Utlendingsdirektoratet
Norwegian Directorate
of Immigration

Justis og beredskapsdepartementet

Deres ref: **Vår ref:** 23/46049-6 **Dato:** 06.02.24

UDIs innspill til høringsnotat om implementering i norsk rett av forordningene (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer m m.

Utlendingsdirektoratet (UDI) viser til Justis- og beredskapsdepartementets høringsbrev av 21. desember 2023, med tilhørende høringsnotat om forslag til lov- og forskriftendringer for å gjennomføre i norsk rett forordningene om opprettelse av en ramme for interoperabilitet mellom Schengen/EU-informasjonssystemer (jf. forordning (EU) 2019/817 for grense og visum og forordning (EU) 2019/8118 for politisamarbeid, asyl og migrasjon.

Høringsfristen er satt til 8. februar.

1. Generelle merknader

De nye forordningene utgjør en del av det såkalte Schengen-acquis, og forplikter Norge som assosiert medlemsland. Departementet foreslår at forordningene inkorporeres i grenseloven, og gjennom regler i ny forskrift om interoperabilitet (heretter IO-forskriften). Det foreslås også noen nye hjemler i politi- og utlendingsloven som omhandler biometriske data.

I vårt svar til departementet har vi valgt å fokusere særlig på bestemmelsene i (EU) 2019/817 om grense og visum. Bakgrunnen for dette er at interoperabilitets-forordningene stort sett har likelydende bestemmelser. Vi har også valgt å benytte betegnelsen EU/Schengen-systemer når vi omtaler de nye og reviderte informasjonssystemene. Vi omtaler også interoperabilitetsforordningene som IO-forordningene.

Som departementet er kjent med, er det allerede betydelig forsinkelser med igangsettelsen av de nye EU/Schengen-systemene, EES og ETIAS. Dette påvirker også tidspunktet for den fremtidige interoperabiliteten mellom disse og eksisterende informasjonssystemer. Den opprinnelige planen la opp til at

Innspurten 11D NO-0663 Oslo
Postboks 2098 Vika NO-0125 Oslo
+47 23 35 15 00

udi@udi.no, www.udi.no
Bankkontonummer 7694 05 10712
Organisasjonsnummer 974 760 746
Saksbehandler: Catherine Anne Olga Marie de Coster

interoperabilitet skulle være på plass innen utgangen av 2024. Ny tidsplan vedtatt i Rådet i oktober 2023 tilsier at dette ikke vil skje før slutten av 2026.

Interoperabiliteten skal gjelde for de ulike EU/Schengen-systemene; EES, ETIAS, VIS, SIS og Eurodac. Forordningene som hjemler systemene, er gjennomført på ulik måte i nasjonal lovgivning. De tjener ulike formål, herunder migrasjon og/eller sikkerhet. Overordnet mener UDI at det vil være en fordel om regelverket som legger en ramme for utveksling av informasjon mellom systemene forankres i en egen lov med en detaljert forskrift. Vi viser her til at informasjonsutveksling på de ulike områdende grenseforvaltning, migrasjon, rettshåndhevelse og bekjempelse av alvorlig kriminalitet og terrorisme vil falle under samme paraply.

Som sentral utlendingsmyndighet er det avgjørende for UDI at implementeringen av IO-forordningene tydelig fastslår hvilke rettigheter og plikter som tilfaller de ulike utlendingsmyndighetene, grensemyndighetene, politi- og retthåndshevelses-myndighetene, samt personer hvis personopplysninger er lagret i ett eller flere EU/Schengen-systemer.

Hensynet til personvern er en sentral del av forordningene, og de inneholder bestemmelser som konkretiserer kravene i personvernforordningen (GDPR og/eller LED - Law Enforcement Directive).

I det følgende vil UDI gjøre rede for gjennomføring av IO-forordningene i norsk rett (punkt 2), personvern (punkt 3), kommentar til høringsnotatet (punkt 4), UDIs forslag til IO-lov og IO-forskriftsbestemmelser (punkt 5) og økonomiske og administrative konsekvenser (punkt 6). Endelig presenterer vi vårt forslag til endringer i de foreslåtte bestemmelsene (punkt 7).

