POLITIET

Politidirektoratet

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres referanse:	Vår referanse:	Sted, dato:
23/5535	23/278860 - 23	Oslo, 08.02.2024

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

1. Innledning

Politidirektoratet viser til Justis- og beredskapsdepartementets høringsbrev av 21.desember 2023. Høringsfristen var 8.februar 2024, Politidirektoratet fikk utsatt frist til 12.februar 2024.

Departementet foreslår endring i grenseloven, samt andre forslag til lov- og forskriftsbestemmelser for å gjennomføre EUs forordninger om interoperabilitet, (EU) 2019/817 og (EU) 2019/818, mellom EUs informasjonssystemer. Forslaget innebærer at forordningene inkorporeres og vil gjelde direkte som norsk lov. Gjennomføring av forordningene vil føre til en mer effektiv utnyttelse av EUs informasjonssystemer som ved forvaltning av grense-, migrasjons- og sikkerhetsområdet.

Departementet foreslår også en ny forskrift om interoperabilitet mellom felles europeiske informasjonssystemer som angir hvilke informasjonssystemer Norge er tilsluttet og hvem som er behandlingsansvarlige for de ulike systemene.

Politidirektoratet har forelagt høringen for Kripos, Politiets utlendingsenhet (PU), Politiets IT-tjenester (PIT) og samtlige politidistrikt.

Politidirektoratet har mottatt uttalelser fra Kripos, Politiets Utlendingsenhet (PU), Politiets IT-tjenester (PIT), Øst politidistrikt, Innlandet politidistrikt, Oslo politidistrikt, Møre og Romsdal politidistrikt og Finnmark politidistrikt. Mottatte svar følger vedlagt dette høringssvaret.

2. Interoperabilitet mellom EU systemer

Ved gjennomføring av de to forordningene om interoperabilitet (EU) 2019/817 og (EU) 2019/818 er målet å bidra til økt sikkerhet i Europa og sikre at tredjelandsborgere opererer med én identitet. Dette skal skje gjennom å styrke grensekontroll, migrasjonskontroll og politisamarbeid for å forebygge, avdekke og etterforske grenseoverskridende kriminalitet, ulovlig migrasjon og terrorisme.

Med løsningene som følger av disse forordningene følger det mange nye endringer som vil påvirke norsk politi i fremtiden. Politidirektoratet er enig med PU i at dette vil føre til nye oppgaver, nye arbeidsformer og nye metoder for innhenting av informasjon for politiet. Det er derfor viktig at departement og lovgiver legger vekt på underliggende etaters vurderinger om hvordan dette vil påvirke norsk politi og hvordan dette på best måte bør gjennomføres.

Det er en omfattende reform som skal gjennomføres i Europa gjennom innføring av interoperabilitets forordningene og andre nye forordninger, samt endringer i eksisterende forordninger på område. Politidirektoratet mener at departementet gjennom høringsnotatet ikke fullt ut belyser de omfattende endringene dette vil føre til for norske myndigheter, særs for politiet. Politidirektoratet ber derfor departementet om at det legges stor vekt på høringsinnspill fra politiet.

3. Innspill til omtalen av ESP – den europeiske søkeportal

Politidirektoratet viser til departementets høringsnotat punkt 3.3.2. Den europeiske søkeportalen (ESP) er en av interoperabilitetskomponentene. Den gjør det mulig for medlemsstatenes myndigheter og unionsorganer å få tilgang til opplysninger i ulike EU-informasjonssystemer (EES, VIS, ETIAS, Eurodac, CS-SIS og ECRIS-TCN), CIR, MID, Europol-data og Interpol-databaser (TDAWN, SLTD) i samsvar med deres tilgangsrettigheter.

Tilgangen til data lagret i de nevnte databasene og komponentene gis på grunnlag av "ESP-profiler". Disse profilene er definert i henhold til de rettslige instrumentene som styrer bruk av EU-informasjonssystemer og databaser. Inn- og svardataene skal være i samsvar med ESP-profilen som brukes i forespørselen om å få utføre en spørring etter data. Det vil ikke være mulig å logge seg på ESP og bruke denne som en søkemotor, søk skjer gjennom de ulike fagsystemene som er koblet på ESP.

En "ESP-bruker" er definert som en medlemsstats myndighet (i praksis vil dette være de ulike nasjonale fagsystemene), et unionsorgan eller ett av de sentrale systemene for EES, ETIAS, VIS, ECRIS-TCN, Eurodac, SIS, CIR, MID, som har tilgang til minst ett av EU-informasjonssystemene eller interoperabilitetskomponentene i samsvar med de rettslige instrumentene som styrer disse informasjonssystemene, og som kan benytte seg av den europeiske søkeportalen og dataene som tilbys av den til sine mål og formål.

ESP-profiler er opprettet for å gi tilgang til ESP-funksjonene basert på hver kategori av ESP-bruker og på formålene med forespørslene, i samsvar med de tekniske detaljene og tilgangsrettighetene til hver spesifikk ESP-bruker.

Den ESP-profilen som tildeles en ESP-bruker, bestemmer:

- dataene som kan brukes til å sende en forespørsel
- de EU-informasjonssystemene som det er tillatt å stille spørringer til;
- de EU-informasjonssystemene som har tillatelse til å gi et svar;
- kategoriene av data som skal oppgis i svaret.

ESP-profiler administreres av autorisert personale i medlemsstatene. Tilgangen til relevante data for hver ESP-bruker vil bli konfigurert av teamene som er ansvarlige for nasjonal implementering i hver enkelt medlemsstat.

4. Inkorporering av forordningene om interoperabilitet i grenseloven

Departementet foreslår at forordningene gjennomføres i norsk rett ved inkorporasjon i form av en henvisningsbestemmelse i grenseloven. Departementet begrunner dette med at det ikke anses hensiktsmessig å gi en egen lov om interoperabilitet og viser til at det har vært noe utfordringer knyttet til plasseringen av en slik henvisningsbestemmelse.

Politidirektoratet er positive til at forordningene om interoperabilitet (IO) gjennomføres i norsk rett. Forordningene vil tilrettelegge for og bidra til en økt digitalisering av grensekontrollen, utlendingsområdet og politisamarbeid, samt bidra til en bedre og mer effektiv verifisering av identitet av tredjelandsborgere. Forordningene skal også i stor grad bidra til å forebygge og bekjempe alvorlig kriminalitet og terror. IO-forordningene legger til rette for en mer effektiv utnyttelse personopplysningene i de underliggende EU-systemene for å gjennomføre målet om én identitet i EU.

Direktoratet stiller imidlertid spørsmål ved hvorfor forordningene skal gjennomføres med en inkorporerings bestemmelse i grenseloven. Departementet skriver selv at det er vanskelig å innplassere forordningene i eksisterende lovverk, ettersom interoperabilitetsforordningene etablerer et felles teknisk system til bruk på tvers innen utlendingsforvaltning, grensekontroll og politisamarbeid. Uten videre begrunnelse skriver departementet at de etter en samlet vurdering foreslår å gjennomføre forordningene ved en inkorporasjonsbestemmelse i grenseloven.

Politidirektoratet mener implementering gjennom inkorporasjon i grenseloven gjør regelverket og innholdet i forordningene mindre tilgjengelig. Dette støttes av Kripos, PU, Oslo politidistrikt, Øst politidistrikt og Møre og Romsdal politidistrikt i deres innspill til høringen. Direktoratet mener det er behov for en egen interoperabilitetslov (IO-lov) som kan fungere som er en paraplyregulering for de underliggende kildesystemene som er underlagt IO, hvor også interoperabilitetsforskriften eventuelt kan hjemles.

Politidirektoratet viser til både PU og Møre og Romsdal politidistrikts grundige redegjørelser om behovet for IO-lov. Også Oslo politidistrikt, Innlandet politidistrikt og Øst politidistrikt viser til at det bør utarbeides en IO-lov med tanke på forordningenes kompleksitet og at systemene skal brukes på tvers av utlendingsforvaltning, grensekontroll og politisamarbeid. Oslo politidistrikt fremholder blant annet at det er nødvendig med et brukervennlig og lett forståelig regelverk for å kunne treffe effektive og korrekte avgjørelser i en operativ hverdag.

Politidirektoratet viser også til at anvendelsesområdet og formålet for grenseloven og IO-forordningene ikke er sammenfallende. Politidirektoratet mener at en presisering av forordningenes anvendelsesområde og formål er nødvendig, da for eksempel i en IO-lov, slik at dette er i overensstemmelse med IO-forordningene art. 1 og 2.

Interoperabilitet er komplekst og direktoratet mener at det er behov for klare nasjonale reguleringer som kan inneholde nærmere bestemmelser om blant annet formål, definisjoner og personvernet. Dette vil bidra til en tydeliggjøring av hva interoperabilitet er og hvilke konsekvenser det får for den registrerte og sluttbrukeren. Det er utfordrende for den registrerte å forstå sine rettigheter og også for myndighetene å ha oversikt over sine plikter. Det er også utfordrende og lite hensiktsmessig for brukere å veksle mellom flere regelverk og forstå systemet. Det er kun Entry Exit (EES) som er hjemlet i grenseloven. Visum information system (VIS), Eurodac og European Travel Information

and Authorisation System (ETIAS) er gjennomført i utlendingsloven og SIS i en egen SIS-lov. Dette taler for å samle systemene og forordningene i en IO-lov slik at det blir enklere å forstå sammenhengen og informasjonsutvekslingen mellom de ulike systemene.

Det er et behov å tydeliggjøre hvilke roller og ansvar de ulike myndighetene får ved gjennomføring av forordningene. Noe har departementet gjort ved å peke på behandlingsansvarlig i forslag til forskrift, men det er flere ting som gjenstår. Forordningene bruker begreper som kompetent myndighet og ansvarlig myndighet for verifikasjon av manuelle lenker. Dette er begreper som burde vært nærmere definert i en IO-lov, eventuelt IO-forskriften. I departementets høringsnotat kunne det vært redegjort for hvilke myndigheter som i de ulike situasjonene er kompetent myndighet, ansvarlig myndighet og behandlingsansvarlig i de ulike tilfellene. Dette hadde gjort forordningene mer forutsigbare for borgeren.

En eventuell IO-lov bør være tydelig og det bør ses hen til Digitaliseringsdirektoratets veileder for digitaliseringsvennlig og automatiseringsvennlig regelverk.

Dersom departementet likevel gjennomfører IO-forordningene ved inkorporasjon i grenseloven er det viktig at det utarbeides grundige forarbeider for å avhjelpe regelverkets tilgjengelighet og brukervennlighet, slik at det blir enklere å utarbeide instrukser og retningslinjer om systemet og avklare rettstilstanden.

5. Gjennomføring av IO-forordningenes artikkel 20

Departementet foreslår en ny hjemmel i politiloven § 10 a og § 12 sjette ledd for opptak av biometriske opplysninger for identifiseringsformål. Bakgrunnen for forslagene er behovet for å få på plass nasjonale lovgivningstiltak slik at politiet i større grad skal kunne benytte seg av mulighetene for søk i CIR (Central Identity Repository) som følger av IO-forordningene artikkel 20. Forslagene er ikke nødvendig for å gjennomføre IO-forordningene, men er i praksis en forutsetning for at politiet skal kunne nyttiggjøre seg av den søkeadgangen som artikkel 20 åpner for. I forslaget til § 10 a legges det opp til at opptak av biometri skal være begrenset til de tilfeller der en person kan innbringes etter politiloven § 8 nr. 3, samt at personen må samtykke til slik opptak.

Politiet har et overordnet ansvar for identitetsfastsettelse i samfunnet, noe som er avgjørende for samfunnssikkerheten. Endringene i politiloven for å gjennomføre art. 20 vil innebære et stort løft for identitetsarbeidet i politiet og effektivisering av arbeidet for politipatruljene.

Artikkel 20 i interoperabilitetsforordningene gir politiet, på nærmere angitte vilkår, adgang til å foreta biometriske søk i EUs felles identitetsregister (CIR) for identifiseringsformål. Norge får en mulighet til å utvikle prosessene rundt identitetsavklaring og på denne måten effektivisere politiets arbeid. En forutsetning for å kunne benytte seg av den muligheten er at det foreligger hjemmel i nasjonal rett.

Departementet skriver i høringsnotatet at de er noe i tvil om den reelle nytteverdien for politiet av en slik bestemmelse, og at de derfor ikke har konkludert om en slik hjemmel bør innføres. Her viser Politidirektoratet til PUs innspill (punkt 6) som underbygger behovet for en slik hjemmel, samt direktoratets innspill nedenfor. Kripos, Øst politidistrikt, Oslo politidistrikt og Finnmark politidistrikt stiller seg positive til forslagene om å gjennomføre hjemmel for opptak av biometriske data og søk i CIR for identifiseringsformål.

5.1. Politiets behov for nasjonal hjemmel for å søke i CIR

Å avklare identiteten til de involverte personene er essensielt for alle oppdrag politiet er involvert i. Det er få oppdrag hvor man ikke innhenter identitet. Politiet skal som hovedregel loggføre alle som politipatruljen kontrollerer i politisystemet PO. For eksempel dersom politiet ønsker å bortvise en person må tilfellet knyttes til et navn og adresse. Det er alltid en jobb for politipatruljen å vite hvem man har med å gjøre og hva man har hjemmel til å gjøre for å bringe identiteten på det rene og oppdraget for øvrig.

Politiets mulighet for å benytte søk i henhold til IO-forordningens art. 20 vil gi økt kvalitet i alle prosesser som berører ID-kontroll og avdekking av personer som opererer med flere identiteter.

Politiet har i forbindelse med ordenstjenesten generelt et behov for å avklare identiteten til personer de er i kontakt med, og enhver plikter å oppgi personalia til politiet på forespørsel. Det at personer kan opptre med, og bli registrert med, flere ulike identiteter i ulike systemer og etablere flere oppholdstillatelser på ulike identiteter, er uheldig og åpner for alvorlig kriminalitet, grenseoverskridende organisert kriminalitet, terrorisme, opphold på urettmessig grunnlag i Norge og Europa samt mulig misbruk av velferdssystemer mv.

Opptak og bruk av biometriske data for identitetsformål vil bli en sentral del for politiets arbeid med å fastslå riktig identitet i årene som kommer, i ulike digitale verktøy. Å avgjøre identiteten til personer på stedet hvor hendelsen skjer vil være svært ressursbesparende. Per nå må politipatruljene kjøre personen til arrest for signalering/identifisering når de motsetter seg eller ikke samarbeider, eller eventuelt kjøre vedkommende til bopel for kontroll av ID-dokument.

