Datatilsynet

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

| Deres referanse | Vår referanse | Dato |
|---|---|---|
| 23/5535 - MALO | 23/04906-3 | 09.02.2024 |

## Høringssvar - forslag til gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer m.m.

Vi viser til Justis- og beredskapsdepartementets høringsbrev av 21. desember 2023 med tilhørende høringsnotat. Høringen gjelder forslag til nye lov- og forskriftsbestemmelser for gjennomføring av to forordninger om interoperabilitet 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. Høringsfrist var opprinnelig 8. februar, men Datatilsynet har etter avtale fått forlenget fristen til 12. februar.

Interoperabilitetsforordningene foreslås gjennomført ved inkorporasjon i grenseloven § 8 første ledd nye nr. 4 og 5. Siden forordningene gjør endringer i en rekke andre forordninger som allerede er inkorporert i norsk rett, foreslås også endringer i grenseloven, SIS-loven og utlendingsloven. Med hjemmel i grenseloven § 25 nr. 12 og ny nr. 13 foreslås videre en ny forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for grensepassering, utlendingsforvaltning og politisamarbeid. I tillegg 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.

### Innledning og oppsummering av Datatilsynets merknader

Som nasjonal tilsynsmyndighet ligger det til Datatilsynet å føre tilsyn med norske myndigheters bruk av de felleseuropeiske informasjonssystemene knyttet til Schengen- og Dublin-samarbeidet. Våre merknader knytter seg til de personvernrettslige aspektene ved forslaget og kan i hovedsak oppsummeres slik:

- Det rettslige rammeverket for behandling av personopplysninger i informasjonssystemene er komplekst. Med innføringen av interoperabilitetsløsningen økes kompleksiteten ytterligere. En generell bekymring fra vår side er at det vil bli

krevende å anvende dette regelverket, både for behandlingsansvarlige, tilsynsmyndigheten og ikke minst de registrerte.
- Behandling av store mengder personopplysninger, herunder særlige kategorier av personopplysninger, mange involverte aktører og et komplisert regelverk kan i seg selv utgjøre risiko for brudd på personvernregelverket
- Med mange aktører innen utlendingsforvaltningen og politiet vil vi også understreke betydningen av klare ansvarsforhold. Vi mener at enkelte av bestemmelsene om behandlingsansvar bør utformes mer presist.
- Datatilsynet vil fremheve betydningen av et klart og tilgjengelig regelverk. Etter vårt syn bør forordningene gjennomføres i egen lov.
- Datatilsynet støtter ikke forslaget til politiloven ny § 10 a om opptak av biometriske opplysninger ved brudd på identifikasjonsplikten.
- Gjennomføring av interoperabilitetsforordningene vil ha økonomiske og administrative konsekvenser for Datatilsynet.

**Generelle merknader**

De senere årene er det vedtatt flere endringer i eksisterende felleseuropeiske informasjonssystemer. I tillegg er nye informasjonssystemer under etablering. En gjennomgående trend ved utviklingen er at det behandles flere personopplysninger, for flere formål, med tilgang for flere myndigheter og med en tettere integrasjon mellom systemene. Det foreliggende forslaget må bl.a. ses i sammenheng med endringer i visuminformasjonssystemet (VIS), jf. Justis- og beredskapsdepartementets høringsnotat av 7. juni 2023.

Interoperabilitetsforordningene (IO-forordningene) tar sikte på å legge til rette for en mer effektiv utnyttelse av EU-informasjonssystemene som understøtter forvaltningen av grense-, migrasjons- og sikkerhetsområdet. For Norges del omfattes visuminformasjonssystemet (VIS), Schengen informasjonssystem (SIS), Eurodac, inn- og utreisesystemet Entry/exit (EES) og fremreisetillatelsessystemet ETIAS. De to sistnevnte systemene er ennå ikke satt i drift.

Interoperabilitetsløsningen består av fire komponenter; en felles søkeportal (European Search Portal – ESP), en felles biometrisk sammenligningstjeneste (shared Biometric Matching Service – sBMS), et felles identitetsregister (Common Identity Repository – CIR) og en fleridentitetsdetektor (Multiple Identity Detector – MID).