2. Gjennomføring av IO-forordningene i norsk rett

Departementet foreslår at IO-forordningene blir gjennomført ved inkorporasjon, på samme måte som forordningene som ligger til grunn for de andre EU/Schengen-systemene.

UDI er positive til forslaget om inkorporasjon, ved at regelverket gjennomføres i norsk rett uten omskrivinger. Vi mener imidlertid at det er et behov for å regulere avgjørende bestemmelser i en egen IO-lov, eventuelt mer utfyllende i den foreslåtte IO-forskriften. Vi vil også gi innspill til bestemmelsene slik de er foreslått i høringsnotatet.

UDI stiller spørsmål til om grenseloven er riktig sted for å hjemle IO-forordningene. Dersom IO-forordningene hjemles i en egen lov, tilsvarende SIS-loven, er UDI av den oppfatning at ansvarsfordelingen mellom de ulike oppgavene på utlendingsfeltet, grensekontrollen og politi- og rettshåndhevende myndigheter, blir tydeligere. Vi mener også at dette vil være en fordel for brukere ettersom regelverket er meget komplisert. Vi viser til at flere myndigheter er involvert og at privatpersoner er registrert med sensitive data i ett eller flere systemer. Med en egen lov kan både utlendings-, grense- og politiloven henvise til det IO-regelverket for sine respektive oppgaver.

IO-forordningene kan sammenliknes med en paraply som holder de ulike informasjonssystemene sammen. De regulerer også utveksling og deling av data etter tilgangen for de autoriserte brukerne i de aktuelle kompetente myndighetene. UDI mener derfor at IO-forordningene, og ikke minst definisjonen av de ulike

komponenter/formål/virkeområde, samt bestemmelsene om personvern og databehandleransvar, bør reguleres i en egen lov.

En IO-lov kan utarbeides på tilsvarende måte som den nye SIS-loven. UDI mener at den bør være mer detaljert og mer oversiktlig enn det departementet foreslår regulert på ulike steder i lov og forskrift. UDI viser til implementering via inkorporering av grenseforordningen, SIS-forordningene, samt EUs personvernforordning (GDPR) som eksempler. Viktige bestemmelser i samtlige forordninger er tydeliggjort i lov eller forskrift:

- Lov om grensetilsyn og grensekontroll av personer (grenseloven) som hjemler grenseforordningen, jf. § 8. Loven har ulike bestemmelser som gjenspeiler forordningen, se eksempelvis § 15 om gjennomføring av inn- og utreisekontroll, samt kapittel 5 om behandling av opplysninger og taushetsplikt.
- SIS-loven med eksempelvis kapittel 2 om «Behandlingsansvar, informasjonssikkerhet og internkontroll», kapittel 3 om «Behandling av opplysninger» og kapittel 4 om «Tilgang, utlevering og taushetsplikt».
- Lov om behandling av personopplysninger (personopplysningsloven) er også et eksempel på en viktig EU/EØS-forordning (GDPR) som er blitt gjennomført i norsk rett via inkorporasjon samtidig som den inneholder en rekke bestemmelser som supplerer reglene i forordningen.

I sitt høringsnotat av 7. juni 2023 om endringer i visuminformasjonssystemet (VIS) og tilknytning av VIS til andre europeiske informasjonssystemer, skrev departementet på side 7:
"Justis- og beredskapsdepartementet er også i ferd med å utarbeide forslag til en ny lov om interoperabilitet mellom felleseuropeiske informasjonssystemer for grensepassering, utlendingsforvaltning og politisamarbeid med tilhørende forskrift, hvor interoperabilitetsforordningene vil bli inkorporert".

I foreliggende høringsnotat fremgår det imidlertid at departementet *ikke* finner det «*hensiktsmessig at det gis en egen lov om interoperabilitet. Det har samtidig vist seg noe vanskelig å innpasse gjennomføringen av forordningene i en eksisterende lov*», side 11. Dette blir imidlertid ikke begrunnet ytterligere. Vi viser her til at departementet:

- ikke har kommenterer konsekvensene for de ulike brukerne i utlendingsforvaltningen slik som ansvar, oppgaver, rettigheter i henhold til de nye forordningene.
- ikke drøfter ulike løsninger og alternativer for implementering av forordningene i norsk rett, eller begrunnelser for den løsningen som er valgt.