Det spiller ut mannskaper over lang tid, noe som fører til store tidstap og svekker beredskapen. Dette gir ulike utslag i ulike deler av landet. Større byer, hvor det er større aktivitet og flere hendelser, kan få redusert kapasitet i tider på døgnet/uken hvor behovet er stort. Mindre steder hvor det er langt til nærmeste politilokasjon eller arrest vil være helt uten politidekning i flere timer. Tiltak for raskt å kunne fastslå identitet vil dermed virke direkte inn på tilgjengeligheten til politiet. Fordelen med hjemmelen er at den i framtiden vil kunne bidra til at flere saker kan avsluttes på stedet, og vil øke nytteverdien av personkontroll for politipatruljen. Slik Politidirektoratet ser det fremmer det også interessene til den som kontrolleres ved at tvil om identitet raskt kan avklares i langt flere saker.

Behovet for å søke i CIR må også ses i sammenheng med et av IO-forordningene sitt hovedmål om én identitet for tredjelandsborgere i Europa. Forslaget i politiloven § 10 a vil være med å bidra til å nå dette målet.

PU skriver at de som særorgan i politiet på utlendingsfeltet må ivareta og ha fokus på de polisiære oppgavene knyttet til asylankomster og registrering av asylsøknader. En slik oppgave er å klarlegge søkernes rette identitet for å hindre at uønskede personer oppholder seg i riket. Grunnen til dette er at politiet av kontrollhensyn bør vite hvem som til enhver tid befinner seg i landet.

PU skriver også at det i ankomstfasen er en sentral oppgave for politiet å avklare identiteten til søker og om søker allerede har internasjonal beskyttelse eller annen tillatelse i Schengen. I den forbindelse anvender PU politiets metoder for undersøkelser for å avklare søkers rette identitet, herunder søk i politiregistre og anvendelse av tvangsmidler. PU legger til grunn at dette er polisiært arbeid og at PU opptrer som politimyndighet.

Politidirektoratet er enig i dette utgangspunktet. Det følger av artikkel 20 nr.1 at politimyndigheter kan gis adgang til å søke i CIR for identifiseringsformål. For å sikre et tydelig og praktisk regelverk er det viktig at departementet avklarer om PU vil ha tilgang til å søke i CIR som politimyndighet i ankomstfasen med formål om tidlig identifisering.

PU legger også til grunn at arbeidet med å avdekke utlendingens identitet i forbindelse med returarbeidet er en polisiær oppgave og iverksettelse av tvangsretur forutsetter politimyndighet. Politidirektoratet er enig i dette. Det er på sammen måte som nevnt ovenfor essensielt at dette stadfestes av departementet slik at det ikke er tvil om at PU vil ha adgang til å søke mot CIR for identifisering av utlendinger med utreiseplikt og i arbeidet med tvangsretur. Politidirektoratet viser til PUs høringssvar for ytterligere begrunnelse.

Politidirektoratet viser til høringsnotatets kapittel 2 om bakgrunnen for forordningene. Politiets søk og bruk av biometriske opplysninger kan være avgjørende for å avdekke svært alvorlig kriminalitet. Det refereres til terrorangrepene i Paris og Brüssel 2015 og 2016 som bakteppe for Europakommisjonens meddelelse i april 2016, om sterkere og smartere informasjonssystemer for grense og sikkerhet.

Direktoratet viser også til internasjonale organiserte kriminelle nettverk som knyttes til nyere hendelser mot flere europeiske land, eksempelvis i Belgia, Nederland og Sverige og som er av en slik karakter at det truer rettstaten.

Kripos narkotika- og dopingstatistikk for 2023 viser at det ble beslaglagt 2292 kilo kokain i Norge i fjor. Det er ikke tidligere beslaglagt mer enn 160 kilo noe år. Riksadvokaten skriver følgende i rundskriv nr. 1. 2024 – Mål og prioriteringer for straffesaksbehandlingen i 2024: *"Enkelte straffesaker viser at Norge brukes som et transittland for transport av narkotika. Dette er bekymringsfullt og kan tyde på at etablerte internasjonale kriminelle nettverk får fotfeste i Norge".*

Høy evne til tidskritisk identifisering av personer er derfor avgjørende å inneha. Nettverkenes kapabiliteter bla. til å produsere fiktive identiteter som verktøy til å gjennomføre kriminalitet er raskt økende i takt med ressursene disse nettverkene har tilgjengelig. Europol melder at narkotikakartellene tjener omkring 24 milliarder euro årlig i Europa, noe som illustrerer størrelsen på ressursene i den kriminelle økonomien.

Effektiv tilgang til biometriske opplysninger, samt opplysningenes integritet og konfidensialitet er av vesentlig betydning for politiets bruk av opplysningene. Opptak og søk med biometriske opplysninger må derfor være av rett og god nok kvalitet, og må kunne gjøres raskt og effektivt. Samtidig som at opptak og søk må gjøres på best mulig måte for å bevare konfidensialiteten. Dette vil for politiets vedkommende bety økt fokus på verktøy og teknologi innen biometrifeltet, men også på rett kompetanse og standarder.

5.2. Samtykkekravet

Politidirektoratet stiller seg, i likhet med ytre etat, svært positive til en innføring av en nasjonal hjemmel for søk i CIR ved brudd på identifikasjonsplikten. Direktoratet stiller seg imidlertid kritisk til forslaget om at opptak av biometri bør være betinget av samtykke. Kripos, PU, Innlandet politidistrikt, Møre og Romsdal politidistrikt og Øst politidistrikt har i sine høringssvar stilt spørsmål ved om det er formålstjenlig å sette samtykke som vilkår for opptak av biometri.

I Norge er det identifikasjonsplikt, uten hensyn til samtykke. Samtykkekrav til opptak av biometriske opplysninger gir lite mening sett i sammenheng med politiets andre mer inngripende hjemler. Direktoratet bemerker at det i tillegg til innbringelse vil være

adgang til etterfølgende visitasjon dersom en person på politiets forespørsel nekter å oppgi navn, fødselsdato, fødselsår, stilling eller bopel for å bringe en persons identitet på det rene, jf. politiloven § 10 (1).

Departementet har i høringsnotatet erkjent at det kan stilles spørsmål ved frivilligheten av samtykke der alternativet er innbringelse, men argumenterer likevel for at innbringelse er et reelt alternativ til samtykke og at innbringelse vil oppleves som mer inngripende enn å avgi biometri basert på samtykke. Etter direktoratets syn kan et samtykke som er avgitt for å unngå en mer inngripende handling vanskelig anses som frivillig. Et samtykke skal blant annet være informert og kunne trekkes tilbake. Det vises i den forbindelse til Møre og Romsdal politidistrikts høringssvar punkt 5.1.3, hvor distriktet peker på utfordringer knyttet til innhentingen av et informert, skriftlig samtykke og mulighetene for tilbaketrekking av samtykke i denne sammenheng. Politidirektoratet stiller spørsmål om innhenting av samtykke i disse tilfellene vil være gyldig i henhold til personvernregelverket.

Øst politidistrikt stiller i sitt høringssvar punkt 5.1.3 også spørsmål ved frivilligheten av samtykke i en situasjon der alternativet er innbringelse. Videre stiller distriktet også spørsmål ved den praktiske gjennomføringen av samtykke, herunder formkravene til slik samtykke. I sitt høringssvar punkt 6.1 viser PU til at samtykke som vilkår ikke understøtter formålet med artikkel 20 som blant annet er å kunne foreta søk i CIR der den det gjelder ikke vil samarbeide. Kripos etterlyser i sitt høringssvar punkt 5.1 en nærmere begrunnelse for kravet om samtykke i høringsnotatet og en beskrivelse av hvordan en slik samtykkeregel er tenkt implementert og praktisert. Politidirektoratet er enig i PU, Kripos og Øst politidistrikt sine betraktninger og viser i den forbindelse til deres høringssvar på punktet.

Politidirektoratet mener at utgangspunktet for reguleringen må være behovet for en tilstrekkelig klar hjemmel for både rettsansvender og publikum for at bestemmelsen skal oppnå sin materielle hensikt; nemlig å avklare identitet. Samtykke som rettslig grunnlag representer noe nytt i politiloven, som sitt utgangspunkt regulerer politiets maktbruk, og det vil kunne reises spørsmål ved adgangen til bruk av samtykke som rettsgrunnlag for opptak av fingeravtrykk (jf. rettsutviklingen knyttet til GDPR og EMK art. 8), og hvor reelt et valg mellom opptak og innbringelse vil være. Etter forslaget til ordlyd kan det synes som at den kontrollerte skal kunne velge mellom innbringelse eller opptak av fingeravtrykk på stedet, og det kan da oppstå spørsmål om det er adgang til innbringelse dersom opptak og søk likevel ikke gir noen treff.

For at søk i situasjoner som nevnt i artikkel 20 nr. 2 skal være tillatt, kreves det etter artikkel 20 nr. 5 at medlemslandene i nasjonale lovgivningstiltak angir *de nøyaktige formålene med identifiseringen i henhold til artikkel 2 nr. 1 bokstav b) og c).* Formålene i bokstav b) og c) er 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*". Det er etter dette et spørsmål om nasjonale bestemmelser om frivillig opptak av biometri er forenlig med de rammene for nasjonale lovgivningstiltak som oppstilles i artikkel 20 jf. artikkel 2. nr. 1 bokstav b) og c).

Politidirektoratet mener at en bestemmelse om opptak av biometri for de ovennevnte formål må utformes med utgangspunkt i politiets behov og slik at den registrertes samtykke ikke skal være avgjørende. Politidirektoratet savner også en redegjørelse i høringsnotatet for gjeldende bestemmelser for opptak av biometri i Sverige og Danmark, samt nasjonale lovgivningstiltak for å gjennomføre artikkel 20 nr. 2 i disse landenes nasjonale rett.

Avslutningsvis til dette punktet viser Politidirektoratet til at kravet om samtykke uansett ikke understøtter formålet med artikkel 20 søk. Ettersom søk i CIR etter artikkel 20 bokstav e) skal kunne anvendes i de tilfeller der en person ikke kan eller vil samarbeide. Dette viser PU også til i sin kommentar til politiloven § 10 a.

5.3. Søk i andre nasjonale register

Politidirektoratet støtter Kripos sitt forslag om å endre overskriften til politiloven § 10 a til "*Opptak av biometriske opplysninger for identifiseringsformål*". Dette vil gjøre formålet med bestemmelsen tydeligere for både politiet og borgerne.

I forslaget til ny politilov § 10 a avgrenses opptak av biometriske opplysninger til søk i foto- og fingeravtrykkregisteret. Dette reduserer etter Politidirektoratets mening kost-nytteverdien for bruk av biometriske opplysninger i politiets oppdragsutøvelse. Bakgrunnen for dette er at det foreslåtte registeret inneholder en begrenset personkrets og er lite egnet til effektiv identifisering. Artikkel 20 nr. 2 i forordningen stadfester at formålet bak opptak av biometriske opplysninger må være begrunnet i identifisering av en person. Paragraf 10 a bør i større grad tilrettelegge for en reell mulighet for identitetsavklaring uavhengig av borgerens status i nevnte register.

Forslag til ny bestemmelse bidrar til en effektivisering av politipatruljens identifiseringsarbeid og øker kvaliteten i personkontrollen. Faren for diskriminering og beskyldninger om diskriminering reduseres sammenlignet med dagens rettstilstand. Foreslått bestemmelse tar utgangspunkt i identifikasjonsplikten enhver har ovenfor politiet, uansett opprinnelse. Dette tilrettelegger i større grad for at likebehandling blir ivaretatt. Direktoratet mener imidlertid at hensynet til likebehandling ivaretas enda bedre dersom søk med biometriske opplysninger for identifiseringsformål gjøres bredere enn i departementets forslag.

Det fremgår av artikkel 20 nr. 5 at en nasjonal regulering skal være utformet slik at tredjelandsborgere ikke forskjellsbehandles. Politidirektoratet mener denne forutsetningen ikke oppnås gjennom foreslått hjemmel. Bestemmelsen bidrar til styrket identifisering av tredjelandsborgere, men vil i liten grad øke muligheten for en reel identifisering av øvrige personer.

På bakgrunn av nevnte forhold overfor mener direktoratet at det for identifiseringsformål bør inntas hjemmel for søk mot pass- og id-kortregisteret og utlendingsregisteret, og med foto- og fingeravtrykkregisteret som supplement.

Pass- og ID-kortregisteret har foto av alle norske statsborgere som har søkt om pass og nasjonalt ID-kort. Fotoene er av svært god kvalitet og registrene har gjennomgått en deduplisering slik at hvert foto kun er knyttet til én identitet. Dette i kombinasjon med at dekningsgraden for pass- og nasjonalt ID-kort er på over 90 % av innbyggerne vil registrene derfor egne seg meget godt til identifiseringsformålet.

Verken departementets forslag eller vårt forslag til registersøk gir anledning til å identifisere EØS-borgere med biometriske opplysninger, utover EØS-borgere som er registrert i foto- og fingeravtrykkregisteret. Innføring av nasjonalt ID-kort til utenlandske borgere vil imidlertid bidra til at en stor andel EØS-borgere med opphold i Norge vil være registrert med biometriske opplysninger i ID-kortregisteret. Dette vil i større grad ivareta identifiseringsformålet og hensynet til likebehandling.

Et ytterligere tiltak for å øke graden av likebehandling er å innta i forslaget til politiloven § 10 a at politiet for identifiseringsformål kan oppta biometriske data for å sammenligne foto av innehaveren med foto som er lagret i personens reise eller ID-dokument. Dette vil i særlig grad ivareta kontroll av personer viss biometriske opplysninger ikke er

tilgjengelig i våre registre eller CIR. Direktoratet understreker at identitetsavklaring ikke er fullført uten at personen, identitetsdokumentet og registeropplysningene er knyttet til hverandre og funnet i orden. Politidirektoratet forslår derfor en tilføyelse av et nytt andre ledd i forslag til ny politilov § 10 a:

> *Dersom en person identifiserer seg med et dokument som inneholder biometriske data som kan benyttes av politiets verktøy, kan politiet oppta biometriske data for å kontrollere om personen er rette innehaver av det fremviste dokumentet.*

Politidirektoratet viser i denne anledning til Kripos sitt innspill angående forslag til søk i flere nasjonale register for å gi best mulig tilgang for treff på identitetsopplysninger.

5.4. Kystvaktens tilgang for søk i CIR

Når det gjelder Kystvaktens tilgang til søk i CIR som politimyndighet ser Politidirektoratet at Kystvakten har et behov for å kunne gjennomføre identitetskontroller om bord i fartøy. Kystvakten kan bistå politiet i inn- og utreisekontroll i medhold av grenseloven § 15 eller i utlendingskontroll på territoriet i medhold av utlendingsloven § 21, jf. § 22. Dette er imidlertid ikke i egenskap av å være politimyndighet. Kystvakten har per nå heller ikke tilgang til de grunnleggende systemene for å gjennomføre denne type kontroll.

Politidirektoratet viser til innspill fra PU, Møre og Romsdal politidistrikt og Oslo politidistrikt for en nærmere gjennomgang av spørsmålet.

5.5. Forslag til politiloven § 12 sjette ledd

IO-forordningene artikkel 20 nr. 4 gir adgang til å søke i CIR med biometriske opplysninger for identifiseringsformål ved ulykke, naturkatastrofe og terrorangrep. Hjemmel for opptak av biometriske data inntas i politiloven § 12 sjette ledd.