Det rettslige rammeverket for behandling av personopplysninger i informasjonssystemene er komplekst. Med innføringen av interoperabilitetsløsningen økes kompleksiteten ytterligere. En generell bekymring fra vår side er at det er vil bli krevende å anvende dette regelverket.

Behandling av store mengder personopplysninger, herunder særlige kategorier av personopplysninger, mange involverte aktører og et komplisert regelverk kan i seg selv utgjøre risiko for brudd på personvernet.

Datatilsynet vil derfor fremheve betydningen av klare og tilgjengelige nasjonale regler. På enkelte punkter mener vi det er behov for mer utfyllende lov- og forskriftsregulering enn det departementet legger opp til. Videre mener vi at det kan være behov for utfyllende omtale og veiledning til enkelte av bestemmelsene i lovens forarbeider. Grunnen til dette er de generelle utfordringene med forordningers struktur, språk og detaljnivå – som avviker fra norsk lovgivningsteknikk. Dette kan gjøre regelverket vanskelig tilgjengelig for de som skal anvende det, og dermed føre til risiko for feil praktisering. I tillegg kan regelverket være vanskelig tilgjengelig for registrerte og for allmennheten ellers.

Videre vil vi fremheve viktigheten av å gi informasjon til de registrerte ved behandlinger etter IO-forordningene. Vi merker oss at det skal etableres en egen nettportal for å forenkle utøvelsen av de registrertes rettigheter etter personvernregelverket.

Nedenfor følger Datatilsynets merknader til de aktuelle punktene i høringsnotatet.

**Til punkt 3.3.7 Kapittel VII – Vern av personopplysninger**

Som departementet påpeker i høringsnotatet innebærer ikke interoperabilitetsløsningen at flere personer blir registrert eller at noen må oppgi flere opplysninger om seg selv. Personopplysningene det gis tilgang til gjennom interoperabilitetsløsningen er innhentet med grunnlag i rettsaktene som regulerer de underliggende informasjonssystemene. Interoperabilitetsløsningen innebærer imidlertid flere nye behandlingsformål for av personopplysningene, herunder behandling av særlige kategorier av personopplysninger, jf. personvernforordningen art. 9.

I fortalen til IO-forordningene er det lagt til grunn at personvernforordningen får anvendelse for nasjonale myndigheters behandling av personopplysninger for interoperabilitetsformål, med mindre behandlingen utføres av medlemsstatenes utpekte myndigheter for å forebygge, avsløre eller etterforske terrorhandlinger eller andre alvorlige straffbare forhold. I slike tilfeller kommer direktiv (EU) 2018/680 (Law Enforcement-direktivet/LED) til anvendelse, se fortalepunkt 53 og 54. Personvernforordningen og LED er gjennomført i norsk rett i henholdsvis personopplysningsloven og politiregisterloven.

IO-forordningene inneholder også særlige bestemmelser om personvern, som enten presiserer eller i noen grad avviker fra personvernforordningen og LED. I art. 48 nr. 1 vises det til den registrertes rettigheter etter personvernforordningen art. 15-18 og LED art. 14-16. Art. 48 inneholder videre regler om innsyn, retting og sletting av personopplysninger, herunder håndtering av begjæringer fra registrerte.

Hvilke behandlinger som faller inn under politiregisterloven er ikke nærmere omtalt i høringsnotatet. Politiet behandler personopplysninger i kraft av ulike roller (utlendingsmyndighet, grensekontrollmyndighet og politimyndighet), og grensen mellom personopplysningsloven og politiregisterloven kan i noen tilfeller være uklar. Hvilket regelverk som kommer til anvendelse vil bl.a. ha betydning for den registrertes rettigheter og Datatilsynets kompetanse og virkemidler. I det videre lovarbeidet bør det derfor klargjøres hvilke behandlinger i interoperabilitetsløsningen som faller inn under politiregisterloven.

Datatilsynet bemerker videre at forholdet til bestemmelsene om registrertes rettigheter i personopplysningsloven og politiregisterloven heller ikke er nærmere omtalt i høringsnotatet. Vi vil særlig fremheve betydningen av klare regler om de registrertes rettigheter ved behandling av personopplysninger gjennom interoperabilitetsløsningen. Etter vårt syn bør det vurderes å innta en bestemmelse om registrertes rettigheter i lov eller forskrift.