UDI viser for øvrig til at Sveits, et annet Schengen assosiert medlemsland, har valgt en implementeringsform som synliggjør *viktigheten og konsekvensene av* interoperabilitet mellom EU/Schengen-systemer: Ordonnance sur l'interopérabilité des systèmes d'information Schengen-Dublin (Ordonnance N-IOP) (admin.ch)

Under punkt 5 redegjør vi nærmere for innholdet i lov- og forskriftsbestemmelser.

3. Særlig om personvern

3.1 Overordnet om systematikken i reguleringen av personvern

Bestemmelsene om personvern og behandlingsansvar knyttet til EU/Schengen-systemene er regulert ulikt i norsk rett. Regelverket fremstår som fragmentert og

lite tilgjengelig, særlig for den registrerte. UDI er av den oppfatning at regelverket knyttet til personvern og behandlingsansvar bør fremgå av en IO-lov og at bestemmelsene utformes med lik systematikk. Behandling av store mengder personopplysninger med tilgang for flere etater for ulike formål og med en tettere integrasjon mellom systemer, skjerper kravene til at forordningene implementeres på en klar og brukervennlig måte.

UDI stiller spørsmål ved om de foreslåtte endringene i grenseloven, og en kort IO-forskrift, sikrer den nødvendige tilgjengeligheten. Forskriften slik den er foreslått har også et videre virkeområde enn grenseloven og er heller ikke utgangspunkt for utlendingsmyndighetenes virksomhet. Det fremstår derfor lite tydelig og brukervennlig at IO-forordningene skal hjemles der. Et klart og tilgjengelig nasjonalt regelverk blir desto viktigere grunnet de generelle utfordringene med forordningers struktur, språk og detaljnivå som avviker fra norsk lovgivningsteknikk.

Dersom departementet ikke ønsker en IO-lov, foreslår UDI ytterligere presiseringer i forskriftsteksten. Se våre kommentarer i punkt 3.2 nedenfor.

3.2 Regulering av behandlingsansvaret (jf. IO-forskrift § 3)

Behandlingsansvar for SIS, VIS, Eurodac og de kommende EES og ETIAS er i dag regulert ulikt i norsk regelverk, noen på lov og forskrifts nivå, andre kun i instruks (EES og ETIAS).

En tydelig plassering av behandlingsansvaret i regelverket er å foretrekke. UDI støtter derfor departementets forslag der de ulike offentlige aktørene ilegges et selvstendig behandlingsansvar for behandling av personopplysninger til egne formål. En slik regulering vil også være i tråd med Personvernkommisjonens anbefalinger. Der deling av personopplysninger inngår som en del av et større samarbeid mellom forvaltningsorganer, og hvor uklarhet kan medføre alvorlige personvernkonsekvenser, anbefales det at ansvarsfordelingen i større grad lov- eller forskriftsfestes (NOU 2022 nr. 11 pkt. 1.3.2).

UDI er av den oppfatning at det er viktig å få ryddet opp og klargjort behandlingsansvaret for eksisterende systemer, og mener at implementeringen av IO-forordningen er en god mulighet. Vi ser samtidig at dagens fragmenterte regelverk og uklarheter rundt behandlingsansvar for de underlagte systemene videreføres i departementets forslag. Eksempelvis ser vi at det i SIS-loven angis at utlendingsmyndighetene er behandlingsansvarlige, mens det i forslaget til § 3 b angis spesifikke deler av utlendingsmyndighetenes ansvar. Vi gjør samtidig oppmerksom på at utenrikstjenesten ikke er nevnt i SIS-loven. UDI er av den oppfatning at angivelsen av behandlingsansvaret bør være mest mulig presist, til hvert konkret organ. I departementets forslag er det ikke angitt hvem som er behandlingsansvarlig når politiet opptrer som utlendingsmyndighet, som etter instruks er Politidirektoratet, og heller ikke hvem som er behandlingsansvarlig når utenrikstjenesten behandler personopplysninger, som etter utlendingsforskriften § 17-7b er Utenriksdepartementet.