Politidirektoratet er i hovedsak enig i departementets vurderinger og forslag, men viser til vårt eget innspill vedrørende bruk av nasjonale register ovenfor i 5.3. Dette gjør seg tilsvarende gjeldende for søk i forbindelse med identitetsavklaring for ukjente personer ute av stand til å legitimere seg og fra uidentifiserte levninger.

6. Tilgang for politimessige formål

Opplysninger fra internasjonale kilder bidrar til å øke kvaliteten i etterforskningen og er i større grad en forutsetning for å løse saker. Som et tiltak for bekjempelse av alvorlig kriminalitet og terror kan det under visse vilkår gis tilgang til opplysninger i de ulike EU-systemene til politimessige formål.

De ulike kildesystemene i EU har egne hjemler som regulerer når politiet kan få tilgang til opplysninger i systemene og på hvilke vilkår. Når opplysningene behandles til politimessige formål, reguleres denne behandlingen av politiregisterlov og -forskrift.

Det er det sentrale aksesspunktet/Central Access Point (CAP) i Kripos som er ansvarlig for å ta imot og saksbehandle anmodninger fra operative enheter i politi- og påtalemyndigheten med oppgaver innen forebygging, avdekking og etterforsking av alvorlig kriminalitet og terror. Dersom vilkårene er oppfylt skal CAP iverksette søk og tilgjengeliggjøre de relevante opplysningene for de operative enhetene.

IO forordningenes artikkel 22 gir utpekt myndighet en mulighet til å søke i CIR for å få informasjon om hvorvidt det finnes opplysninger om en bestemt person i EES, VIS, Eurodac eller ETIAS. Ved denne type søk vil man få informasjon om det finnes opplysninger om personen i et av de underliggende kildesystemene. Svaret fra CIR skal

bare brukes med det formål å inngi en anmodning om full tilgang på vilkårene og etter framgangsmåtene fastsatt i de respektive rettslige instrumenter for slik tilgang.

Slik Politidirektoratet forstår bestemmelsen vil de ulike operative politi- og påtalemyndighetene etter dette ha hjemmel til å søke i CIR for å sjekke om det i det hele tatt finnes opplysninger i de ulike kildesystemene. Dersom disse opplysningene finnes i et av systemene vil den operative enheten måtte gå veien om CAP og vanlige prosedyrer for å hente ut opplysningene. Direktoratet ber om en vurdering av om denne forståelsen er riktig etter departementets syn.

Direktoratet mener at denne artikkelen burde vært nærmere utredet i departementets høringsnotat, og at bestemmelsen også begrunner behovet for en IO-lov hvor slik særlovgivning kan tydeliggjøres. Finnmark politidistrikt har i sitt innspill kommentert et behov om å vurdere om dagens nasjonale regelverk hjemler søk i CIR i straffesaker. Politidirektoratet støtter behovet om å gå gjennom dagens regelverk slik at dette spørsmålet kan besvares. Direktoratet viser igjen til behovet for en IO-lov.

7. Innspill til forslag om forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning

Til forskriftens § 3
Departementet foreslår en henvisningsbestemmelse i interoperabilitetsforskriften (IO-forskriften) § 3 som skal liste opp de behandlingsansvarlige etter EES, VIS, SIS, Eurodac og ETIAS i Norge, med henvisning til hvor behandlingsansvaret er regulert i norsk rett.

Kripos uttaler i sitt høringssvar, under overskriften "*Om valg av gjennomføring i norsk rett*", at det er positivt med egen forskrift som beskriver komponentene i interoperabilitet, samt plasserer behandlingsansvar for behandling i de ulike komponentene. Møre og Romsdal politidistrikt anbefaler derimot i sitt høringssvar punkt 4.2 at det ikke opprettes en egen interoperabilitetsforskrift. Etter direktoratets syn er det et spørsmål om det er hensiktsmessig at det gis egne bestemmelser om behandlingsansvar i en IO-forskrift som lister opp behandlingsansvaret for de underordnede systemene i tillegg til reguleringen i de enkelte forskriftene som regulerer ansvaret knyttet til de enkelte systemer og om dette vil gjøre regelverket mindre, og ikke mer tilgjengelig. Det er videre et spørsmål om det ville være lovteknisk bedre å regulere behandlingsansvaret for IO-komponentene kun i de ulike hjemmelslovene istedenfor i en egen IO-forskrift til grenseloven.

Direktoratet bemerker også at enkelte deler av behandlingsansvaret for de underliggende systemene i dag er uklare, dette gjelder for eksempel VIS. Der det er uklarheter rundt behandlingsansvaret for de underliggende systemene, blir dette en følgefeil i IO-forskriften jf. § 3. Direktoratet ser derfor at det er behov for en tydelig avklaring av behandlingsansvaret som omtales i forskriften § 3.

Politidirektoratet ønsker også at behandlingsansvaret omtalt i forslag til §§ 4, 5 og 6 redegjøres nærmere i det videre lovarbeidet.

Til forskriftens § 3 bokstav b
Departementet har i forslag til IO-forskriften § 3 bokstav b) omtalt hvem som er behandlingsansvarlig for deres respektive behandling av opplysninger om innreiseforbud etter grensekontrollforordningen art. 24 og etter returforordningen, jf. SIS-forskriften § 1 første ledd.

Politidirektoratet mener det er behov for at departementet presiserer nærmere hvem "utlendingsmyndigheten" omfatter. Det er heller ikke beskrevet i hvilke situasjoner politiet utfører oppgaver som utlendingsmyndighet. Direktoratet mener at departementet må beskrive konkret hvilken myndighet som anses å være behandlingsansvarlig for å unngå ulike fortolkninger av for eksempel begrepet "utlendingsmyndighet".

Til forskriftens § 3 bokstav c og d, og grenseforskriftens § 1-6:
Kripos er behandlingsansvarlig for behandlingen som skjer i forbindelse med tilgang til opplysninger i EES for rettshåndhevende myndigheter. Dette bør også fremgå av opplistingen. Alternativt vil det fremstå som om POD er behandlingsansvarlig også for dette, noe som ikke blir korrekt. Behandlingsansvaret for slike opplysninger etter at de er delt med politiet for politimessige formål, vil følge av politiregisterlov- og forskrift/ LED og vil i hovedsak gjelde for alle kildesystemene. Direktoratet viser til at dette bare er nevnt for Eurodac i forslag til forskrift § 3 bokstav i).

Til forskriftens § 3 bokstav e:
Departementet har i utlendingsforskriften § 3-3 b) og IO-forskriften § 3 bokstav e) foreslått følgende formulering knyttet til reguleringen av behandlingsansvaret for ETIAS: "*Den nasjonale ETIAS-enheten ved Politiets utlendingsenhet er behandlingsansvarlig for behandlingen av opplysninger i det sentrale ETIAS-systemet [...]*".

PU har i sitt høringssvar punkt 5.2 redegjort for deres vurdering av at behandlingsansvaret for ETIAS bør legges til PU og ikke den nasjonale ETIAS-enheten (ENU). Politidirektoratet støtter denne vurderingen. Vi foreslår at man legger ansvaret til PU som organisatorisk enhet. Personopplysningsloven slår fast at den behandlingsansvarlige skal være både strafferettslig ansvarlig og erstatningsansvarlig, og kan være enten en juridisk eller fysisk person, herunder en virksomhet eller enkeltperson. Ved behandling av personopplysninger i offentlig forvaltning vil den behandlingsansvarlige alltid være en juridisk person. I de tilfellene hvor behandlingsansvaret ligger hos en juridisk person, vil det være den juridiske personen som helhet som har behandlingsansvaret, ikke enkeltpersoner i virksomheten. Dette er et syn som etter våre vurderinger understøtter at PU som virksomhet har dette ansvaret, uten hinder av at ENU som en underliggende enhet i PU er delegert det faktiske arbeidet og oppfølgingen.

Direktoratet er videre enig med PU om at den foreslåtte ordlyd i ny § 3-3 b) i utlendingsforskriften, ikke vil stenge for PU, og direktoratets, forståelse av plassering av behandlingsansvaret hos PU. Direktoratet stiller likevel spørsmål ved om det i norsk rett bør stå bare "Politiets utlendingsenhet", siden enheten blir organisert inn under PU som ansvarlig organ.

Til forskriftens § 6:
Politidirektoratet mener bestemmelsen ikke tydeliggjør hvem som vil være behandlingsansvarlig ved avklaring og korrigering av lenker i MID. Myndighet med ansvar for manuell kontroll av lenken vil bli behandlingsansvarlig for personopplysninger i MID. Her må det defineres nærmere hvem som er ansvarlig myndighet i de ulike tilfellene. Politidirektoratet viser her til kommentaren ovenfor i vårt punkt 4 om behovet for en egen IO-lov. Det er behov for en nærmere avklaring av roller og ansvar etter IO-forordningene.

Det bør også gjøres klart og tydelig at med "*behandlingsansvarlig for endring og tilføyelser*" i identitetsbekreftelsesmappen så menes de myndigheter som avklarer eller korrigerer lenker i MID. Det er de myndigheter som avklarer eller korrigerer lenkefargen

som blir behandlingsansvarlig, eller den myndighet som tilføyer eller endrer opplysninger etter artikkel 29, 34 nr.7 og artikkel 48.

Behandlingsansvarlig kan være den myndighet som behandler en gul lenke ved å sette en lenkefarge til hvit, grønn eller rød. På samme måte vil den myndighet som retter en lenke, på eget initiativ eller etter anmodning fra den registrerte, kunne bli behandlingsansvarlig. Dette betyr at myndigheten som til slutt ender opp som behandlingsansvarlig for opplysninger i identitetsmappen ikke trenger å være den myndigheten som hadde ansvar for manuell verifikasjon i første omgang.

I departementets forslag knyttes behandlingsansvaret for MID seg opp mot hvem som er behandlingsansvarlig for behandlinger i kildesystemene. Politidirektoratet foreslår å fjerne bokstav a) til e) i bestemmelsen.

8. Personvern og informasjonssikkerhet

8.1. Generelle innspill – LED og GDPR

Departementet uttaler i høringsnotatet pkt. 3.2 at GDPR gjelder for myndighetenes behandling av personopplysninger etter forordningene, med mindre politiet utfører oppgaver som rettshåndhevende myndighet med sikte på å forebygge, avsløre eller etterforske terrorhandlinger eller andre alvorlige straffbare forhold. Da vil det være politiregisterlov/LED og politiregisterforskrift som kommer til anvendelse. Politi og påtalemyndighet må derfor forholde seg til to regelsett som direkte regulerer behandling av personopplysninger. Dette kommer i tillegg til det fragmenterte regelverksarbeidet der de underliggende systemene i Norge med tilhørende rettsakter har ulikt oppheng i nasjonale lover og forskrifter.

Ved gjennomføring av EUIS-forordningene på norsk side utfører politiet oppgaver som faller innenfor politimessige formål, men også forvaltningsformål. Politidirektoratet savner en tydeligere beskrivelse av når LED får anvendelse for politi og påtalemyndighet i deres ivaretakelse av oppgaver etter EUIS-forordningene på norsk side.

8.2. Generelle innspill – angående begrepet "tilgang"

Politidirektoratet ber om at departementet har en gjennomgang av begrepet "*tilgang til personopplysninger*" de stedene dette er et begrep som er tatt inn i forordningene eller vurderinger gjort av forordningen. Det bør vurderes om man heller kan benytte seg av "*gjøre tilgjengelig personopplysninger*" for å enklere avgrense for eksempel behandlingsansvaret for opplysningene.

8.3. Generelle innspill – VIS og Svalbard

VIS-forordningen er gjennomført i norsk lov gjennom utlendingsloven. Sysselmesteren på Svalbard er delegert visummyndighet, jf. utlendingsloven § 13. I denne sammenheng vil også Sysselmesteren bli berørt av IO-forordningene, som for eksempel ved lenkebehandling. Politidirektoratet mener at betydningen av behandlingsansvaret for sysselmesterens behandlinger av opplysninger i forbindelse med IO bør komme tydeligere frem og beskrives nærmere.

8.4. Innspill til IO-forordningenes kapittel VII – Vern av personopplysninger

Departementet har i punkt 3.3.7 omtalt IO-forordningenes kapittel VII som omhandler personvernet. Direktoratet har følgende innspill til dette punktet:

8.4.1. Behandlingsansvaret

Etter IO-forordningene artikkel 40, er medlemsstatene behandlingsansvarlig for personopplysninger de legger inn i felles BMS, CIR og MID på EU-siden. EU-Lisa er etter

forordningene artikkel 41 databehandler for personopplysninger i den felles BMS, CIR og MID. Artikkel 51 regulerer tilsynsmyndighetenes tilsyn på nasjonal side. For Norge vil dette være Datatilsynet.

Politidirektoratet mener at utformingen av IO-forordningene innebærer at behandlingsansvaret som nasjonale myndigheter har inn i de underliggende systemene på EU-siden fraviker fra behandlingsansvaret, slik vi kjenner det etter personvernforordningen. Utformingen av IO-forordningene innebærer blant annet at medlemslandene som behandlingsansvarlig ikke selv kan påvirke hvilke informasjonssystemer opplysningene ender opp i på EU-siden, hvem som har tilgang til opplysningene eller hvem som er databehandler. Politidirektoratet mener det er behov for at departementet i sitt videre arbeid tydeliggjør hva som ligger i behandlingsansvaret etter IO-forordningene art. 40. Et effektivt tilsyn etter IO-forordningene art. 51 tilsier også at nasjonale myndigheter og Datatilsynet har en felles forståelse av behandlingsansvarets omfang.

8.4.2. De registrertes rettigheter

Departementet skriver i sitt høringsnotat at IO-forordningene enkelte ganger har gitt regler som enten presiserer eller i noen grad avviker fra de tilsvarende reglene i de nevnte personvernrettsaktene. Direktoratet savner en tydeligere presisering av de områder der IO-forordningene avviker fra reguleringene i LED eller GDPR. For de registrertes rettigheter er det flere områder som skiller seg fra GDPR, blant annet når det gjelder tidsfrister i artikkel 48, og Politidirektoratet mener det er viktig for lik håndtering av de registrertes rettigheter at departementet i sitt videre arbeid omtaler disse ulikhetene nærmere.

IO-forordningene gir gjennom art. 48 den registrerte rett til innsyn i, retting av og sletting av personopplysninger lagret i MID og begrensning av behandlingen. Retten til dataportabilitet og retten til å protestere, er rettigheter de registrerte har etter GDPR, men som ikke omtales i IO-forordningene.

Direktoratet ber om at departementet tydeliggjør hva det vil si at de registrertes rettigheter i IO-forordningene artikkel 48 fraviker fra tilsvarende regulering i GDPR.