Det fremgår av høringsnotatet at medlemsstatene etter art. 45 skal påse at misbruk av opplysninger eller behandling eller utveksling av opplysninger i strid med forordningen sanksjoneres i samsvar med nasjonal rett. I høringsnotatet vises det til at man finner slike regler i henholdsvis personopplysningsloven § 29 og politiregisterloven § 60 siste ledd, hvoretter Datatilsynet kan ilegge den behandlingsansvarlige tvangsmulkt dersom disse ikke etterkommer tilsynets pålegg. Datatilsynet bemerker at det er noe uklart om bestemmelsen i art. 45 innebærer at det må være adgang til *straffesanksjonering* etter nasjonal rett. Formuleringene i den engelske[1] og den danske[2] versjonen kan etter vårt syn tyde på det. Overtredelsesgebyr etter personopplysningsloven § 26 anses som straff i relasjon til EMK, mens pålegg og tvangsmulkt etter personopplysningsloven og politiregisterloven er å anse som ikke-pønale tiltak.

**Til punkt 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 henvisningsbestemmelse 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. Samtidig har det vist seg å være vanskelig å innpasse gjennomføringen av forordningene i en eksisterende lov. Etter en samlet vurdering foreslås interoperabilitetsforordningene gjennomført i grenseloven ved en tilføyelse av rettsaktene til listen over gjennomførte rettsakter i § 8 første ledd.

Som nevnt innledningsvis vil Datatilsynet fremheve betydningen av et klart og tilgjengelig nasjonalt regelverk. Vi stiller spørsmål ved om forslaget om å gjennomføre IO-forordningene i grenseloven bidrar til dette. Vi viser til at forordningene, som dekker utlendingsforvaltning, grensekontroll og politisamarbeid, har et bredere anvendelsesområde enn grenseloven. Etter vårt syn bør forordningene gjennomføres i en egen lov.

**Til punkt 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 IO-forordningene i norsk rett.

---

[1] «Member States shall ensure that any misuse of data, processing of data or exchange of data contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive.»

[2] «Medlemsstaterne sikrer, at enhver form for misbrug af oplysninger, databehandling eller udveksling af oplysninger i strid med denne forordning er strafbar i overensstemmelse med national ret. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.»

Av informasjonshensyn foreslås det at det i forskriften § 1 angis hvilke av informasjonssystemene i rammeløsningen som Norge er tilknyttet. Datatilsynet ser dette som positivt.

I forskriftens § 2 foreslås hjemmel for politiets søk i det felles identitetsregisteret (CIR) for identifiseringsformål. Vi viser til våre merknader til punkt 4.4.

*Behandlingsansvar for underliggende systemer*
Forskriftens §§ 3 – 6 regulerer behandlingsansvaret. Forslaget bygger på forordningenes art. 40, som slår fast at den behandlingsansvarlige for det underliggende systemet også skal være behandlingsansvarlig for opplysninger som behandles i den felles biometriske sammenligningstjenesten (shared Biometric Matching Service – sBMS) og det felles identitetsregisteret (Common Identity Repository – CIR).

I gjeldende rett er behandlingsansvaret for VIS, SIS, Eurodac, EES 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 i henholdsvis ny § 1-6 i grenseforskriften og ny § 3-3 b i utlendingsforskriften.

I utkastet til ny IO-forskrift § 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.

Datatilsynet ser det som positivt at det i forskriften gis en samlet oversikt over behandlingsansvarlige for de underliggende systemene, med henvisning til aktuelle bestemmelser. Vi støtter også forslaget om å forskriftsfeste behandlingsansvaret for ETIAS og EES.

Sett hen til at de felleseuropeiske informasjonssystemene involverer mange aktører innen utlendingsforvaltningen og politiet vil Datatilsynet understreke betydningen av klare ansvarsforhold. Bestemmelser om behandlingsansvar bør derfor utformes så presist som mulig.