Det er krevende å angi behandlingsansvaret før vi vet hvordan systemene implementeres. Ordlyden i forslagets §§ 4, 5 og 6 er ikke tilstrekkelig klar på hva behandlingsansvaret innebærer. UDI mener det er uklart hva behandlingsansvaret omfatter og hva den enkelte myndighet er behandlingsansvarlig for. Vi mener dette må klargjøres.

UDI er av den oppfatning at ordlyden i § 3 bør harmoniseres med ordlyden i utlendingsforskriften § 17-7 b slik at det refereres til behandling av personopplysninger for egne formål.

Vi kan ikke se at § 3 i forslaget til IO-forskrift klargjør tydelig nok de kompetente utlendingsmyndighetene under bokstav g. Her bør det angis hvilken etat som har ansvar for behandling av disse søknadene. Vi gjør også oppmerksom på at IO-forordningene skiller behandling av visum som hører under definerte visummyndigheter (*visa authorities*) iht. Schengen-regelverket, og behandling av søknader om opphold og D-visum som er et nasjonalt anliggende og hører under utlendingsmyndigheter (*migration authorities*) som den enkelte medlemstat selv må definere. Vi kommer tilbake til dette under pkt. 5.

3.3 GDPR eller LED?

Behandlingen av personopplysninger reguleres av personvernforordningen (GDPR) eller politiregisterloven (LED), avhengig av om det er forvaltningsoppgaver eller oppgaver som hører under rettshåndhevende myndigheter. UDI savner mer informasjon i høringsnotatet om i hvilke tilfeller personvernforordningen og politiregisterloven (LED) kommer til anvendelse. Dette bør klargjøres av departementet i arbeidet med implementeringen, da dette også vil kunne være førende for hvem som kan ilegges et behandlingsansvar og gir den registrerte noe ulike rettigheter. Dersom det ikke presiseres tydelig nok i forskriften vil det være krevende både for den registrerte og de mange brukerne som skal anvende regelverket.

3.4 Vurdering av personvernkonsekvenser

Den fremtidige interoperabiliteten mellom eksisterende og nye informasjons-systemer vil åpne for raskere og sikrere utveksling av informasjon om de registrerte.

Vi kan ikke se at departementet i sitt høringsnotat har vurdert konsekvensene for de registrertes rettigheter og forpliktelser iht. de nye forordningene. Rettsaktene legger opp til omfattende deling og sammenstilling av personopplysninger.

De vide hjemlene for inngrep i den registrertes personvern tilsier at konsekvensene i enda større grad burde vært underlagt en konkret vurdering i høringsnotatet. Dette ble påpekt av flere høringsinstanser under høringen om "Endringer i visuminformasjonssystemet (VIS) og tilkobling til andre europeiske informasjonssystemer".

Advokatforeningen bl.a. har kommentert følgende «*På bakgrunn av det vi oppfatter som manglende systematisk vurdering av de personvernmessige konsekvensene av forslagene i denne høringen, vil Advokatforeningen understreke behovet for at lovgiver i det videre arbeidet med gjennomføringen av disse reglene, herunder i det videre arbeidet med ny lov og forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for grensepassering, utlendingsforvaltning og politisamarbeid, sørger for å gjennomføre tilstrekkelige vurderinger av konsekvensene for individenes rettigheter og friheter på dette området» (side 2, pkt.4).*

Vi kan heller ikke se at det er foretatt noen vurderinger av hvorvidt den registrertes rettigheter bør fremkomme særskilt i norsk lovgivning. Også de ulike frister for lagring av data i informasjonssystemene burde med fordel gjenspeiles i det nye regelverket.

UDI foreslår at deler av kapittel VII som gjelder de registrertes rett til informasjon, retting, sletting, erstatning, samt rollen til tilsynsmyndighetene kommer frem i norsk lovgivning. Her mener vi det bør sees hen til SIS-loven, og systematikken

der. Departementet bør videre angi hvilken kompetent myndighet den registrerte kan ta kontakt med etter artikkel 48 nr.1.