Retten til å protestere vil også kunne få en indirekte påvirkning på andre områder da denne rettigheten ikke gjelder når GDPR art. 6 nr. 1 bokstav c) er valgt som behandlingsgrunnlag. Direktoratet mener det er viktig at departementet omtaler den fravikende reguleringen av de registrertes rettigheter i sitt videre arbeid, selv om det skulle vært vurdert at rettighetene i MID/CIR-sammenheng ikke vil ha relevans.

8.4.3. Identifisering av og kommunikasjon med de registrerte

Det skal opprettes en webportal for å forenkle den registrertes utøvelse av sine rettigheter om innsyn, retting, sletting og begrensning av behandlingen, jf. artikkel 49 i IO-forordningene. Det vil i denne portalen ikke være mulig å identifisere eller kommunisere med den registrerte.

Verken IO-forordningene eller fortalepunktene sier hvordan medlemsstatene er ment å kommunisere med den registrerte. Det er derimot nærmere redegjort for av EU-kommisjonen gjennom deres foreløpige forslag til IO-håndbok. Her anbefales det at den registrerte skal anvende webportalen for å utøve sine rettigheter etter artikkel 48 i IO-forordningene når portalen er kjent for den registrert. Direkte kommunikasjon mellom medlemsstaten og den registrerte kan ikke foregå i webportalen. Hvordan medlemstatene skal svare ut den registrerte er ikke klart.

Det vil være store utfordringer knyttet til kommunikasjon med tredjelandsborgere, både når det gjelder valg av kommunikasjonskanaler og sikker identifisering. Politidirektoratet ser med bekymring på måter kommunikasjonen kan foregå uten nærmere retningslinjer den registrerte og mener Departementet her må komme med innspill til rammer som kan tas med i vurdering for å sikre at lik og forsvarlig kommunikasjon mellom nasjonal behandlingsansvarlig og den registrerte finner sted.

8.5. Informasjonssikkerhet

Politidirektoratet stiller spørsmål ved hvorfor departementet har valgt å ikke gjengi kravene som fremgår av artikkel 42 om informasjonssikkerhet i nasjonal lovgivning.

Direktoratet mener at kravene knyttet til informasjonssikkerhet fra interoperabilitetsforordningene bør tydeliggjøres i norsk regelverk, for eksempel en IO-lov. Det er allerede i dag komplisert å orientere seg i alle krav til informasjonssikkerhet som følger av ulike regelverk. Det er hensiktsmessig å samle og vise til disse kravene for å unngå å måtte lete frem og gjennomgå forordningene dersom det er spørsmål om hvilke krav som stilles til informasjonssikkerhet. Fordelen med å unngå en fragmentarisk tilnærming forsterkes også ettersom tiden går.

9. Innspill til forslag til endringer i utlendingsloven og utlendingsforskriften

I høringsnotatet punkt 5.2.1 omtales departementets forslag til endringer i utlendingsloven § 100. Det foreslås først en presisering i første ledd bokstav a) for å ta med tilfeller der utlendingen ikke medvirker til å klarlegge sin identitet i samsvar med utlendingsloven §§ 21 og 83. Politidirektoratet ser at det er hensiktsmessig med en slik presisering.

Direktoratet viser til distriktenes og PUs innspill for ytterligere begrunnelse for behovet for en slik presisering. Etter Øst politidistrikts syn er det viktig at bestemmelsen om biometriopptak i utlendingsloven § 100 ikke endres på en slik måte at den fremstår som å gi grunnlag for kontroll med norske borgere. Det vil være uheldig dersom den kan oppfattes som en hjemmel for å oppta biometrisk personinformasjon om norske borgere uten at det har forbindelse til utlendingslovens formål.

Politidirektoratet er enig med Øst politidistrikt i at dette vil være uheldig, og viser i den sammenheng også til Oslo politidistrikts innspill. De foreslår at beviskravet knytter seg til begrep som hjelper den praktiske anvendelsen. I stedet for usikkert kan for eksempel "grunn til å anta at personen er utlending" være begreper som letter vurderingen av hvilket beviskrav som ligger til grunn. Direktoratet støtter distriktets innspill.

PU skriver at dersom departementet opprettholder at ny bestemmelse i politiloven § 10 a skal forutsette at vilkårene for innbringelse etter politiloven § 8 nr. 3 skal være oppfylt og at personen samtykker til opptak av biometri, bør det i utlendingsloven § 100 også gis en bestemmelse om adgang til søk mot CIR, jf. artikkel 20 nr. 1.

Det vises til PUs rolle i ankomstfasen som politi for å avdekke korrekt identitet, og politiets arbeid med verifisering av identitet i arbeidet med tvangsretur. Politidirektoratet er enig i at dette kan være hensiktsmessig. Det vises til at søk mot CIR for politiet i ankomstfasen og i forbindelse med verifisering og arbeidet med tvangsretur, samsvarer med formålene angitt i forordningene artikkel 2 nr. 1 bokstav b) og c), som i henhold til artikkel 20 nr. 5 skal fremgå ved søk. Formålene er forebygge og bekjempe ulovlig innvandring og opprettholde offentlig sikkerhet og den offentlige orden, samt ivareta sikkerheten på medlemsstatenes territorier.

Politidirektoratet vil også fremme et innspill til forslaget om nåværende femte ledd, fremtidige sjette ledd, skal lyde:

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

Av høringsbrevet fremgår det at endringen her skal sørge for at opptatt biometri etter utlendingsloven § 100 første ledd skal kunne gjenbrukes for å gjenfinne en person i EES. Formålet er å slette vedkommendes personinformasjon i EES (f.eks. der personen er innvilget statsborgerskap i Norge). Ordlyden er imidlertid svært vid/vag, og kan tilsi et mye videre anvendelsesområde. En henvisning til EES artikkel 35, ev til formålet om å slette personopplysninger i EES, vil her være oppklarende.

Politidirektoratet viser til kommentar til forslag til endring i grenseforskriften § 1-6 under vårt punkt 7.

Politidirektoratet ønsker også å kommentere forslag til endringer i utlendingsforskriften ved ny § 3-3 b) og omfanget av behandlingsansvaret. Den nasjonale ETIAS-enheten (ENU) har ansvaret for den nasjonale behandlingen av fremreisetillatelser jf. ETIAS-forordningen art. 8 og oppføring av opplysninger på ETIAS watchlist art. 34 og 35. Deler av saksbehandlingen av fremreisetillatelser vil gjøres i et nasjonalt fagsystem, mens behandlingen av opplysninger for oppføring på ETIAS Watchlist vil behandles i et eget fagsystem for dette. Fagsystemene er utviklet for å ivareta nasjonale krav til blant annet saksbehandling og notoritet.

I § 3-3 andre ledd reguleres UDIs behandling av personopplysninger i forbindelse med klagebehandlingen av fremreisetillatelser i det nasjonale fagsystemet. Bestemmelsen bør endres til også å omfatte ENUs behandlingen av personopplysninger nasjonalt. Siden ENU behandler personopplysninger i begge fagsystemer som nevnt over bør det reflekteres i ordlyden.

Et forslag er at det i § 3-3 b første ledd tilføyes i siste setning "*og for egne formål i nasjonale fagsystemer*".

Bestemmelsen vil da 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* ***og for behandlinger for egne formål i nasjonale fagsystemer.***
>
> *Utlendingsdirektoratet er behandlingsansvarlig for personopplysninger for egne formål i forbindelse med klagebehandling*

Tilsvarende bør forslag til forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning etter forordning (EU)2019-817 og (EU) 2019-818 § 3 første ledd bokstav e) endres.

10. Økonomiske og administrative konsekvenser

Gjennomføringen av IO-forordningene vil føre til økonomiske og administrative konsekvenser for politiet.

I lys av at EU implementere nye dataløsninger med CIR (Common Identity Reposetory) som en sentral komponent som har pekere til alle underliggende systemer som SIS, VIS, m.fl. for å oppnå en identitet på alle tredjelandsborger så har Norge en stor utfordring. I dag har vi ikke en identitet knyttet til kun en person i våre nasjonale applikasjoner. Det være seg for nasjonale borgere, EU-borgere og tredjelandsborgere. En person kan han mange ulike identiteter i Norge. Dette vil i hovedsak være for å oppnå ulovlige hensikter enten det er for å utnytte velferdsordninger eller begå grenseoverskridende kriminalitet. Det vil med ny forsterket grensekontroll bli desto mer ettertraktet å skaffe seg flere ID innenfor Schengen området.

Norge må derfor på sikt etterstrebe å få på plassen en nasjonal CIR-løsning som gir den samme identitet i ulike fagsystem (enten det er i BL, DUF, UTSYS eller andre løsninger). I lys av forsinkelser i EU og at implementeringen av interoperabilitet strekker seg fram i lang tid fremover så oppfordrer politiet departementet å utrede mulighet for å få en NCIR (nasjonal CIR), hvor utredningsarbeidet skjer innenfor EUIS programmet med tilhørende finansiering.

Politidirektoratet viser til vårt innspill (05.09.2023) angående gjennomføring av interoperabilitet i vårt høringsinnspill til endringer i visuminformasjonssystemet (VIS) og tilkobling av VIS til andre europeiske informasjonssystemer.

Politidirektoratet viser til at PU har gjennomgått og vurdert økonomiske og administrative konsekvenser i deres høringsnotat punkt 10. Politidirektoratet mener at innspillet kan sies være allmenngyldig for politiet og støtter med det konklusjonen at det er svært mange usikkerhetsfaktorer som gjør det vanskelig å vurdere de økonomiske og administrative konsekvensene av reformen. Det bør tas høyde for denne usikkerheten i det fremtidige budsjettarbeidet.

Med hilsen

Kari-Grethe Stave
Politiinspektør

Kristina Sandbu Netland
Seniorrådgiver

Dokumentet er elektronisk godkjent uten signatur.

Vedlegg:
Høringsinnspill IO - Øst pd
Høringsinnspill IO - Oslo pd
Høringsinnspill IO - Politiets Utlendingsenhet
Høringsinnspill IO - Kripos
Høringsinnspill IO - Møre og Romsdal pd
Høringsinnspill IO - Innlandet pd
Høringsinnspill IO - Finnmark pd

POLITIET

Øst politidistrikt

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:	Vår referanse:	Sted, dato:
23/278860-3	23/278748 - 3	Ski, 10.01.2024

Høring - Forslag til gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer mm

Det vises til Politidirektoratets henvendelse 09.01.2024 vedr. forslag om nye lov- og forskriftsbestemmelser for gjennomføring av EUs to forordninger om interoperabilitet mellom felleseuropeiske informasjonssystemer. Politidirektoratet ber om innspill til forslagene, som er sendt på høring av Justis- og beredskapsdepartementet, innen 29.01.2024.

Innspill fra Øst politidistrikt

Generelt

Øst politidistrikt er i det vesentlige positive til forslagene i høringsnotatet.

Vi støtter forslaget om å gjennomføre interoperabilitetsforordningene gjennom inkorporasjon, i tråd med hovedregelen i EØS-avtalen artikkel 7 bokstav a. Vi vil imidlertid påpeke det uheldige ved at forordningene gjøres til norsk rett "som sådan" når de inneholder henvisninger til regelverk som Norge ikke er bundet av, jf. ECRIS-TCN og direkte tilgang til Europol-opplysninger. Det er videre nokså uklart hvorfor interoperabilitetsforordningene er foreslått inkorporert gjennom grenseloven, all den tid systemet skal brukes på tvers av utlendingsforvaltning, grensekontroll og politi-samarbeid. Etter vårt syn bør det i stedet utformes en lov om interoperabilitet, som inkorporerer forordningene, gir forskriftshjemmel for gjennomføringen og fastsetter uttrykkelig hvilke informasjonssystemer og bestemmelser som skal være omfattet for Norges del.

Innspill til punkt 5.1.3 (politiloven § 10 a)

ØST POLITIDISTRIKT
Post: Postboks 3390, 1402 Ski / Besøk: Vestveien 16, 1400 Ski / (+47) 64 99 30 00
post.ost@politiet.no / www.politiet.no / Organisasjonsnummer: 974760584

I høringsnotatet punkt 5.1.3 omtales departementets forslag til ny § 10 a i politiloven. Bestemmelsen skal gi nasjonal hjemmel til biometriopptak og søk i det felles identitetsregisteret for identifiseringsformål dersom en person ikke samarbeider. Det fremgår av høringsnotatet at hjemmelen vil kunne bidra til å effektivisere politiets arbeid og unngå unødvendige innbringelser. Øst politidistrikt støtter innføringen av en hjemmel for biometriopptak og søk ved manglende samarbeid. Vi deler departementets syn om at biometriopptak og søk "på stedet" i hovedsak vil være et mindre inngrep som av de fleste vil oppleves som et bedre alternativ enn innbringelse.

Etter vårt skjønn er det imidlertid lite formålstjenlig å sette som vilkår at den angjeldende personen samtykker til opptak av biometri. I Norge er det identifikasjonsplikt, uten hensyn til samtykke. Når en person ikke samarbeider med å avklare sin identitet, må det etter vår erfaring påregnes at vedkommende heller ikke vil samtykke til søk i det felles identitetsregisteret.

Samtykkekrav til biometriopptak gir lite mening sett i sammenheng med at vilkårene for innbringelse etter politiloven § 8 nr. 3 må foreligge. En kan vanskelig si at personen er i posisjon til å avgi et reelt, fritt samtykke når handlingsalternativet er innbringelse. Det kan også være tale om personer påvirket av alkohol, annen rus eller med psykiske lidelser, som kan gjøre det uklart om personen har evne til å avgi et reelt, fritt samtykke. Dette fører også til at samtykke er lite egnet som behandlingsgrunnlag i disse sakene.

Formkravet til samtykket er også noe uklart, og all den tid samtykket skal være skriftlig eller nedtegnes i ettertid, vil dette uansett være en ekstraoppgave for patruljen. Det vil i en del tilfeller være lite praktisk for en ordenspatrulje å håndtere skriftlige samtykkeskjemaer, f.eks. i den nevnte situasjonen der patruljen påtreffer en større gruppe personer som ikke kan identifisere seg. Dersom det gis mulighet for at muntlig samtykke skal nedtegnes av politiet på stedet, vil det åpne for bestridelser i ettertid.

Uten bedre tilgjengelighet av utstyr for opptak av biometri, vil den foreslåtte hjemmelen uansett ha liten verdi. I dag benyttes Biometra-maskiner i politiets lokaler, typisk i sentralarresten. Øst politidistrikt har én mobil enhet, som befinner seg i politidistriktets grensebil. Dette er imidlertid et stort spesialkjøretøy beregnet på bruk i grense- eller utlendingskontroll og er således ikke tilgjengelig for enhver politipatrulje. Dette vil medføre at det i de aller fleste tilfeller vil være mest effektivt å innbringe personen til nærmeste politistasjon.

Innspill til punkt 5.2.1 (utlendingsloven § 100)

I høringsnotatet punkt 5.2.1 omtales departements forslag til endringer i utlendingsloven § 100. Det foreslås først en presisering i første ledd bokstav a for å ta med tilfeller der utlendingen ikke medvirker til å klarlegge sin identitet i samsvar med utlendingsloven §§ 21 og 83. Øst politidistrikt støtter den foreslåtte presiseringen.