I forbindelse med den nye IO-forskriften mener vi det er behov for å foreta enkelte presiseringer i reglene om behandlingsansvar for underliggende systemer. Vi viser til at bestemmelsene om behandlingsansvar for de underliggende systemene er ulikt utformet, ved at det i noen tilfeller er vist til hvilket *organ* som er behandlingsansvarlig (f.eks. Utlendingsdirektoratet og Kripos), mens det i andre tilfeller er vist til hvilke *myndigheter* som er behandlingsansvarlige (f.eks. «politiet som utlendingsmyndighet» eller «myndigheter med ansvar for behandling av søknader om visum, D-visum og oppholdstillatelse»).

Når det gjelder behandlingsansvaret for SIS er det i IO-forskriften § 3 første ledd bokstav b vist til at behandlingsansvarlige er «Utlendingsdirektoratet, Utlendingsnemnda, politiet som utlendingsmyndighet og utenrikstjenesten for deres respektive behandlinger av opplysninger

om innreiseforbud etter grensekontrollforordningen art. 24 og etter returforordningen, jf. SIS-forskriften § 1 første ledd». Datatilsynet bemerker at bestemmelsen avviker fra ordlyden i SIS-forskriften § 1 første ledd, som slår fast at «utlendingsmyndighetene» er behandlingsansvarlig for behandling av opplysninger om innreiseforbud etter grensekontrollforordningen artikkel 24 og etter returforordningen.

Hvilke aktører som omfattes av begrepet «utlendingsmyndighetene» etter SIS-forskriften § 1 er ikke nærmere presisert i bestemmelsen. I høringsnotat av 10. desember 2021[3] om forslag til ny SIS-forskrift uttalte departementet følgende:

> *«Aktørene i utlendingsforvaltningen som behandler personopplysninger etter SIS-loven er Utlendingsdirektoratet (UDI), Utlendingsnemnda (UNE) og politiet som utlendingsmyndighet. Det er disse forvaltningsorganene som fatter vedtak og tar beslutningene som ligger til grunn for en SIS-innmelding. I forbindelse med vedtaksfatting og beslutning om SIS-innmelding må de samme organene behandle personopplysninger og andre opplysninger som er nødvendige for at SIS-innmeldingen skal være korrekt og oppdatert til enhver tid. Departementet foreslår derfor at behandlingsansvaret for behandling av opplysninger om innreiseforbud etter grensekontrollforordningen artikkel 24 legges til utlendingsmyndighetene, slik at også UNE er omfattet. Det er kun UDI og UNE som har kompetanse til å fatte utvisningsvedtak som ligger til grunn for meldinger etter grensekontrollforordningen artikkel 24.*
>
> *Utgangspunktet er at de ulike organene i utlendingsforvaltningen er behandlingsansvarlig for behandling av personopplysninger knyttet til de oppgaver de er pålagt etter returforordningen. Det foreslås derfor også at behandlingsansvaret etter returforordningen legges til utlendingsmyndighetene, og ikke bare UDI slik lovens § 4 legger opp til. Dette vil omfatte UDI, UNE og politiet som utlendingsmyndighet.»*

Datatilsynet forstår departementets uttalelser i høringsnotatet slik at «utlendingsmyndighetene» i relasjon til grensekontrollforordningen artikkel 24 omfatter Utlendingsdirektoratet og Utlendingsnemnda, mens det i relasjon til returforordningen omfatter Utlendingsdirektoratet, Utlendingsnemnda og politiet som utlendingsmyndighet. Utenrikstjenesten er ikke omtalt i høringsnotatet. Datatilsynet stiller derfor spørsmål ved om også utenrikstjenesten er behandlingsansvarlig etter SIS-forskriften § 1.

Dersom utenrikstjenesten er behandlingsansvarlig etter SIS-forskriften § 1 er det spørsmål om det er den enkelte utenriksstasjon eller Utenriksdepartementet som utøver behandlingsansvaret. Dette bør i så fall fremgå av bestemmelsen. Vi viser i den forbindelse til utlendingsforskriften § 17-7b, der det slås fast at behandlingsansvaret i utenrikstjenesten utøves av Utenriksdepartementet.

[3] Høring - ny forskrift om Schengen informasjonssystem (SIS) - regjeringen.no

Etter vårt syn bør det også fremgå klart av SIS-forskriften § 1 og IO-forskriften § 3 hvilket organ som er behandlingsansvarlig for *politiet som utlendingsmyndighet*. Slik Datatilsynet forstår det er Politidirektoratet behandlingsansvarlig i henhold til gjeldende etatsinstruks om personvern. Vi mener at også dette bør forskriftsfestes, i likhet med behandlingsansvaret for EES og ETIAS.