4. Kommentarer til høringsnotatet

Kapittel 1 i IO-forordningene angir alminnelige bestemmelser om formål, mål, virkeområde og definisjoner. Formålet er å opprette en ramme for å sikre interoperabilitet mellom EU/Schengen-systemene. Vi mener imidlertid at dette i liten grad fremkommer av foreslått regelverk. Vi foreslår derfor at forordningenes art. 1 og 2 gjenspeiles og tas inn i sin helhet.

Videre bør IO-forordningen § 1 presisere *hvilke* norske myndigheter som blir tilknyttet interoperabilitet. De norske myndighetene utgjør grense-, utlendings- og politimyndigheter.

I høringsnotatet står det noe om de ulike komponenter som inngår i interoperabilitetsløsningen, dvs. ESP (jf. IO-forordningene kapittel 2), sBMS (jf. IO-forordningene kapittel 3), CIR (jf. IO-forordningene kapittel 4) og MID (jf. IO-forordningene kapittel 5). De ulike komponentene er imidlertid ikke nærmere definert i IO-forskriften og heller ikke med sine respektive formål.

Av hensyn til rettsikkerheten er det nødvendig å presisere i lov eller forskrift:

- for ESP at det skal opprettes ulike profiler for hver kategori av brukere av portalen. De ulike profilene 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.
- for sBMS at den felles biometrisk sammenligningstjeneste har til formål å forenkle identifiseringen av en person som er registrert i flere databaser ved bruk av en felles teknologisk sammenligningsløsning.
- for CIR at det felles identitetsregisteret gir den kompetente grense- og utlendingsmyndigheten tilgang for manuell verifisering av forskjellige identiteter når det oppstår tvil om den registrertes identitet og at politimyndigheter/LEA under visse forhold også kan få tilgang (bl.a. for å avverge alvorlig kriminalitet)
- for MID at den fleridentitetsdetektoren skal opprette og lagre identitets-bekreftelsesmapper 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.

I § 3 g i IO-forskriften har departementet en felles bestemmelse for behandlingsansvaret for visum, oppholdstillatelse og D-visum. Vi viser til vår redegjørelse i punkt 3.2 om at visum er et Schengen-anliggende. Vi foreslår derfor at bestemmelsen deles i to. Det vil bedre reflektere de siste og viktige endringene i VIS-forordningen som ble innført ved forordningene (EU) 2021/1133 og 1134 (VIS-revised) om utveksling av informasjon mellom medlemsstatene om visum for korttidsopphold (C-visum), visum for langtidsopphold (D-visum) og oppholdstillatelse.

Departementet fremholder også at interoperabilitet «*vil gjelde på Jan Mayen, men ikke på Svalbard*», se punkt 4.1. Samtidig bør det presiseres at Sysselmesteren likevel har fått delegert ansvar på visumfeltet (jf. utl. § 13 og utf. § 3-14) og har tilgang til både VIS og SIS, samt EES når dette produksjonsettes.

5. Forslag til IO- lov eller IO-forskriftsbestemmelser

Informasjonshensyn og rettssikkerhetshensyn taler for at IO-forordningene reguleres i lov med utfyllende bestemmelser som synliggjør de særlige reglene som forordningene oppstiller. IO-loven bør derfor ha en avslutningsbestemmelse som åpner for at departementet kan gi ytterligere presiseringer i forskrift.

UDI anbefaler at en større del av kapittel 1 om «Alminnelig bestemmelser» i IO-forordningene inkluderes i egen lov og/eller i IO-forskrift:

- Artikkel 1 formål: IO-forskriften § 1 gjenspeiler kun pkt. 1 til artikkel 1 i IO-forordningene. Vi mener at også pktene 2 til 5 bør være med:

  2. *Denne rammen skal omfatte følgende interoperabilitetskomponenter: (a) en europeisk søkeportal (ESP), (b) en felles biometrisk sammenlignings-tjeneste (sBMS), (c) et felles identitetsregister (CIR), (d) en fleridentitetsdetektor (MID).*