Videre foreslår departementet et nytt annet ledd for presisere at hjemmelen for opptak av biometri også gjelder når det ikke kan stadfestes om personen det gjelder er utlending grunnet vedkommendes manglende evne eller vilje til å identifisere seg. Det fremgår at endringen bare er en klargjøring av gjeldende regelverk, og ikke er ment å innebære noen utvidelse av adgangen til å oppta biometriske opplysninger.

Etter Øst politidistrikts syn er det viktig at bestemmelsen om biometriopptak i utlendingsloven § 100 ikke endres på en slik måte at den fremstår som å gi grunnlag for kontroll med norske borgere. Det vil være uheldig dersom den kan oppfattes som en hjemmel for å oppta biometrisk personinformasjon om norske borgere uten at det har forbindelse til utlendingslovens formål.

Som beskrevet i høringsnotatet gir gjeldende § 100 grunnlag for opptak av biometriske opplysninger fra *utlendinger og personer som antas å være utlendinger*. Forslaget til nytt annet ledd har etter vår mening en noe plundrete ordlyd, og bidrar ikke til å klargjøre gjeldende regelverk mht. hjemmelens rekkevidde. Tvert imot er det uklart hva som menes med begrepet "usikkert", altså hvilken sannsynlighetsgrad som skal anvendes sammenlignet med andre normer som "grunn til å anta at vedkommende er utenlandsk statsborger" (§ 21), "konkrete holdepunkter for å anta" (§ 103 m.fl.) og den forvaltningsrettslige hovedregel om alminnelig sannsynlighetsovervekt.

På denne bakgrunn støtter ikke Øst politidistrikt forslaget om nytt annet ledd. Vi mener at det er unødvendig med denne presiseringen, og at endringen som foreslått ikke er egnet til å klargjøre regelverket. Dersom departementet likevel vurderer det som ønskelig å innta en presisering i § 100, mener Øst politidistrikt at ordlyden bør endres, f.eks. til at hjemmelen "…gjelder også når det er grunn til å undersøke om personen er utlending" eller "…gjelder også for å avklare om personen er utlending".

Med hilsen

Merete Christin Beck
Seksjonssjef

Erik Kongsgaard
Politiadvokat 2

Dokumentet er elektronisk godkjent uten signatur.

Kopi:
Merete Christin Beck

POLITIET

Oslo politidistrikt

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Deres referanse:	Vår referanse:	Sted, dato:
23/278860 - 3	24/6526 - 2	Oslo, 25.01.2024

Høring - Forslag til gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer mm

Oslo Politidistrikt viser til Justis- og beredskapsdepartementets høringsbrev av 21. desember 2023 og Politidirektoratets brev av 09. januar 2024. Vi takker for muligheten til å kommentere på forslaget.

Til pkt. 4.1 Gjennomføring av forordningene i norsk rett

Oslo Politidistrikt mener det kan være svakheter ved løsningen om å inkorporere interoperabilitetsforordningene kun gjennom grenseloven, og med tilhørende forskrift som også hjemles i grenseloven. Det vises til at det kan fremstå som at regelverket er begrenset til grenselovgivningen, samt at det bør vurderes om dette kan få betydning for spørsmålet om rettskildemessig rang. Regelverket kommer til å bli benyttet i operativ tjeneste og det er nødvendig at det er brukervennlig og lett forståelig for å kunne treffe effektive og korrekte avgjørelser. Det bør vurderes om en egen lov om interoperabilitet vil være mer hensiktsmessig i det lange løp, fremfor en inkorporasjon kun gjennom grenseloven.

Videre ønsker Oslo Politidistrikt å kommentere at det kan være utfordringer knyttet til grenselovens forhold til barnevernsloven som politiet benytter i mange tilfeller for forebygging av kriminalitet mot barn, eksempelvis for å hindre barn i å bli tatt med til utlandet.

Til pkt. 4.4.1 til artikkel 20 og 12 års aldersgrense

Oslo Politidistrikt vil påpeke at momenter i vurderingen av barnets beste med fordel bør kommenteres i forarbeidene. Det kan etter Oslo Politidistrikts syn tenkes flere hensiktsmessige årsaker til å legge inn informasjon om personer under 12 år som er av hensyn til barnets beste, herunder forhindre barnebortføring, oppfølgning av mindreårige

asylsøkere som forsvinner fra mottak med videre, samt for å forebygge straffbare forhold som rammes av strl. §§ 253 og 261.

Til pkt. 4.4.2 Departementets vurdering – Kystvakten

Kystvakten har per dags dato ikke tilgang til de grunnleggende systemene for å gjennomføre grensekontroll på vegne av politiet. Oslo Politidistrikt mener at en vurdering rundt Kystvaktens tilgang til søk i CIR bør tas når det er avklart hvorvidt Kystvakten skal ha tilgang til grense- og territorialkontrollsystemet (GTK) som er det primære inn- og utreisesystemet i grensekontrollen.

Til pkt. 5.1.3 Ny hjemmel for opptak i politiloven § 10 a

Oslo Politidistrikt stiller seg positiv til ny hjemmel for opptak i politiloven § 10 a så lenge dette supplerer og ikke innskrenker dagens regelverk på noe vis. Det er veldig tidsbesparende for patruljene ute å slippe å reise inn for å foreta disse søkene.

Det forutsettes at samtykkeerklæring skjer på en smidig måte, for eksempel gjennom en digital løsning. Det stilles spørsmål til hvor dette skal loggføres dersom vedkommende får gå etterpå – holder det at dette loggføres i PolitiOperativt system (PO), og hvor skal samtykket lagres?

Videre legges det til grunn at opplysningene straks skal slettes når søket er gjennomført. Oslo Politidistrikt går ut fra at dette kun gjelder de biometriske opplysningene, og at øvrige opplysninger nedtegnes et sted for notoritet.

Til pkt 7.3 Endringer i utlendingsloven

Oslo Politidistrikt er positive til forslaget om endring i utlendingsloven § 100 a for å eksplisitt dekke også tilfeller der vedkommende ikke medvirker til å klarlegge sin identitet i samsvar med §§ 21 og 83.

Til forslag om ny § 100 annet ledd: *Bestemmelsen i første ledd bokstav a gjelder også for personer som det er usikkert om er utlending.*

Det foreslås at beviskravet knytter seg til begrep som hjelper den praktiske anvendelsen. I stedet for *usikkert* kan for eksempel "grunn til å anta at personen er utlending" være begreper som letter vurderingen av hvilket beviskrav som ligger til grunn.

Med hilsen

Ida Melbo Øystese
Politimester

Dokumentet er elektronisk godkjent uten signatur.

POLITIET
POLITIETS UTLENDINGSENHET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Deres referanse:	Vår referanse:	Sted, dato:
	24/6642 - 3	Oslo, 29.01.2024

Høringssvar - gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer mm

Politiets utlendingsenhet (PU) viser til Politidirektoratets (POD) brev av 09.01.2024, vedlagt Justis- og beredskapsdepartementets (JD) høringsbrev av. 21.12.2023.

Høringen gjelder forslag om 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.

PU har fått frist til å komme med innspill innen utløpet av mandag 29.01.2024.

1. Innledning

EUs interoperabilitetsløsninger for utveksling av opplysninger mellom EUs informasjonssystemer er en viktig og svært omfattende reform i EU, som fører til store endringer i norsk politi fremover. Med interoperabilitetsløsningene følger mange nye oppgaver for politiet, nye arbeidsformer og nye metoder for innhenting av informasjon. De nye oppgaver vil spesielt medføre økt oppgavemengde for politiet innen grense- og utlendingsområdet. Av den grunn mener vi at det er viktig at lovgiver og departementet er lydhøre for underliggende etaters vurderinger om hvorledes inkorporeringen i norsk rett kan gjennomføres, da politietaten er den som må forstå hva reformene vil innebære i praksis og er de som på best mulig måte skal kunne anvende et komplisert regelverket i den daglige oppgaveløsningen.

POLITIETS UTLENDINGSENHET
Post: Postboks 2095 Vika, 0125 Oslo / Besøk: Økernveien 11–13, 0653 Oslo / (+47) 22 34 24 00
politiets.utlendingsenhet@politiet.no / www.politiet.no / Organisasjonsnummer: 986210504

Som særorgan i politiet på utlendingsfeltet, hvor en stor del av PUs samfunnsoppdrag er knyttet til asylfeltet, vil interoperabilitetsforordningene bli av sentral betydning og vil påvirke det meste av vår oppgaveutførelse, både polisiært og forvaltningsmessige. Andre sentrale deler av PUs virksomhet som internasjonalt arbeid, utarbeidelse av statikk og analyser, behandlingsansvar for ETIAS og UTSYS vil også bli berørt av interoperabilitetsforordningene. PU mener det er en svakhet ved høringsnotatet at det i liten grad omhandler asylfeltet, til tross for at forordning (EU) 2019/818 dreier seg om ramme for interoperabilitet mellom EU-informasjonssystemer for politisamarbeid og rettslig samarbeid, **asyl** og migrasjon (vår utheving).

PU har ikke hatt anledning til å kommentere alle punktene i høringsnotatet, men våre innspill er basert på PUs samlede erfaringsgrunnlag som særorgan på utlendingsfeltet. Vi har derfor funnet det hensiktsmessig å redegjøre for PUs samfunnsansvar og oppgaver, for å vise hvilke grunnlag våre vurderinger baserer seg på, se punkt 2 og 3. Vi ønsker med dette også å synliggjøre at formålene med interoperabilitetsforordningene nærmest er identisk med, og treffer rett inn i PUs mandat.

Våre øvrige innspill er om følgende:

- Gjennomføring av IO-forordningene i norsk rett og om lovgivningsteknikken, se punkt 4
- Reguleringen av behandlingsansvaret, se punkt 5
- Søk i CIR i medhold av implementering av artikkel 20, se punkt 6
- Implementering av artikkel 20 for å understøtte PUs oppgaver, se punkt 7
- Hvilke nasjonale myndigheter kan få tilgang til søk i CIR, se punkt 8
- Kommentarer til endringer i utlendingsloven § 100, se punkt 9
- Økonomiske og administrative konsekvenser, se punkt 10

2. Bakgrunnen og formålet med forordningene – høringsnotatets pkt. 2

Det overordnede formålet med interoperabilitet er å bidra til økt sikkerhet i Europa og én identitet i EU. Dette skal skje gjennom styrket grensekontroll, migrasjonskontroll, politisamarbeid og rettslig samarbeid, for å forebygge, avdekke og etterforske grenseoverskridende kriminalitet, ulovlig migrasjon og terrorisme. Et sentralt virkemiddel er målet om én identitet i EU.

Interoperabilitet vil blant annet bidra til å:

- I større grad sikre riktig ID på personer og bekjempe ID-misbruk, ved at politiet får tilgang til tidligere registrerte identiteter i EU-systemene innenfor gitte vilkår
- Forbedre datakvalitet i EUs informasjonssystemer og i nasjonale registre i politiet og utlendingsforvaltningen
- Styrke personvern og datasikkerhet
- Støtte opp om EES, VIS, ETIAS, Eurodac og SIS

Interoperabilitetsforordningene er således nøkkelen for styrking av den samlede effekten av EUs informasjonsverktøy på grense-, migrasjons-, asyl- og sikkerhetsområdet. Målet er å sikre at ansvarlige myndigheter får den informasjonen de trenger, når de trenger den. PU mener at interoperabilitetsforordningene skal inkorporeres i norsk rett i form av egen IO-lov, hvor det ikke kun gis en henvisningsbestemmelse, men at det gis bestemmelse om formålet med forordningene og at sentrale bestemmelser i forordningen inntas i lovteksten, se mer under punkt 4.

PU synes at høringsnotatet ikke fullt ut formidler hvor omfattende reform EU nå gjennomfører med interoperabilitet. Etablering av flere nye informasjonssystemer og utvidelse/revidering av de gamle, sammenholdt med at informasjon også skal utveksles på tvers av systemene, vil til sammen føre til en betydelig mengde ny informasjon i hvert av systemene. Dette skal håndteres i den daglige oppgaveløsningen i politiet, i enkeltsaker hos grense– og utlendingsmyndigheten, men også i straffesaksbehandlingen.

IO-forordningene medfører også oppgaver i forbindelse med at de store mengdene med innsamlet data skal sammenstilles, analyseres og vurderes. Det skal rapporteres og lage statistikk sentralt til EU, til euLISA og EU-kommisjonen. Det omfatter data som tidligere ikke har vært tilgjengelig, for eksempel data fra EES om hvem og hvor mange som returnerer når visum og fremreisetillatelse (ETIAS) utløper. Det er en del av PUs mandat å lage statistikk samt å analysere og rapportere på trender i migrasjon og smuglerruter. Vi er imidlertid usikre på hvordan og når innsamlet datamaterialet i EU blir gjort tilgjengelig igjen for nasjonale myndigheter. På migrasjonsfeltet kan endringer skje fort, og datamaterialet bør være "ferskvare", slik at nasjonale myndighetene raskt kan iverksette adekvate tiltak når det er nødvendig av samfunnsikkerhetsmessige hensyn. Vi ønsker å bemerke dette nå til høringsnotatet, fordi denne usikkerheten med omfanget av håndtering av enkeltsaker og behandling av statistikk og analyse, gjør det utfordrende å kunne vurdere de økonomiske og administrative konsekvensene av reformen for PU.

3. PUs samfunnsoppdrag

PUs mandat
PU har et nasjonalt ansvar for registrering av alle asylsøkere, undersøkelser om asylsøkernes reiserute, fastsette identiteten til utlendingen, forberede og iverksette alle negative vedtak i asylsaker, samt koordinering og kvalitetssikring av alle uttransporteringer fra Norge[1]. PU skal samle inn, bearbeide og informere rett politimyndighet om personer som tilhører kriminelle nettverk eller antas å ha begått alvorlige straffbare handlinger, herunder terrorhandlinger og krigsforbrytelser. PU har også ansvar for å bistå politidistriktene med kontrollvirksomhet og identitetsundersøkelser, samt samle inn, bearbeide og analyserer informasjon om illegal innvandring og ulovlig opphold.

Utover det som følger av mandatet har PU behandlingsansvaret for UTSYS (Politiets utlendingsregister), se politiregisterforskriften kapittel 56. ENU (National Unit ETIAS) er blitt plassert hos PU og det samme er NKS[2] (Nasjonalt koordineringssenter for grensekontroll).

PU som politimyndighet
I ankomstfasen plikter PU å gjøre undersøkelser i egenskap av å være politimyndighet[3]. Dette følger av politiloven § 2 som regulerer politiets plikter generelt. Politiet skal forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet, og avdekke og stanse kriminell virksomhet jf. politiloven § 2 nr. 2 og 3.

