3 og (EU) 2021/1134*

2. *Forordning* (EU) 2018/1861 om opprettelse, drift og bruk av Schengen-informasjonssystem (SIS) på området inn- og utreisekontroll, om endring av konvensjonen om gjennomføring av Schengen-avtalen og om endring og oppheving av forordning (EF) nr. 1987/2006 (grensekontrollforordningen), *som endret ved forordning (EU) 2019/817*

3. *Forordning* (EU) 2018/1860 om bruk av Schengen-informasjonssystem i forbindelse med retur av tredjestatsborgere med ulovlig opphold (returforordningen).

7.3 Endringer i utlendingsloven

I lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og dere opphold her (utlendingsloven) gjøres følgende endringer:

§ 9 a første ledd skal lyde:

Forordning (EU) 2018/1240 om etableringen av fremreisesystemet (ETIAS-forordningen*), som endret ved forordning (EU) 2019/817 og forordning (EU) 2021/1134,* gjelder som lov.

§ 100 første ledd bokstav a skal lyde:

a. ikke kan dokumentere sin *identitet, som* det er grunn til å mistenke for å oppgi uriktig identitet, eller som *ikke medvirker til å klarlegge sin identitet, jf. §§ 21 og 83,*

Nytt annet ledd skal lyde:

Bestemmelsen i første ledd bokstav a gjelder også for personer som det er usikkert om er utlending.

Nåværende annet til syvende ledd blir tredje til åttende ledd.

Nåværende femte ledd, fremtidige sjette ledd, skal lyde*:*

Biometrisk personinformasjon opptatt i medhold av første ledd kan brukes i forbindelse med registrering av returvedtak og innreiseforbud i SIS i medhold av SIS-loven §§ 7 og 8 og forordningene som nevnt i SIS-loven § 1 nr. 2 og nr. 3, samt artikkel 22 i forordningen om politisamarbeid som nevnt i SIS-loven § 1 nr.

1. *Biometrisk personinformasjon opptatt i medhold av første ledd kan også brukes for behandling etter forordning (EU) 2017/2226, jf. grenseloven § 8 første ledd.*

§ 102 første ledd skal lyde:

Forordning (*EF*) nr. 767/2008 om visuminformasjonssystemet VIS (VIS-forordningen), *endret ved forordning (EU) 2019/817 og forordning (EU) 2021/1134*, gjelder som lov. VIS fastsetter bestemmelser om lagring og deling av opplysninger mellom landene i Schengen-samarbeidet, om søkere og søknader om visum og oppholdstillatelser, via nasjonale brukergrensesnitt.

7.4 Endringer i politiloven

I lov 4. august 1995 nr. 53 om politiet (politiloven) skal ny § 10 a lyde:

§ 10 a *Opptak av biometriske opplysninger*

Politiet kan oppta biometriske opplysninger fra en person til identifiseringsformål når vilkårene for innbringelse etter § 8 nr. 3 er oppfylt og vedkommende samtykker. Opplysningene kan kun brukes til søk som angitt i artikkel 20 nr. 2 i forordning (EU) 2019/817, til søk som angitt i artikkel 20 nr. 2 i forordning (EU) 2019/818 og til søk i foto- og fingeravtrykkregisteret, jf. politiregisterloven § 13.

Før en person velger å avgi biometriske opplysninger til politiet etter første ledd, skal vedkommende underrettes om bruken av opplysningene og aktuelle handlingsalternativer. Bekreftelse på at opptaket er frivillig kan gis muntlig eller skriftlig. Muntlig bekreftelse skal nedtegnes av politiet på stedet.

Opplysningene skal straks slettes når søket er gjennomført.

Politiloven § 12 nytt sjette ledd skal lyde:

I forbindelse med en naturkatastrofe, en ulykke eller et terrorangrep kan politiet oppta biometriske opplysninger fra ukjente personer ute av stand til å legitimere seg og fra uidentifiserte menneskelige levninger. Opplysningene kan kun brukes for å fastslå vedkommendes identitet med søk som angitt i artikkel 20 nr. 4 i forordning (EU) 2019/817 og i artikkel 20 nr. 4 i forordning (EU) 2019/818 og til søk i foto- og fingeravtrykkregisteret, jf. politiregisterloven § 13. Opplysningene skal slettes straks søket er gjennomført.

7.5 Forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning

Ny forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning skal lyde:

Forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning etter forordning (EU) 2019-817 og (EU) 2019-818

§ 1 Interoperabilitet mellom informasjonssystemer

I rammeløsningen for interoperabilitet mellom EUs informasjonssystemer, er norske myndigheter tilknyttet inn- og utreisesystemet (EES), visuminformasjonssystemet (VIS), fremreisesystemet (ETIAS), Eurodac og Schengen Informasjonssystem (SIS).

§ 2 *Tilgang til felles identitetsregister (CIR) for identifiseringsformål*

Politiet kan søke i CIR for å identifisere en person i tråd med artikkel 20 nr. 1 til 3 i forordning (EU) 2019/817 og artikkel 20 nr. 1 til 3 i forordning (EU) 2019/818 for formål som angitt i forordningene artikkel 2 nr. 1 bokstav b og c. Slike søk kan gjøres når det innhentes biometriske opplysninger i medhold av straffeprosessloven § 160 og politiloven § 10 a.

Politiet kan søke i CIR i situasjoner som nevnt i artikkel 20 nr. 4 i forordning (EU) 2019/817 og artikkel 20 nr. 4 i forordning (EU) 2019/818 når det er innhentet biometriske opplysninger i medhold av politiloven § 12 sjette ledd.