  3. *Ved denne forordning fastsettes også bestemmelser om krav til opplysningenes kvalitet, et universelt meldingsformat (UMF), et sentralt register for rapportering og statistikk (CRRS) og om ansvaret til medlemsstatene og Det europeiske byrå for driftsforvaltning av store IT-systemer innenfor området frihet, sikkerhet og rettferdighet (eu-LISA) når det gjelder utformingen, utviklingen og driften av interoperabilitets-komponentene.*

  4.Ved denne forordning tilpasses også framgangsmåtene og vilkårene for at de utpekte myndighetene og Den europeiske unions byrå for politisamarbeid (Europol) skal få tilgang til EES, VIS, ETIAS og Eurodac for å forebygge, avsløre eller etterforske terrorhandlinger eller andre alvorlige straffbare forhold.

  5. *Ved denne forordning fastsettes også en ramme for verifisering av personers identitet og for identifisering av personer.*

- Artikkel 2 mål:

  2. Ved å sikre interoperabilitet har denne forordning følgende mål
  (a) forbedre formålstjenligheten og effektiviteten av inn- og utreisekontrollene ved de ytre grensene,
  (b) bidra til å forebygge og bekjempe ulovlig innvandring,
  (c) bidra til et høyt sikkerhetsnivå innenfor frihet, sikkerhet og rettferdighet i Unionen, herunder opprettholde den offentlige sikkerhet og den offentlige orden og ivareta sikkerheten på medlemsstatenes territorier,
  (d) forbedre gjennomføringen av den felles visumpolitikken,
  (e) bistå ved gjennomgåelsen av søknader om internasjonal beskyttelse,
  (f) bidra til å forebygge, avsløre og etterforske terrorhandlinger og andre alvorlige straffbare forhold,
  (g) gjøre det enklere å identifisere ukjente personer ute av stand til å legitimere seg eller uidentifiserte menneskelige levninger ved en naturkatastrofe, en ulykke eller et terrorangrep,

  2. *Målene i nr. 1 skal oppnås ved å*

  (a) sikre korrekt identifisering av personer,

(b) bidra til å bekjempe identitetsbedrageri,

(c) forbedre opplysningenes kvalitet og harmonisere kvalitetskravene til opplysninger som lagres i EU informasjonssystemene, samtidig som kravene til behandling av opplysninger i de rettslige instrumentene for de enkelte systemene og standardene og prinsippene for personvern, oppfylles,

(d) forenkle og støtte medlemsstatenes tekniske og praktiske implementering av EU-informasjonssystemer,

(e) styrke og forenkle de vilkår for datasikkerhet og personvern som regulerer de respektive EU-informasjonssystemene, og gjøre dem mer enhetlige, uten at det påvirker det særlige vernet og de særlige beskyttelsestiltakene som gjelder for visse kategorier av opplysninger,

(f) effektivisere vilkårene for utpekte myndigheters tilgang til EES, VIS, ETIAS og Eurodac, og samtidig sikre nødvendige og forholdsmessige vilkår for denne tilgangen,

(g) støtte formålene med EES, VIS, ETIAS, Eurodac, SIS og ECRIS-TCN.

I tillegg og som nevnt ovenfor foreslår UDI at det hjemles i IO-lov eller forskrift deler av kapittel VII om personvern som gjelder de registrertes rett til informasjon med tilgang, retting og eventuelt sletting, erstatning, samt rollen til tilsynsmyndighetene komme frem i norsk lovgivning.

6. Administrative og økonomiske konsekvenser av IO

Innføring av interoperabilitet vil føre til en økning av driftskostnadene i UDI. Interoperabilitet vil kreve flere interne årsverk både hos IT og på fagsiden, samt økte utgifter til forvaltning og drift av IKT-systemer**.** Utgiftene knyttet til forvaltning, drift og vedlikehold omfatter:

- Teknisk drift og forvaltning av IT-løsningene
- Deltakelse i ulike ekspertgrupper, arbeidsgrupper og prosjektlederfora i Schengen.
- Økt saksmengde på prosessområdene i UDI som følge av verifisering av identitetsavvik samt merarbeid knyttet til avledede saker, inkludert tilbakekall.