---

[1] Følger av Instruks for PU av 01.06.05 og Politidirektoratets (POD) rundskriv 2012-005 *Politiets arbeid med søknader om beskyttelse (asyl), identifisering og uttransportering av utlendinger etter utlendingsloven*

[2] *NKS skal koordinere informasjonsdelingen på operativt nivå mellom alle etater som arbeider med grensekontroll og migrasjon nasjonalt, og med Frontex (den europeiske grense- og kystvakt), og risikovurdere og kvalitetskontrollere grensekontrollen, med hjemmel i EBCG forordningen (EU 2019/1896 section 3-5 art. 18-29 og art. 32-25)*

Det følger av POD rundskriv 2012-005[4] at politiet i forbindelse med asylregistrering skal vurdere om asylsøkeren kan antas å tilhøre et kriminelt nettverk eller antas å ha begått alvorlige straffbare handlinger som nevnt ovenfor i tilknytning til PUs mandat.

Videre følger det av forarbeidene til utlendingslovgivningen at formålet med utlendingslovgivningen også er å forhindre kriminalitet, se blant annet **Ot. Prp. Nr 75 (2006-2007) s. 288**: *"Det er en grunnleggende del av innvandringsreguleringen å kunne holde utenfor landets grenser personer som er uønsket her på grunn av kriminalitet eller visse andre forhold."*

For å ivareta dette formålet må vedtaksmyndighetene få informasjon fra politiet dersom en søker er kriminell eller på andre måter kan utgjøre en fare for samfunnssikkerheten.

Formålet med politiets informasjonsinnhenting i ankomstfasen er således todelt. For det første skal det gjøres nødvendige undersøkelser for å ivareta politiets ansvar for samfunnssikkerheten. For det andre skal PU som saksforberedende organ innhente opplysninger for vedtaksmyndighetene.

PU som utlendingsmyndighet
Som særorgan i politiet på utlendingsfeltet må PU ivareta og ha fokus på de polisiære oppgavene knyttet til asylankomster og registrering av asylsøknader. En slik oppgave er å klarlegge søkernes rette identitet for å hindre at uønskede personer oppholder seg i riket. Grunnen til dette er at politiet av kontrollhensyn[5] bør vite hvem som til enhver tid befinner seg i landet.

PUs arbeid med ID-avklaring i ankomstfasen understøtter to formål, ivaretakelse av samfunnssikkerhet og bidra til å avklare beskyttelsesbehovet. Det er en kombinasjon av forvaltningsmessige gjøremål og politioperative oppgaver. Arbeidet med å avdekke utlendingens identitet i forbindelse med returarbeidet er en polisiær oppgave og iverksettelse av tvangsretur forutsetter politimyndighet.

Denne gjennomgangen viser at PUs samfunnsoppdrag er sammenfallende med formålet bak IO-forordningene. Det er på bakgrunn av dette at PU ønsker at Norge fullt ut skal implementere artikkel 20 som gir politimyndighetene tilgang til CIR for identifiseringsformål. PUs identifiseringsarbeid omfatter både identifisering av asylsøkere i ankomstfasen og identifisering av utlendinger ved iverksettelse av negative vedtak. Sistnevnte gjelder ikke bare ved tvangsretur, men også ved ledsaget retur, for eksempel i regi av Frontex med returstøtte, se mer om dette i punkt 7.2.

4. Gjennomføringen av IO-forordningene i norsk rett – høringsnotatets pkt. 4.1 og 4.2

4.1. Generelt om lovgivningsteknikk – inkorporering i eksisterende lov eller egen IO-lov

Departementet foreslår at forordningene gjennomføres i norsk rett ved inkorporasjon i form av en henvisningsbestemmelse. En slik henvisningsbestemmelse kan inntas i egen

---

[4] Politidirektoratets (POD) rundskriv 2012-005 *Politiets arbeid med søknader om beskyttelse (asyl), identifisering og uttransportering av utlendinger etter utlendingsloven*

[5] Fra Kommentarutgaven til utlendingsloven (Vevstad, 2010, s. 520) om hvorfor det er politiet som tar imot søknader om asyl.

lov eller i eksisterende lov. Departementet mener at det ikke er hensiktsmessig med en egen lov om interoperabilitet, men har likevel merket seg at det kan være noe vanskelig å tilpasse gjennomføringen av forordningene i en eksisterende lov. Dette skyldes at interoperabilitetsforordningene etablerer et felles teknisk system for informasjonsutveksling til bruk på tvers innen utlendingsforvaltning, grensekontroll og politisamarbeid, og at de underliggende systemene i Norge er regulert i ulike lover.

Uten noen ytterligere begrunnelse konkluderer departementet at de etter en samlet vurdering foreslår at interoperabilitetsforordningene gjennomføres i grenseloven ved en tilføyelse av rettsaktene til listen over gjennomførte rettsakter i § 8 første ledd. PU mener dette er en uheldig løsning. Sett hen til bakgrunnen og formålene med interoperabilitetsforordningene er plasseringen i grenseloven lite logisk. Det er bare EES, som er *ett* av de underliggende informasjonssystemene som interoperabilitet skal koble sammen opplysninger fra, som er listet opp i grenseloven § 8. VIS, EURODAC og ETIAS er gjennomført i utlendingsloven og SIS i egen lov (SIS-loven). Inkorporering i grenseloven gir mindre forståelse for sammenhengene i regelverket om informasjonsutveksling på tvers av systemene og av hva interoperabilitet egentlig er.

Etter PU sin vurdering er det *nettopp* fordi informasjon skal utveksles på tvers av utlendingsforvaltning, grensekontroll og politisamarbeid, at inkorporering av interoperabilitet i norsk rett bør skje i form av egen lov. Ved behandling av opplysninger som er innhentet til både politimessige og forvaltningsmessige formål, slik IO-funksjonalitetene legger opp til, kan vi ikke se hvilke hensyn som kan taler for en annen løsning. Vi viser også til at IO-forordningene er selve grunnmuren for EUs omfattende reform. Alene av den grunn bør inkorporasjon skje i form av en egen lov om interoperabilitet.

Vi bemerker til slutt at Norge også bør ta høyde for utviklingen i EU fremover. Interoperabilitet er ment å være dynamisk. Det betyr at flere elementer vil legges til etter hvert. En IO-lov vil derfor være en bedre langsiktig løsning. Vi nevner i den sammenheng at rammeløsning for interoperabilitet per nå også omfatter andre informasjonssystemer, som ECRIS-TCN[6], som Norge ikke er bundet av gjennom Schengen-samarbeidet og heller ikke er tilknyttet gjennom egen avtale. Hvis Norge inngår avtale om tilknytning til ECRIS-TCN, vil inkorporasjon enkelt gjennomføres i IO-loven. Ved å legge IO funksjonalitet under grenseloven vil det komplisere en senere tilkobling av nye informasjonssystemer som for eksempel ECRIS-TCN.

4.2. Utfordringer med henvisningsbestemmelse og at sentrale bestemmelser forordningene inntas i forskrift

PUs vurdering er at det ikke er tilstrekkelig at inkorporeringen skjer med en henvisningsbestemmelse i grenseloven, samt at enkelte elementer av forordningene reguleres i en interoperabilitetsforskrift som gis i medhold av grenseloven § 25 nr 12. Generelt vil det være en bedre løsning at de sentrale materielle bestemmelsene i forordningene fremgår av ordlyden i lov- og/eller forskriftstekst, i stedet for henvisninger til forordningenes artikler. Vi viser til at IO-forordningene er omfattende, detaljerte og tekniske. Av den grunn bør sentrale deler av forordningen fremkomme av lov, hvor forordningenes bestemmelser formuleres i lovteksten, med mer forståelig språkbruk.

Loven må ha en delegasjonsbestemmelse om adgangen til å gi ytterligere bestemmelser i en interoperabilitetsforskrift, men sentrale og overordnede kompetansebestemmelser om materiell- og personell kompetanse bør fremgå av loven. Av informasjonshensyn bør også formålene bak EUs interoperabilitetsforordninger fremkomme i loven, jf. vår

[6] Det europeiske straffesaksregisteret for tredjelandsstatsborgere

kommentar om dette i punkt 2 ovenfor. Ved at EUs formål med interoperabilitet kommer klart frem, bidrar det til større forståelse for nødvendigheten av politiets oppgaver etter forordningene. Vi viser til at interoperabilitetsforordningene medføre store endringer for oppgavene og arbeidsmetodene for norsk politi. Videre viser vi til at bestemmelser av sentral betydning for enkeltindivider og politiets handlingsrom bør være enkelt tilgjengelig, synlige og gi forutsigbarhet for borgerne og for politiets tjenesteutførelse.

Prosessuelle bestemmelser, samt mer detaljerte bestemmelser om håndteringen av de ulike komponentene i IO-forordningene som gir adgang til å få samlet informasjon fra de underliggende informasjonssystemene, kan reguleres i forskriften.

Hva som skal reguleres i loven og hva som er mest hensiktsmessig å regulere i forskrift må vurderes i det videre lovarbeidet. Umiddelbart er vår vurdering at når det gjelder de fire viktige interoperabilitetskomponentene som forordningene introduserer, mener vi bestemmelser om disse bør fremgå av loven, herunder bestemmelser om behandlingsansvaret. Det vises til ESP (felles søkeportal), sBMS (felles biometrisk sammenligningstjeneste), CIR (felles identitetsregister) og MID (fleridentitetsdetektor). Det samme gjelder bestemmelser om behandlingsansvar for ESP, sBMS og CIR i henhold til artikkel 40, samt bestemmelsen om implementering av artikkel 20 i norsk rett, tilgang til CIR for identifiseringsformål. Se våre innspill om artikkel 20 under punkt 6 og 7.

Når det gjelder forslag til interoperabilitetsforskrift[7], mener vi at det innholdet som foreslås regulert der er av slik art at det bør fremgå av loven. Når det gjelder de mest detaljerte bestemmelser i forordningen, blant annet om fremgangsmåter og krav om rutiner, kan de fremgå av en interoperabilitetsforskrift. Som eksempel nevnes bestemmelsen om behandling av lenker i artikkel 30-33.

5. Behandlingsansvar – høringsnotatets pkt. 4.3

5.1. Innledende bemerkninger

Gjeldende rett har regulert behandlingsansvaret for EUs informasjonssystemer ulikt, for de fleste av systemene er behandlingsansvaret regulert i lov og forskrift, men behandlingsansvaret for ETIAS og EES er regulert i instruks. Departementet foreslår at behandlingsansvaret skal reguleres i forskrift til henholdsvis utlendingsloven og grenseloven. PU støtter forslaget.

5.2. Behandlingsansvaret for ETIAS

Departementet legger opp til at Den nasjonale ETIAS-enheten (ENU), ved PU skal ha behandlingsansvar for behandling av personopplysninger i det sentrale ETIAS-systemet etter ETIAS-forordningens artikkel 57 nr. 2. Det gis ingen begrunnelse, men vi antar at ENU er valgt grunnet ordlyd og utforming av ETIAS-forordningens artikkel 57 nr. 2.

PU har etter forespørsel fra POD allerede redegjort for hvorfor behandlingsansvaret for ETIAS bør legges til PU og ikke ENU. Vår vurdering av behandlingsansvaret gjelder det overordnede behandlingsansvaret. Den daglige oppgaveutførelsen mener vi må ligge hos ENU. For ordens skyld inntas våre innspill nedenfor. De er sammenfallende med nevnte redegjørelse. Det vises til vårt brev av 23.01.2024[8].

---

[7] Forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning (punkt 7.5 i høringsnotatet)

[8] Vår ref. ws 22/253134-5

Bakgrunn
POD ved EUIS vurderte spørsmålet om behandlingsansvar i et notat av 27.05.21. Der ble det konkludert med at det var naturlig at sjef PU hadde det øverste ansvaret både for ENU og behandlingsansvaret. Vi er ikke kjent med hvilke vurderinger POD har gjort om behandlingsansvaret etter dette. Det følger imidlertid av PODs rundskriv 2023/006 *Informasjon om EUs informasjonssystemer* (pkt. 11.2) at ENU skal ha behandlingsansvaret for "den nasjonale behandlingen av personopplysninger i det sentrale ETIAS-systemet, jf. ETIAS-forordningen art. 57 (2) og for sin behandling i nasjonale systemstøtte".

ETIAS-forordningens artikkel 57. nr. 2
Det følger av ordlyden i art. 57 nr. 2 at ENU skal ha behandlingsansvaret for behandling av personopplysninger i det sentrale ETIAS-systemet i tråd med personvernforordningens artikkel 4 nr. 7. Selv om behandlingsansvaret her legges til ENU, kan vi ikke se at det vil være i strid med bestemmelsen om ansvaret plasseres hos den øverste lederen i det organet hvor ENU er organisert.

En naturlig forståelse av ordlyden tilsier at det er opp til medlemslandene å ta stilling til den nærmere utformingen og organiseringen av behandlingsansvaret, herunder at det i vurderingen må kunne legges vekt på nasjonale systemer og forhold. For øvrig slutter vi oss til PODs vurdering i notatet av 27.05.21 om at *"Forordningen setter ikke noe annet krav til organisering av ETIAS-enheten annet enn at det skal utpekes en myndighet som skal ha rollen som nasjonal ETIAS-enhet."*

Fordeler med at behandlingsansvaret legges til PU
En plassering av behandlingsansvaret i PU vil sikre en bedre kontroll med at ansvaret blir overholdt. Samtidig vil det gi et økt handlingsrom om det oppstår behov for avklaringer fra andre fagmiljøer i PU, eksempelvis kan juridisk seksjon og etterretningsseksjonen bistå der ENU har behov for å løfte prinsipielle problemstillinger. Samlet sett vil en plassering av behandlingsansvaret i PU sikre muligheten for et bredere forankringsgrunnlag hva gjelder ulike løpende problemstillinger som en må påregne at vil kunne dukke opp. I motsatt tilfelle må ENU som behandlingsansvarlig måtte få muligheten til å delegere oppgaver/ansvar til personer med tilstrekkelig kompetanse innad i PU.

Dersom behandlingsansvaret plasseres hos PU, vil sjef PU igjen kunne delegere det daglige praktiske ansvaret for utøvelsen av behandlingsansvaret til ENU. Det sikres da at behandlingsansvaret ivaretas av ansatte som er tettest på den faktiske behandlingen av opplysninger i systemet. Selv om det er en fordel at det daglige ansvaret håndteres av ENU, vil det likevel være en klar fordel å ha noe avstand til oppgaveutførelsen når det gjelder den overordnede delen av behandlingsansvaret. Som eksempel nevnes godkjenning av styrende dokumenter som vil være førende for ENUs behandling av opplysninger, herunder også utøvelse av instruksjonsmyndighet og tilsynsoppgaver.

Det er naturlig at sjef PU på vanlig måte skal kunne styre alle sider av ENUs virksomhet. Det er uheldig om behandlingsansvaret bare håndteres av ENU, når PU har alt annet ansvar for enheten. Utformingen og håndteringen av behandlingsansvaret vil også kunne få økonomiske og administrative konsekvenser for PU, noe som igjen taler for at dette ansvaret bør legges til PU. I den anledning viser vi til at behandlingsansvarlig kan bli erstatningsansvarlig om personopplysninger behandles på en ulovlig måte.