I lys av forslaget til ny IO-forskrift mener vi departementet bør endre SIS-forskriften § 1, slik at det fremgår klart hvilke organer som er behandlingsansvarlige for behandling av opplysninger om innreiseforbud etter grensekontrollforordningen artikkel 24 og etter returforordningen. Etter vårt syn er dette nødvendig for å unngå uklare ansvarsforhold knyttet til interoperabilitetskomponenten sBMS (shared Biometric Matching Service), jf. utkast til § 4.

I utkastet til § 3 første ledd bokstav g er det vist til at «myndigheter med ansvar for behandling av søknader om visum, D-visum og oppholdstillatelse» er behandlingsansvarlige for deres respektive behandling av opplysninger etter VIS-forordningen, jf. utlendingsforskriften § 18-7. Slik vi forstår det vil bestemmelsen omfatte Utlendingsdirektoratet, Utlendingsnemnda, politiet som utlendingsmyndighet, Sysselmesteren på Svalbard og utenrikstjenesten. Datatilsynet mener det bør fremgå klart av utlendingsforskriften § 18-7 og IO-forskriften § 3 hvilke organer som er behandlingsansvarlige for behandling av opplysninger etter VIS-forordningen. Vi viser også til vårt høringssvar av 30. august 2023 om endringer i VIS.

*Behandlingsansvar for interoperabilitetskomponentene sBMS, CIR og MID*
For å angi behandlingsansvarlig for opplysninger i sBMS og CIR henvises det i IO-forskriften §§ 4 og 5 tilbake til oversikten i forskriftens § 3. Det følger av § 4 at de behandlingsansvarlige 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». Videre følger det av § 5 at de behandlingsansvarlige for behandling av opplysninger i Eurodac, ETIAS, EES og VIS som nevnt i § 3 er «behandlingsansvarlig for sine respektive biometriske opplysninger i CIR samsvar med interoperabilitetsforordningene art. 40 nr. 1».

Datatilsynet har ikke innvendinger mot den regeltekniske løsningen. Vi bemerker at slik behandlingsansvaret er plassert for de underliggende systemene i Norge vil det være mange behandlingsansvarlige for interoperabilitetskomponentene. Etter vår vurdering er det viktig at ansvarsforholdene klargjøres i regelverket.

Samtidig fremstår det som noe uklart hva behandlingsansvaret for interoperabilitetskomponentene vil innebære for norske myndigheter. Vi viser bl.a. til at ansvaret for informasjonssikkerheten i stor grad er lagt til eu-LISA, som etter forordningene art. 41 er databehandler for sBMS, CIR og MID.

Forskriften § 6 regulerer behandlingsansvaret for behandling av lenker i fleridentitetsdetektoren (Multiple Identity Detector - MID), i samsvar med IO-forordningene art. 40 nr. 3. I § 6 bokstav a - e angis hvilke organer/myndigheter som er

behandlingsansvarlige for endringer og tilføyelser i identitetsbekreftelsesmappen, knyttet til meldinger til de underliggende systemene.

Etter § 6 bokstav d er «myndigheter med ansvar for behandling av søknader om visum, D-visum og oppholdstillatelse» behandlingsansvarlig for deres respektive meldinger til VIS. Datatilsynet mener bestemmelsen bør presiseres nærmere, slik at det fremgår klart hvilke organer som er behandlingsansvarlige. Vi viser til våre merknader til § 3 over.

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

Politimyndigheter kan i henhold til IO-forordningene art. 20 gis adgang til å søke i CIR for identifiseringsformål i nærmere angitte tilfeller. Bruk av søkeadgangen forutsetter hjemmel i medlemslandenes nasjonale lovgivning. Departementet foreslår at politiet gis hjemmel til å foreta identifiseringssøk mot CIR til de formål som er nevnt i art. 20 nr. 1 til 4. Søkeadgangen foreslås hjemlet i forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning § 2, jf. grenseloven § 25 ny nr. 13. Bestemmelsen gir ikke hjemmel for å oppta biometriske opplysninger og må ses i sammenheng med de foreslåtte endringene i politiloven.