Det er bevilget en felles kostnadsramme ifm. innføring av SIS Recast, Interoperabilitet, VIS Revised og Eurodac Recast for perioden 2022-2024. Gjennomføringen av tiltakene er betydelig forsinket og er per dagsdato planlagt gjennomført innen 2027.

UDI har i konsekvensjustert budsjett 2025 spilt inn et økt kostnadsbehov til interne årsverk i UDI med ansvar for gjennomføringen av tiltakene i den forlengede programperiode (2025 – 2027).

7. Forslag til endringer i de foreslåtte bestemmelser
(høringsnotat pkt. 7)

7.1. Utlendingsloven § 100

Første ledd bokstav a presiserer «*ikke kan dokumentere sin identitet, som det er grunn til å mistenke for å oppgi uriktig identitet, eller som ikke medvirker til å kartlegge sin identitet, jf. §§ 21 og 83*». Vi mener det er hensiktsmessig at lovteksten henviser til §§ 21 og 83 for å klargjøre hjemmelen om at den enkelte skal bidra til å avklare hvem de er, herunder ved personkontroll. Derimot er nytt annet ledd «*Bestemmelsen i første ledd bokstav a gjelder også for personer som det er usikkert om er utlending*» upresis. Vi kan ikke se at det fremkommer en redegjørelse om hvor langt den nye bestemmelsen vil rekke, og i hvilke situasjoner man ser for seg at denne skal anvendes. Teksten kunne med fordel erstatte «usikkert» med «hvor det er grunn til å anta».

7.2. IO-forskrift

- § 1 Interoperabilitet mellom informasjonssystemer:

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

I tillegg og som nevnt ovenfor mener vi at § 1 bør gjenspeile hele artikkel 1 (formål) til forordningene og i det minste pkt.1 med en beskrivelse av de ulike interoperabilitetskomponenter samt pkt.5 om identifisering og verifisering av personen.

Også artikkel 2 som viser til de ulike mål som interoperabilitet mellom informasjonssystemer vil oppnå, bør tas med i IO-lov eller forskrift.

- § 3 Behandlingsansvar for informasjonssystemer som inngår i interoperabilitetsforordningene

Under bokstav a annet ledd (SIS) er Sysselmesteren uteglemt dersom også utenrikstjenesten skal være med. UDI er i tvil om disse utlendingsmyndigheter som kun har lesetilgang til SIS for behandling av søknader om visum er å betrakte som behandlingsansvarlig. Enten må begge listes opp eller de må tas ut.

Under ny bokstav d (VIS) bør det presiseres «utlendingsmyndigheter» fremfor kun «myndigheter», samt dele bestemmelsen i to for å skille behandling av søknader om visum fra behandling av søknader om opphold som omtales i den reviderte VIS-forordning.

Vi ser også at departementet bruker begrepet «opplysninger» noen steder og andre steder «personopplysninger», som under behandlingsansvar for ETIAS og Eurodac, samt i forslagene til endring i grenseforskriften § 1-6 og til endring i utlendingsforskriften § 3-3b. Vi mener at begrepsbruken bør være konsekvent både i hele § 3 og i grenseforskriften § 1-6 ,eller det må det redegjøres nærmere for bruk av ikke helt like begrep.

Innspill til teksten og systematikk i § 3 (forslag i fete typer):

Når kompetente myndigheter behandler opplysninger i de av EUs

informasjonssystemer som inngår i rammeløsningen for interoperabilitet, ***er behandlingsansvaret som følger:***

a) Behandlingsansvar for SIS

Kripos ***er*** *behandlingsansvarlig for behandlingen av opplysninger, etter grensekontrollforordningen og politisamarbeidsforordningen, jf. SIS-loven § 4 første ledd*