Sammenheng i regelverket – den norske modellen for behandlingsansvar
Det er nærliggende å sammenligne behandlingsansvar for ETIAS med behandlingsansvar for politiets sentrale registre. Vår vurdering er at de samme grunnleggende hensynene

gjør seg gjeldende idet rollen som behandlingsansvarlig vil være tilnærmet lik etter personvernforordningen og personverndirektivet.

Praksis i politiet er at behandlingsansvaret plasseres i et organ, som Kripos, PU eller POD, og ikke til underliggende enheter i disse organene, jf. bl.a. Etatsinstruks for personvern pkt. 6.1-6.4. Dette er jo for øvrig den norske modellen, så også etter utlendingsloven der ETIAS er hjemlet, jf. utlendingsforskriftens § 17-7b. Denne modellen har gode grunner for seg og hindrer ikke at det daglige ansvaret for oppgaveutførelsen kan delegeres til underordnet organ/enhet, som for eksempel POD har gjort for GTK (til Øst politidistrikt) og som PU har gjort for UTSYS (fra sjef PU til juridisk seksjon). Når POD delegerer behandlingsansvaret for GTK til Øst politidistrikt gis dette ansvaret til politidistriktet som sådan og ikke til den avdeling, seksjon eller avsnitt som i det daglige skal utføre GTK-oppgavene i distriktet.

Sammenheng i regelverket – ENUs behandling av personopplysninger nasjonalt
Den nasjonale ETIAS-enheten (ENU) ved PU gis behandlingsansvaret for behandling av personopplysninger etter ETIAS-forordningens artikkel 57 nr. 2, dvs. for den behandlingen som skjer i det sentrale ETIAS-systemet. Dette er sagt både i forslaget til ny § 3-3 b i utlendingsforskriften og i forslag § 3 bokstav e, jf. også § 5 og § 6 bokstav c, i forslag til ny IO-forskrift.

Det sies imidlertid ikke noe om behandlingsansvaret for den behandling som vil skje i det nasjonale grensesnittet. Vi antar at forordningens artikkel 6 nr. 2 b) ikke er tilstrekkelig til å si at behandlingen som skjer nasjonalt også omfattes av det sentrale systemet, og dermed igjen av behandlingsansvaret etter artikkel 57 nr. 2.

Det vil være oppgaver som er lagt til ENU etter forordningens artikkel 8 som vil føre til at personopplysninger bare behandles nasjonalt og som ikke vil bli delt med det sentrale ETIAS-systemet. For eksempel vil store deler av den saksbehandlingen som skjer for å nekte en fremreisetillatelse etter forordningens artikkel 37 bare skje nasjonalt. Det er i dag POD som er behandlingsansvarlig for alle behandlinger etter personopplysningsloven i politiet, jf. Etatsinstruks for personvern (pkt. 6.2). Deler av behandlingen etter ETIAS-forordningen vil imidlertid reguleres av personverndirektivet og politiregisterloven, jf. artikkel 56.

Vi legger til grunn at behandlingsansvaret også for den nasjonale delen av behandlingen av ETIAS-opplysninger skal legges til ENU/PU, jf. pkt. 11.2 i PODs rundskriv 2023/006 *Informasjon om EUs informasjonssystemer.* Departementet bør vurdere å synliggjøre dette i den foreslåtte bestemmelsen i utlendingsforskriftens § 3-3 b første ledd. Slik vi leser denne bestemmelsen er behandlingsansvaret for den nasjonale behandlingen bare foreslått regulert for klagebehandlingen hos UDI, og ikke den innledende behandlingen hos ENU. At ETIAS-behandlingsansvaret vil gjelde både for sentrale og nasjonale behandlinger medfører nødvendigvis at rollen som behandlingsansvarlig blir mer krevende og komplisert. Etter vårt syn er dette ytterligere et argument for at behandlingsansvaret bør legges til PU, og ikke til ENU.

Praksis i andre EU-land
PU har vært i kontakt med Sverige, Danmark og Tyskland for å høre nærmere om hvordan disse landene har organisert seg og hvor behandlingsansvaret er tiltenkt å bli plassert.

Sverige har valgt en løsning hvor det er svensk politi (Swedish Police Authority – Polisen) som er styrende myndighet for ETIAS, og følgelig behandlingsansvarlig. Politiets interne retningslinjer vil være førende for organiseringen, men det er nærliggende at

behandlingsansvaret vil bli ordnet på samme måte som ellers – at ansvaret delegeres til den enheten som er nærmest den faktiske oppgaveutførelsen.

Tilbakemeldingen fra Danmark er at de er i dialog med sitt datatilsyn og ikke har landet på en endelig løsning. Det ligger an til at de vil organisere seg likt Sverige, dog slik at deres ENU vil ligge på departementsnivå. Det danske immigrasjon- og integrasjonsdepartementet er tiltenkt å være det formelle overhode for ENU. I den sammenheng vil departementet være behandlingsansvarlig. Danmark har ikke tatt endelig beslutning om de nærmere detaljer for organiseringen. Danske myndigheter melder at det er nærliggende å anta at organiseringen vil være lik andre medlemsland når det gjelder EU-informasjonssystemer.

I Tyskland er det besluttet at leder/sjef for ENU vil være den samme som sjef for etaten som ENU ligger til. Tyskland har besluttet at øverste leder for tysk føderasjonspoliti og dennes administrative enhet – nemlig det tyske datatilsynet skal være behandlingsansvarlig for ENU. Tyskland melder tilbake at de tolker reglene dithen at dette vil kun gjelde opplysninger som behandles i den sentrale ETIAS-systemet.

Oppsummert viser svarene fra de andre landene at ingen av dem per i dag har konkludert rundt plasseringen av behandlingsansvaret. Slik vi leser svarene trekker disse i retning av at behandlingsansvaret vil bli lagt til organets/virksomhetens leder, og ikke ENU som sådan.

Kort merknad til den foreslåtte bestemmelsen i utlendingsforskriften § 3-3 b
Når det gjelder foreslått ordlyd i ny § 3-3b i utlendingsforskriften, er vår vurdering at den ikke stenger for vår vurdering av plassering av behandlingsansvaret hos PU.

Imidlertid reiser PU spørsmål om ordlyden heller burde ha vært utformet slik:
"Politiets utlendingsenhet ved den nasjonale ETIAS-enheten er behandlingsansvarlig for behandling av personopplysninger i det sentrale ETIAS-systemet jf. forordningens artikkel 57 nr.2."

Av hensyn til den pågående beslutningsprosessen i POD kan det imidlertid være fornuftig å avvente utforming av den endelige ordlyden i forskriftsbestemmelsen[9].

6. Søk i CIR i medhold av artikkel 20 – høringsnotatets pkt. 4.4 og pkt. 5

6.1. Politiets behov for nasjonal hjemmel for søk i CIR

Søk i CIR kan benyttes ved brudd på identifikasjonsplikten overfor politiet
Det følger av artikkel 20 nr.1 at politimyndigheter kan gis adgang til å søke i CIR for identifiseringsformål når følgende omstendigheter oppstår:

- 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

[9] Se PODs henvendelse i brev av 04.12.23 - deres ref. 23/102389-6.

- det er tvil om identiteten til innehaveren av et reisedokument eller et annet troverdig dokument
- personen ikke kan eller vil samarbeide

Det følger av artikkel 20 nr. 5 at søkeadgangen forutsetter hjemmel i medlemslandenes nasjonale lovgivning og regelen må være utformet slik at tredjelandsborgere ikke forskjellsbehandles. Ved søk skal det angis til hvilke av formålene angitt i forordningenes artikkel 2 nr. 1 bokstav b og c, som tillater søk i CIR. Formålene er forebygge og bekjempe ulovlig innvandring og opprettholde offentlig sikkerhet og den offentlige orden, samt ivareta sikkerheten på medlemsstatenes territorier.

Det følger av artikkel 20 nr. 2 at man, bare med det formål å identifisere en person, kan søke i CIR med biometriske opplysninger. De må være registrert direkte under en identitetskontroll og fremgangsmåten må være innledet i personens nærvær.

Departementets forslag
Hjemmel for opptak av biometri og søk i CIR med identifiseringsformål inntas som ny bestemmelse i politiloven § 10 a, samt at det i forslag til interoperabilitetsforskrift[10], gis hjemmel for at også biometriske opplysninger opptatt med hjemmel i politiloven § 10 a kan benyttes til søk mot CIR.

Departementet skriver i høringsnotatet under punkt 5.1.3 at de er noe i tvil om den reelle nytteverdien for politiet av en slik bestemmelse, og at de derfor ikke har konkludert med om en slik hjemmel bør innføres. Departementet viser til at 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, men søk mot CIR vil ikke gi treff dersom personen er norsk statsborger eller EØS-borger. PU bemerker at det er korrekt, men den komplekse virkeligheten som utlendingsmyndighetene erfarer når det gjelder utfordringer med bruk av flere identiteter, også fordi flere kan ha doble statsborgerskap, gjør at dette kan nyanseres noe. Tredjelandsborger kan ha ervervet norsk statsborgerskap eller statsborgerskap i et annet EU-land. I Norge og de fleste land i EU kan man ha flere statsborgerskap, slik at det er helt legalt å beholde sitt opprinnelige statsborgerskap. Imidlertid er det slik at biometri fortsatt kan gi treff hvis personen benytter seg av sin tredjelandsidentitet.

Som eksempel kan nevnes at en borger av Syria kan ha ervervet svensk statsborgerskap, men søker deretter asyl i Danmark som syrisk borger, uten å gi informasjon sitt svenske statsborgerskap. Vedkommende får avslag og utreiseplikt, men kan enkelt unndra seg utreiseplikten. Vedkommende søker senere om asyl i Norge som syrisk borger. Det er korrekt at søk i CIR kun gir treff på identiteten oppgitt i Danmark, men ytterligere undersøkelser kan føre til at politiet oppdager at vedkommende også er EU-borger. Slike tilfeller er ikke ukjent for PU.

Det er også kjent modus at tredjelandsborgere kan utgi seg for å være EØS-borger ved bruk av falske dokumenter. De utøver EØS-rettigheter og registrerer seg som EØS-borgere med rett til opphold og arbeid i Norge. Noen ganger kan vedkommende ha reist inn lovlig på visum fra tredjelandet, eller være visumfri, og identitetsopplysningene vil således være i CIR. Hvis omstendighetene etter artikkel 20 nr. 1 oppstår og politiet søker mot CIR, vil det da avdekkes at vedkommende ikke er EØS borger.

---

[10] Forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for politisamarbeid og grense- og utlendingsforvaltning (punkt 7,5 i høringsnotatet)

Departementet foreslår 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. PU støtter forslaget om hjemmel for samtidig søk i foto- og fingeravtrykkregisteret, jf. politiregisterloven § 13 og politiregisterforskriften kapittel 46.

I forslag til ny politilov §10 a mener departementet at søk i CIR forutsetter at opptaket er basert på samtykke. Videre skal mulighet for søk kombineres med at vilkårene for innbringelse etter politiloven § 8 nr. 3 er oppfylt. PU mener at det ikke bør være krav om samtykke for opptak av biometri for søk i CIR. Kravet om samtykke understøtter ikke formålet med artikkel 20 som nettopp kan anvendes hvis personen ikke samarbeider. Vi viser til at en av de omstendighetene hvor det er aktuelt å søke mot CIR, vil være hvis personen ikke vil samarbeide. Personer som ikke ønsker å få avdekket at de benytter falsk identitet, vil neppe samtykke til opptak av biometri. Det er for øvrig noe vanskelig å forstå begrunnelsen om at vilkårene for innbringelse etter politiloven må være til stede. Hvis vedkommende motsetter seg det og innbringelsen går over i pågripelse etter straffeprosessloven eller etter utlendingsloven, vil politiet ha hjemmel for å oppta fingeravtrykk med tvang.

Søk i CIR kan benyttes ved behov for identifisering av ukjente personer ute av stand til å legitimere seg eller uidentifiserte menneskelige levninger
Det følger av artikkel 20 nr. 4 at politimyndigheter kan gis adgang til å oppta biometri og søke i CIR for identifiseringsformål når følgende omstendigheter oppstår:

- en naturkatastrofe
- ulykke
- terrorangrep

Departementet forslag:
Hjemmel for opptak og biometri inntas i politiloven § 12 som nytt sjette ledd. PU er enig i departementets vurderinger og støtter lovforslaget.

Når det gjelder lovgivningsteknikk foreslår departementet 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. Dette er inntatt i paragraf 2 i forslag til interoperabilitetsforskrift. PU mener at formålene i artikkel 2 nr. 1 bokstav b og c bør fremgå av teksten i bestemmelsen. Som nevnt ovenfor mener PU også at forskriftsbestemmelsen bør inntas i en egen IO-lov.

6.2. Oppsummert - benytte mulighetene som interoperabilitetsløsningene gir

Utviklingen i EU
Det kan vurderes om høringsnotatet kunne redegjort mer for det paradigmeskiftet som skjer i EU/Schengen når det gjelder regelverket om informasjonsutveksling på tvers av EUs informasjonssystemer og de tekniske løsningene. Både i Norge og EU erfares de globale utfordringene med migrasjonskriser, menneskesmugling, krig, terror og organiserte internasjonale kriminelle nettverk, som gir grunn til alvorlig bekymring for samfunnssikkerheten. Det er viktige og legitime formål å forebygge og bekjempe en slik

utvikling. I den sammenheng taler gode grunner for at Norge fullt ut benytter de virkemidlene som IO-forordningene vil gi for norsk politiarbeid. Noe annet kan gi en pull-effekt i form av at Norge kan fremstå som et attraktivt tilholdssted for personer som har tilknytning til kriminelle og ekstremistiske miljøer. Vi har ikke full oversikt, men har forstått det slik at mange av medlemslandene vil benytte seg av de muligheter som artikkel 20 gir og implementerer bestemmelsen i nasjonal rett. Det bør vurderes å redegjøre mer om dette i lovproposisjonen.

Personvernkonsekvenser
I høringsnotatet nevnes personvernkonsekvenser ved å gi politiet adgang til å søke med biometri mot CIR. PU mener som departementet at tiltaket er mindre inngripende enn å innbringe eller pågripe personen. Videre skal biometriopplysningene slettes straks etter at søket er gjennomført, og opptak og søk skjer mens personen er til stede.

PU bemerker at når personen plikter å medvirke til å opplyse sin identitet, samtidig som politiet skal informere om at det er frivillig å avgi fingeravtrykk for søk mot CIR, legger dette til rette for en del diskusjoner mellom tjenestepersonen og personen. Slike diskusjoner kan også være preget av språkbarrierer og det vil være behov for tolk eller andre hjelpemidler. Et krav om samtykke til medvirkning hvor personen plikter å samarbeide vil gjøre politiets identifiseringsarbeid mer ressurskrevende. Sett hen til at det ofte er lite legitime grunner til å motsette seg identifikasjonsplikten, mener PU at det ikke skal stilles krav om samtykke.