*Søkeadgang når det er innhentet biometriske opplysninger i medhold av straffeprosessloven § 160 og politiloven ny § 10 a*
IO-forskriften § 2 første ledd åpner for at politiet kan søke i CIR når det innhentes biometriske opplysninger i medhold av straffeprosessloven § 160 og politiloven § 10 a.

Datatilsynet har ikke innvendinger mot den foreslåtte bestemmelsen i § 2 første ledd hva gjelder søk mot CIR i tilfeller hvor det er innhentet biometriske opplysninger i en straffesak medhold av straffeprosessloven § 160.

Når det gjelder adgangen til søk ved brudd på identifikasjonsplikten etter politiloven er Datatilsynet av den oppfatning at det ikke bør åpnes for å oppta biometriske opplysninger i slike tilfeller. Vi viser til våre merknader i punkt 5.1.3 om forslaget til ny § 10 a i politiloven. Etter vårt syn bør søkeadgangen etter forskriftens § 2 første ledd derfor begrenses til tilfeller hvor det innhentes biometriske opplysninger i medhold av straffeprosessloven § 160.

*Søkeadgang når det er innhentet biometriske opplysninger i medhold av politiloven § 12 nytt sjette ledd*
Datatilsynet stiller seg positiv til den foreslåtte bestemmelsen i § 2 annet ledd, som åpner for at politiet kan søke i CIR for identifiseringsformål når det er innhentet biometriske opplysninger i medhold av politiloven § 12 nytt sjette ledd.

Vi merker oss at bestemmelsen er begrenset til å gjelde politiet, da det verken anses å være behov for eller hensiktsmessig at påtalemyndigheten gis tilsvarende søkeadgang. Vi merker oss videre at det heller ikke legges opp til at Kystvakten skal gis tilgang til å søke i CIR for identifiseringsformål, men at departementet ønsker innspill om det er behov for slik tilgang.

Det fremgår av høringsnotatet at politiet som grensekontrollmyndighet og utlendingsmyndighet vil kunne gjøre bruk av CIR, men at tilgangen da er hjemlet i artikkel 21. Datatilsynet bemerker at det er uklart om andre myndigheter kan utføre søk i CIR med hjemmel i artikkel 21 når de utøver myndighet på vegne av politiet eller gir bistand til politiet som grensekontrollmyndighet og utlendingsmyndighet. Vi mener dette må klargjøres i det videre lovarbeidet. Vi viser til at grenseloven åpner for at grensekontroll kan utføres av annen myndighet på vegne av eller som bistand til politiet, jf. grenseloven § 4. Nærmere regler om bistand til politiet er gitt i grenseloven § 6 (Forsvaret) og § 7 (Tolletaten). Tilsvarende gjelder ved utlendingskontroll som utføres av andre myndigheter i medhold av utlendingsloven § 22. I tillegg kan Kystvakten etter kystvaktloven § 12 føre kontroll med at bestemmelser gitt i eller i medhold av utlendingsloven og grenseloven blir overholdt.

**Til punkt 5.1 Forslag til endringer i politiloven**

*Til punkt 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. Departementet mener at politiet i slike ekstreme situasjoner bør ha mulighet til å oppta biometriske opplysninger for å kunne identifisere vedkommende.

Datatilsynet har ikke innvendinger mot at det åpnes for opptak av biometriske opplysninger for å gjennomføre søk i CIR for identifiseringsformål i slike tilfeller, jf. utkastet til IO-forskrift § 2. Vi merker oss at politiloven § 12 nytt sjette ledd ikke gir hjemmel for å lagre opplysningene og at disse skal slettes straks søket er gjennomført.

*Til punkt 5.1.3 Opptak av biometriske opplysninger ved brudd på identifikasjonsplikten*
Politiet kan kreve at personer oppgir navn, fødselsdato, fødselsår, stilling og bopel hvis dette er nødvendig av hensyn til tjenesteutførelsen. Ved brudd eller mistanke om brudd på identifikasjonsplikten, kan politiet innbringe personen med hjemmel i politiloven § 8 første ledd nr. 3. 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.