Utlendingsdirektoratet, Utlendingsnemnda, politiet som Utlendingsmyndighet, ***Sysselmesteren*** *og* ***utenrikstjenesten er*** *behandlingsansvarlig for deres respektive behandling av opplysninger om innreiseforbud etter grensekontroll-forordningen art. 24 og etter returforordningen, jf. SIS-forskriften § 1 første ledd.*

b) Behandlingsansvar etter EES-forordningen

Politidirektoratet ***er*** *behandlingsansvarlig for behandlingen av opplysninger etter EES-forordningen, jf. grenseforskriften § 1-6*

Utlendingsdirektoratet ***er*** *behandlingsansvarlig for* ***automatisert sletting av*** *opplysninger etter EES-forordningen art. 35 nr. 6, jf. grenseforskriften §* 1-6

c) Behandlingsansvar etter ETIAS-forordningen

Den nasjonale ETIAS-enheten ved Politiets utlendingsenhet ***er*** *behandlingsansvarlig for behandling av personopplysninger i det sentrale ETIAS-systemet etter ETIAS-forordningen art. 57 nr. 2, jf. utlendingsforskriften § 3-3 b første ledd*

Utlendingsdirektoratet er behandlingsansvarlig for behandling av personopplysninger etter ETIAS-forordningen i forbindelse med egen klagebehandling, jf. utlendingsforskriften § 3-3 b andre ledd

d) Behandlingsansvar etter VIS-forordningen

Utlendingsmyndigheter med ansvar for behandling av søknader om visum er behandleransvarlige for behandling av personopplysninger for egne formål etter VIS-forordningens kapittel II (Visum), jf. utlendingsforskriften § 18-7

Utlendingsmyndigheter med ansvar for behandling av søknader om D-visum og oppholdstillatelse behandlingsansvarlige for behandling av personopplysninger for egne formål etter VIS-forordningens kapittel IIIa (D-visum og oppholdstillatelse), jf. utlendingsforskriften § 18-7

e) Behandlingsansvar etter Eurodac-forordning

Utlendingsdirektoratet ***er*** *behandlingsansvarlig for behandling av opplysninger for egne formål etter Eurodac-forordningen, jf. utlendingsforskriften § 18-5*

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*

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

Også under bokstav d bør det stå «utlendings» foran myndigheter.

Det er også et behov for å se nærmere på ordlyden i foreslått bestemmelse som er ment å regulere det som følger av IO-forordningen artikkel 40 (3) b:

> *«Medlemsstatenes myndigheter som tilføyer eller endrer opplysninger i identitetsbekreftelsesmappen, skal være behandlingsansvarlige i henhold til artikkel 4 nr. 7 i forordning (EU) 2016/679 eller artikkel 3 nr. 8 i direktiv (EU) 2016/680 og skal ha ansvar for behandlingen av personopplysninger i MID».*

I ny § 6 vises det utover dette til ulike myndigheter *etter melding til/for respektive meldinger* til SIS, EES, ETIAS, VIS og Eurodac. Henvisningen til «etter melding til/for respektive meldinger» synes ikke å samsvare med forordningen. For å vise til de kompetente norske myndigheter kunne man se på forordningens artikkel 29 og knytte behandlingsansvaret til treff som forekom ved opprettelse eller ajourføring av en individuell saksmappe.

8. Avsluttende bemerkninger

Prosessen med dette høringssvaret har vært kompleks og krevende, ikke minst fordi det kun foreligger noen få bestemmelser i den foreslåtte IO-forskrift som skal synliggjøre viktigheten og de mange konsekvenser av det nye Schengen-regelverket for både brukere og de registrerte. Når andre høringsinstanser har fått uttale seg utelukker ikke UDI at det kan være nødvendig å komme tilbake til noen av våre innspill. Disse må også ses i sammenheng med tidligere innspill om endringer i VIS og tiknytning til de andre informasjonssystemene som vi formidlet i vårt høringssvar av 28. august 2023.

Med hilsen

Stephan Mo

direktør for Styring og regelverk

Tor-Magne Hovland

seksjonssjef

Saksbehandler: Catherine De Coster

Dokumentet er godkjent elektronisk i Utlendingsdirektoratet og har derfor ingen signatur.

Brevet sendes kun elektronisk.

Mottaker(e):

Justis- og beredskapsdepartementet
v/ Politiavdelingen

Kopi til:

Marit Aarsland Loe