§ 3 *Behandlingsansvar for informasjonssystemer som inngår i interoperabilitetsforordningene*

Når kompetente myndigheter behandler opplysninger i de av EUs informasjonssystemer som inngår i rammeløsningen for interoperabilitet, er

a. Kripos behandlingsansvarlig for behandlingen av opplysninger etter grensekontrollforordningen og politisamarbeidsforordningen, jf. SIS-loven § 4 første ledd
b. Utlendingsdirektoratet, Utlendingsnemnda, politiet som utlendingsmyndighet og utenrikstjenesten behandlingsansvarlig for deres respektive behandling av opplysninger om innreiseforbud etter grensekontrollforordningen art. 24 og etter returforordningen, jf. SIS-forskriften § 1 første ledd
c. Politidirektoratet behandlingsansvarlig for behandlingen av opplysninger etter EES-forordningen, jf. grenseforskriften § 1-6
d. Utlendingsdirektoratet behandlingsansvarlig for behandlingen av opplysninger etter EES-forordningen art. 35 nr. 6, jf. grenseforskriften § 1-6
e. Den nasjonale ETIAS-enheten ved Politiets utlendingsenhet behandlingsansvarlig for behandlingen av opplysninger det sentrale ETIAS-systemet etter ETIAS-forordningen art. 57 nr. 2, jf. utlendingsforskriften § 3-3 b første ledd
f. Utlendingsdirektoratet behandlingsansvarlig for behandling av opplysninger etter ETIAS-forordningen i forbindelse med egen klagebehandling, jf. utlendingsforskriften § 3-3 b andre ledd

g. myndigheter med ansvar for behandling av søknader om visum, D-visum og oppholdstillatelse behandlingsansvarlige for deres respektive behandling av opplysninger etter VIS-forordningen, jf. utlendingsforskriften § 18-7
h. Utlendingsdirektoratet behandlingsansvarlig for behandling av opplysninger etter Eurodac-forordningen, jf. utlendingsforskriften § 18-5
i. Kripos er behandlingsansvarlig for behandlingen av personopplysninger som skal brukes for å forebygge, oppdage og etterforske i samsvar med Eurodac-forordningen artikkel 1 nr. 2, jf. utlendingsforskriften § 18-5

§ 4 *Behandlingsansvar for opplysninger i interoperabilitetskomponentent sBMS (shared Biometric Matching Service)*

Behandlingsansvarlig for behandling av opplysninger i Eurodac, SIS, EES og VIS som nevnt i § 3, er behandlingsansvarlig for sine respektive biometriske opplysninger i sBMS i samsvar med interoperabilitetsforordningene art. 40 nr. 1.

§ 5 *Behandlingsansvar for opplysninger i interoperabilitetskomponentent CIR (Common Identity Repository)*

Behandlingsansvarlig for behandling av opplysninger i Eurodac, ETIAS, EES og VIS som nevnt § 3, er behandlingsansvarlig for sine respektive opplysninger i CIR i samsvar med interoperabilitetsforordningene art. 40 nr. 2.

§ 6 *Behandlingsansvar for opplysninger i interoperabilitetskomponentent MID (Multiple Identity Detector)*

Ved behandling av lenker i MID i henhold til interoperabilitetsforordningene kapittel V, vil følgende myndigheter være behandlingsansvarlig for endringer og tilføyelser i identitetsbekreftelsesmappen (Identity Confirmation File), jf. interoperabilitetsforordningene art. 40 nr. 3:

a. Kripos er behandlingsansvarlig etter melding til SIS
b. Politidirektoratet er behandlingsansvarlig etter melding til EES
c. Den nasjonale ETIAS-enheten er behandlingsansvarlig etter melding til ETIAS
d. myndigheter med ansvar for behandling av søknader om visum, D-visum og oppholdstillatelse er behandlingsansvarlige for deres respektive meldinger til VIS
e. Utlendingsdirektoratet og Kripos er behandlingsansvarlig for deres respektive meldinger til Eurodac

§ 7 Ikrafttredelse

Forskriften trer i kraft når departementet bestemmer.

7.6 Forslag til endringer i grenseforskriften

I forskrift 29. april 2022 nr. 665 om grensetilsyn og grensekontroll av personer (grenseforskriften) skal ny § 1-6 lyde:

§ 1-6 *Behandlingsansvarlige for inn- og utreisesystemet (EES - Entry Exit System), jf. grenseloven § 8*

Politidirektoratet er behandlingsansvarlig for behandling av personopplysninger i inn- og utreisesystemet (EES – Entry Exit System).

Utlendingsdirektoratet er behandlingsansvarlig for behandlingen av opplysninger etter EES-forordningen art. 35 nr. 6.

7.7 Forslag til endringer i utlendingsforskriften

I forskrift 15. oktober 2009 nr. 1286 om utlendingers adgang til riket og deres opphold her (utlendingsforskriften) skal ny § 3-3 b lyde:

§ 3-3 b *Behandlingsansvar for ETIAS (European Travel Information and Authorisation System)*

Den nasjonale ETIAS-enheten ved Politiets utlendingsenhet er behandlingsansvarlig for behandling av personopplysninger i det sentrale ETIAS-systemet, jf. ETIAS-forordningen artikkel 57 nr. 2.

Utlendingsdirektoratet er behandlingsansvarlig for personopplysninger for egne formål i forbindelse med klagebehandling.