Det fremgår av høringsnotatet at Politidirektoratet (POD) har spilt inn at politiet har behov for å kunne ta opp biometri og søke i CIR i tilfeller hvor personer ikke oppfyller identifikasjonsplikten, for å effektivisere politipatruljenes identifiseringsarbeid og øke nytteverdien av personkontroll for patruljen. POD har også fremhevet er at man med den nye hjemmelen vil kunne unngå å bli beskyldt for diskriminering av utlendinger. Departementet vurderer at hensynet til å unngå diskriminering ikke i seg selv er tilstrekkelig for å innføre en ny hjemmel for å oppta biometriske opplysninger, men ser at opptak av biometriske opplysninger i slike tilfeller vil kunne bidra til å effektivisere politiets arbeid og unngå unødvendige innbringelser.

Det fremgår av høringsnotatet at politiet ved søk i CIR vil kunne få treff på tredjelandsborgere som er registrert med biometriske opplysninger i de underliggende EU-informasjonssystemene som 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 politiets foto- og fingeravtrykksregister, jf. politiregisterloven § 13 og politiregisterforskriften kap. 46, til de 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 etterforskning av straffesaker og fullbyrdelse av straffereaksjoner, i utvisningssaker og i saker om utlevering til annen stat, jf. politiregisterforskriften § 45-6.

Forslaget til ny § 10 a i politiloven 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 høringsnotatet vises det til at behandlingen av opplysningene er 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 etter ny § 10 a vil være 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. Selv om den enkelte kan oppleve at det er vanskelig å nekte samtykke er det, ifølge departementet, 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.

Datatilsynet er av den oppfatning at den foreslåtte bestemmelsen i ny § 10 a ikke bør innføres.

Det følger av politiregisterloven § 7 at behandling av særlige kategorier av opplysninger etter bare kan finne sted dersom det er «strengt nødvendig» ut fra formålet med behandlingen. Ordlyden tilsier at det gjelder et skjerpet nødvendighetskrav. Bestemmelsen er imidlertid ikke omtalt i høringsnotatet.

Datatilsynet mener det ikke bør åpnes for å oppta biometriske opplysninger uten at dette er godt begrunnet og vurdert opp mot politiregisterlovens krav. Slik forslaget er begrunnet i høringsnotatet mener vi dette ikke er tilfellet. Det er i liten grad vist til praktiske eksempler hvor bestemmelsen vil effektivisere politiets identifiseringsarbeid. Vi merker oss også at departementet er noe i tvil om den reelle nytteverdien av en slik bestemmelse.

Etter vårt syn er det videre problematisk å basere opptak av biometriske opplysninger på samtykke (frivillighet), når valget står mellom to inngripende tiltak. Vi merker oss ellers at det ikke er aktuelt åpne for å oppta biometriske opplysninger uten samtykke eller ved bruk av tvang.

Forslaget synes å bygge på en forutsetning om at opptak av biometriske opplysninger og påfølgende søk i CIR og politiets foto- og fingeravtrykksregister kan redusere behovet for innbringelser. Slik vi forstår det vil bestemmelsen først og fremst vil ha en effektiviseringsgevinst i de tilfeller hvor personen er registrert i CIR og/eller i politiets foto- og fingeravtrykksregister. Det fremgår ikke av høringsnotatet hvordan saken stiller seg dersom søket ikke gir treff i noen av registrene. Siden vilkårene for innbringelse etter politiloven § 8 nr. 3 må være oppfylt er det spørsmål om innbringelse kan være aktuelt selv om vedkommende har samtykket. I så fall bør politiet informere om dette før et ev. samtykke gis.

Dersom bestemmelsen i politiloven ny § 10 a blir innført er det helt sentralt at politiet gir god informasjon om bruken av personopplysninger og aktuelle handlingsalternativer, jf. bestemmelsen § 10 a annet ledd.

**Til punkt 5.2 Forslag til endringer i utlendingsloven**

*Til punkt 5.2.1 Opptak av biometriske opplysninger ved manglende samarbeid om identitetsavklaring*
Det forslås en endring i utlendingsloven § 100 første ledd bokstav a for eksplisitt å dekke også tilfeller der vedkommende ikke medvirker til å klarlegge sin identitet i samsvar med §§ 21 og 83. Det forslås videre 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.

Datatilsynet merker seg at endringen er bare en klargjøring av gjeldende regelverk, og er ikke ment å innebære noen utvidelse av adgangen til å oppta biometriske opplysninger. Vi har ikke innvendinger mot forslaget.

*Til punkt 5.2.2 Bruk av biometriske opplysninger ved søk mot EES*
Departementet foreslår en endring i utlendingsloven § 100 femte ledd for at biometriske opplysninger opptatt med hjemmel i bestemmelsen også skal kunne brukes til søk mot Entry/Exit--systemet (EES) i tråd med EES-forordningen art. 26, 27 og 35.
Sletteplikten etter artikkel 35 innebærer at det vil måtte foretas systematiske søk mot EES. 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, anses å være legitimt og tungtveiende. Departementet mener 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 og at den foreslåtte hjemmelen er forenlig med personvernforordningen artikkel 9 nr. 2 bokstav g.

Datatilsynet merker seg at det ikke er helt klart i hvilken grad utlendingsforskriften § 17-7 a dekker behandlingen av biometriske opplysninger i slike tilfeller. Vi har ikke innvendinger mot forslaget.

**Til punkt 6 Økonomiske og administrative konsekvenser**

Ved gjennomføringen av interoperabilitetsforordningene vil Datatilsynet få nye oppgaver. Som nasjonal tilsynsmyndighet vil vi ha ansvar for å gjennomføre regelmessige tilsyn, behandling av klager, behandling av meldinger om brudd på personopplysningssikkerheten, råd og veiledning, internasjonalt samarbeid samt offentliggjøring av statistikk. I tillegg skal Datatilsynet utføre loggkontroll i henhold til artikkel 24 nr. 4.

For å utføre oppgavene i samsvar med internasjonale forpliktelser og nasjonal lovgivning er det derfor behov for dedikerte ressurser med særlig kompetanse (juridisk og teknisk). Datatilsynet har behov for å styrke sin kompetanse knyttet til dette komplekse systemlandskapet, både på kort og lang sikt.

Behovet for økte ressurser knytter seg særlig til tilsyn (forberedelser, gjennomføring og etterarbeid) med behandlingsansvarlige og sluttbrukere av systemene. Vi vil også vise til økt ressursbruk knyttet til internasjonalt samarbeid. For å sikre enhetlig og koordinert tilsyn med informasjonssystemene er Datatilsynet representert i koordineringsgrupper etablert innenfor rammen av Det europeiske personvernrådet (EDPB).

Det følger av art. 24 skal det føres logg over søk etter art. 22 og at loggene skal kontrolleres av den nasjonale tilsynsmyndigheten etter Law Enforcement-direktivet eller av EUs datatilsyn, med høyst seks måneders mellomrom. Som nasjonal tilsynsmyndighet vil Datatilsynet ha ansvar for å utføre loggkontroll i samsvar med bestemmelsen. Vi bemerker at bestemmelsen gir anvisning på at loggkontrollen skal foretas av tilsynsmyndigheten *eller* EUs datatilsyn (EDPS). Vi legger til grunn at oppgavedelingen mellom nasjonale tilsynsmyndigheter og EDPS avklares nærmere.

Det følger av IO-forordningene art. 51 at medlemsstatene skal sikre at deres nasjonale tilsynsmyndighet har de ressurser og den ekspertise som kreves for å utføre oppgavene de pålegges i forordningene. Datatilsynet vil ikke kunne utføre de pålagte oppgavene uten tilførsel av tilstrekkelige ressurser. Vi merker oss derfor at de økonomiske og administrative konsekvensene for Datatilsynet vil utredes nærmere.

Dersom det er spørsmål til vårt høringssvar kan saksbehandler kontaktes på e-post maren.vaagan@datatilsynet.no eller tlf. 472 75 513.

Datatilsynet stiller seg ellers positiv til å bidra med ytterligere innspill i lov- og forskriftsarbeidet, dersom dette er ønskelig.

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør, jus

Maren Vaagan
juridisk fagdirektør

*Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer*

Kopi til: DIGITALISERINGS- OG FORVALTNINGSDEPARTEMENTET (DFD)