I denne vurderingen vises vi til at ved vedtakelsen av IO-forordningene og forordningene som reguler de underliggende informasjonssystemene i EU, er det eksplisitt lagt til grunn at forordningene er i samsvar med og ivaretar personvernreglene som følger av Forordning (EU) 2016/679, heretter GDPR og Europaparlamentets – og rådsdirektiv (EU)2016/680, heretter LED-direktivet /politidirektivet.

For IO-forordningene fremgår dette av fortalen. Behandling av personopplysninger skal skje på en måte som ivaretar personvernet og sikrer at behandling av opplysninger skjer i samsvar med GDPR og politidirektivet. Det vises til IO-forordningenes fortale, punkt 54 og 55.

7. Implementering av artikkel 20 for å understøtte PUs oppgaver

7.1. Søk mot CIR i ankomstfasen med formål tidlig identifisering

PU har ansvaret for å fastsette identiteten til asylsøkere. Det er en erfaring gjennom mange år at det er ganske få asylsøkere som fremlegger originale gyldige reise – og identitetsdokumenter samtidig med søknadsfremsettelsen. Unntak fra denne situasjonen har vært i masseankomstene i 2015 og krigen i Ukraina fra 2022. Asylsøkere fra land hvor det er et generelt beskyttelsesbehov eller når søker omfattes av kollektiv beskyttelse jf. utlendingsloven § 34, fremlegger i all hovedsak dokumenter.

Det å fremsette søknad om asyl fritar ikke søkeren fra plikt til å gjøre sitt beste for å fremlegge nødvendig dokumentasjon og medvirke til innhenting av nødvendige opplysninger, se utlendingsloven § 93 og § 83, jf. utlendingsforskriften § 17-7. Det fremgår av loven at utlendingsmyndighetene også har et selvstendig ansvar for å

innhente nødvendige og tilgjengelig opplysninger før vedtak blir truffet. Å vite korrekt identitet til asylsøkeren er viktig for at vedtaksmyndigheten skal kunne vurdere beskyttelsesbehovet. I ankomstfasen er det en sentral oppgave for politiet å avklare identiteten til søker og om søker allerede har internasjonal beskyttelse eller annen tillatelse i Schengen. I den forbindelse anvender PU politiets metoder for undersøkelser for å avklare søkers rette identitet, herunder søk i politiregistre og anvendelse av tvangsmidler. Dette er polisiært arbeid og PU opptrer som politimyndighet, se også vår redegjørelse foran om PUs samfunnsoppdrag i punkt 3.

PU mener det er gode muligheter for bedre informasjon tidlig i saken ved søk mot CIR med biometri. Gjennom søk mot CIR kan PU i saker med ID-tvil få bedre muligheter til å vurdere ytterligere tiltak der det ikke er treff på fingeravtrykk i VIS/Eurodac og når søkere ikke fremlegger ID-dokumenter, eller bildet i dokumentet er av en sånn kvalitet at det ikke med sikkerhet kan fastlås at det er samme person. Hvis søk mot CIR gir treff, vil PU kunne ha færre tvilssaker som krever ytterligere undersøkelser og økt ressursbruk. Søk mot CIR senere i saksløpet når en utlending ikke samarbeider om ID-avklaring, kan også gi treff i CIR.

Slik forslaget til politiloven § 10 a er uformet er bestemmelsen mindre anvendelig for PU i ankomstfasen. PU anbefaler at det ikke innføres vilkår om at det skal være grunnlag for innbringelse etter politiloven § 8 nr. 3 og et krav om samtykke. Hvis forslaget opprettholdes med disse begrensningene, mener PU at opptak av biometri og søk mot CIR også bør implementeres i utlendingsloven § 100, se punkt 9.

7.2. Søkt mot CIR for identifisering av utlendinger med utreiseplikt og i arbeidet med tvangsretur

Utlending med avslag og langvarig ulovlig opphold
I disse sakene kan nytt opptak av biometri for søk i CIR bidra til å avdekke identiteten på vedkommende. Følgende sak gir et godt eksempel på dette:

Utlendingen søkte asyl i Norge i 2017 og fikk endelig avslag i 2018. Hun hadde ikke innlevert ID-dokumenter til PU ved søknad. Etter avslag hadde hun ikke fremskaffet gyldige reisedokumenter, i strid med sin plikt etter utlendingsloven § 90 syvende ledd. I 2022 fikk politidistriktet tips om at utlendingen hadde bodd og arbeidet i Hellas i hele 18 år under en annen identitet enn den hun hadde oppgitt til norske myndigheter.

Basert på denne informasjonen ble det sendt et artikkel 34-søk etter Dublin-forordningen. Hellas svarte at utlendingen var kjent under to identiteter i Hellas. Interpol Athen ble anmodet om ID-verifisering av disse identitetene og PU mottok kopi av pass i den ene identiteten.

Ved å benytte søk mot CIR i PUs arbeid med retur, ville disse opplysningene umiddelbart fremkommet. Det kan ta lang tid å få svar på artikkel 34, og det må også være noen holdepunkter for at det sendes artikkel 34 søk til det enkelte land.

Tilbakekallssaker
Søk i CIR i arbeidet med tilbakekallsaker kan bidra til å løse enkeltsaker. I tilbakekallssaker jobber politiet med å avdekke tillatelser som er gitt på uriktig grunnlag, ofte med bruk av uriktig identitet. Søk i CIR vil være et nyttig virkemiddel. Det vil kunne bidra til å finne en persons riktige identitet. Det forekommer at personer som oppholder seg i Norge også har oppholdstillatelse i annet europeisk land, og da gjerne utstedt i den riktige identiteten. I disse tilfellene er det ikke hensiktsmessig at søkemuligheten i CIR

avgrenses til å gjelde samtykke, da det ikke vil være i personens interesse å samarbeide om avklaring av korrekt identitet.

PUs deltakelse i Frontex-samarbeidet – retur i regi av Frontex
PU bruker Return Case Management System (RCMS) i Bangladesh og har bedt om å få ta i bruk RCMS i Pakistan. RCMS er en dataplattform som brukes for å sende elektroniske anmodninger om ID-verifiseringer med det formål å få utstedt reisedokument, som igjen vil muliggjøre en retur til hjemlandet. Dataverktøyet er finansiert av EU, men eies av hvert enkelt tredjeland der systemet er tatt i bruk.

Medlemsland i EU+ som bruker RCMS i forskjellige land kan ikke se hvilke identiteter andre land har søkt om verifisering på. Det har via Frontex kommet tilbakemeldinger fra tredjeland om at de fra ulike land i Europa mottar forespørsler om samme person, men med ulike identitetsopplysninger. Dette er en av grunnene til at verifiseringer i RCMS-sporet tar tid og kan være ressurskrevende. Søk mot CIR på forhånd vil kunne avhjelpe dette. Avsender av den originale anmodningen vil da være eneste motpart for mottakerlandet. Andre land som får treff i CIR vil kunne supplere avsender av den originale anmodningen med nye opplysninger.

PU er også i ferd med å ta i bruk det Frontex støttede programmet Joint Reintegration Service (JRS), der det er mulig å søke reintegreringsstøtte for returnerte, også tvangsreturnerte. Det kreves at saksbehandlerverktøyet ReIntegration Assistance tool (RIAT) brukes. Også her vil det kunne være mulig for en utlending å søke reintegreringsstøtte under forskjellige identiteter fra ulike medlemsland. Det vil være gunstig at det nå skal være mulig å avdekke om personer har operert med flere identiteter i andre europeiske land.

8. Hvilke nasjonale myndigheter kan få tilgang til søk i CIR

Søk i CIR skal utføres av politimyndighet. Det gjelder søk både etter artikkel 20 nr. 1 og nr. 4.

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

Kystvakten
Etter kystvaktloven § 21 har Kystvaktens tjenestemenn begrenset politimyndighet og kan foreta etterforsking på nærmere bestemte vilkår. Det er i forslag til bestemmelser i politiloven ny § 10 a og § 12 nytt sjette ledd ikke lagt opp til at Kystvakten skal gis tilgang til å søke i CIR for identifiseringsformål. Departementet ber om innspill til om det er behov for slik adgang også for Kystvakten.

NKS[11] i PU har også ansvaret for Frontex' sårbarhetsvurdering for grensekontrollen i medlemslandene. I regi av denne vurderes årlig blant annet samhandlingen mellom etatene som er involvert i grensekontrolloppdraget. I forbindelse med dette er NKS kjent

[11] *NKS koordinerer informasjonsdelingen på operativt nivå mellom alle etater som arbeider med grensekontroll og migrasjon nasjonalt, og med Frontex (den europeiske grense- og kystvakt). NKS risikovurderer og kvalitetskontrollerer grensekontrollen, med hjemmel i EBCG forordningen (EU 2019/1896 section 3-5 art. 18-29 og art. 32-25)*

med at representanter fra Kystvakten har uttrykt behov for/ ønske om bedre systemstøtte for å kunne gjennomføre identitetskontroller om bord i fartøy.

En tilgang til ID-søk i CIR hjemlet i artikkel 20 nr. 1 i IO-forordningen vil kunne bidra til å dekke dette behovet. Kystvaktens behov for identitetskontroll og registersjekk for personer de kontrollerer, for eksempel i fiskerikontroller eller kontrolloppgaver på vegne av Toll, dekkes i dag ved at Kystvakten kontakter lokalt politidistrikt per telefon, og ber disse om å søke i registre ut fra oppgitte personalia. Dette gir en kvalitativt dårligere kontroll av person og oppholdsgrunnlag enn dersom Kystvakten fikk søke selv i systemene, da direkte søk også vil medføre bruk av biometri (foto og fingeravtrykk).

PU er kjent med at Økokrim med flere har rapportert om risiko for menneskehandel i fiskerinæringen og om bord på skip i norske farvann. Kystvakten kan potensielt sett bidra til å avdekke dette ved å gjennomføre identifikasjonssøk på mulige ofre om bord i skip de visiterer.

Kystvaktens behov og grunnlag for tilgang til søk i henhold til artikkel 20 nr. 1 kan knyttes til målene med forordningens søkeadgang i henhold til IO-forordningenes artikkel 2 nr. 1, særlig bokstav c, men også bokstav b. Videre kan en mulig tilgang for Kystvakten etter artikkel 20 nr. 4 begrunnes i artikkel 2 nr. 1 bokstav g. Kystvakten kan for eksempel være blant de første myndighetene som kommer over personer eller levninger som har vært utsatt for en ulykke til havs, og det kan da være hensiktsmessig at Kystvakten gjennomfører identifiseringssøk for å fastslå identiteten til vedkommende.

Forordningenes artikkel 20 nr. 1 gir *politimyndighet* tilgang til søk i CIR for identifiseringsformål. Hva som i denne sammenheng defineres som politimyndighet skal avklares gjennom nasjonal lovgivning. Forslaget til politilov ny § 10 a og § 12 nytt sjette ledd, samt ny interoperabilitetsforskrift § 2 avgrenser dette til *politiet*. Lovforslaget legger således ikke opp til at Kystvakten skal ha samme tilgang. Avgrensningen begrunnes ikke i høringsnotatet. Forsvaret, herunder Kystvakten, er en del av grensemyndigheten, jf. grenseloven § 6 og er slik som politiet ved utøvelse av sin grensemyndighet, ikke avskåret fra tilgang til søk i CIR.

Kystvakten kan bistå politiet i inn- og utreisekontroll i medhold av grenseloven § 15 eller i utlendingskontroll på territoriet i medhold av utlendingsloven § 21, jf. § 22. Dette er nærmere regulert i samarbeidsavtale mellom politidirektøren og sjef Forsvarets operative hovedkvarter vedrørende Kystvaktens kontroll på Schengen yttergrense av 11. mai 2011.

Kystvakten kan videre yte *annen bistand til politiet*, herunder i forbindelse med forebyggelse og bekjempelse av straffbare handlinger og ulovlige aksjoner mot personer, fartøyer eller faste innretninger, jf. § kystvaktloven 17 første ledd. De kan være forpliktet til å gjennomføre etterforskningsskritt ved mistanke om overtredelse av straffbare handlinger begått innenfor Kystvaktens jurisdiksjonsområde, jf. §§ 3, 12 og 17. Blant annet av den grunn er de tildelt begrenset politimyndighet. Kontrollen kan medføre behov for umiddelbar inngripen for å sikre bevis, eller for å ivareta liv og eller helse, og dermed også utøvelse av tildelt begrenset politimyndighet. Utøvelse av myndigheten skjer innen rammene for politilov og straffeprosesslov. Kontrollvirksomheten skjer normalt til sjøs uten tilstedeværelse av politiet. Tiltak som innbringelse, jf. politiloven § 8 nr. 3, eller pågripelse etter straffeprosessloven, kan medføre flere timers seilingstid til stedlig politi. Forholdsmessighetshensyn tilsier at tiltaket bør kunne avbøtes med tilgang også for *Kystvakten* til søk i CIR for identifiseringsformål i henhold til artikkel 20 nr. 1. Slik søkertilgang kan være tilstrekkelig til at personen kan dimitteres eller løslates på

stedet, og at videre seilas kan fortsette som planlagt. I tillegg tilsier hensynet til Kystvaktens generelle effektivitet i kontrollvirksomheten for øvrig en slik løsning.

Politiloven § 27 a første ledd regulerer adgangen for politiet til å anmode *Forsvaret* om bistand i særlig angitte situasjoner. Slike situasjoner dekkes i stor grad av de alternativer som er listet i forordningenes artikkel 20 nr. 4. Omfanget av en naturkatastrofe, ulykke eller terrorangrep kan vanskelig vurderes på forhånd, ei heller omfanget av behovet for politiets bistand fra Forsvaret i slike tilfeller. Et typetilfelle hvor omfanget av politiets behov for bistand fra Forsvaret kan være særlig stort er havari til sjøs av cruiseskip med flere tusen utenlandske passasjerer ombord.

Vi mener derfor at politiloven ny § 10 a og § 12 nytt sjette ledd bør åpne for at Forsvarets personell som er tildelt begrenset politimyndighet etter politiloven § 20 femte ledd eller kystvaktloven § 21 kan oppta biometriske opplysninger.

9. Kommentarer til endring i utlendingsloven § 100

PU er enig i forslagene til endring av utlendingsloven § 100.

Dersom departementet opprettholder at ny bestemmelse i politiloven § 10 a skal forutsette at vilkårene for innbringelse etter politiloven § 8 nr. 3 skal være oppfylt og at personen samtykker til opptak av biometri, mener PU at det i utlendingsloven § 100 også bør gis en bestemmelse om adgang til søk mot CIR, jf. artikkel 20 nr. 1. Vi viser til redegjørelse i punkt 3 om PUs rolle i ankomstfasen som politi for å avdekke korrekt identitet, og politiets arbeid med verifisering av identitet i arbeidet med tvangsretur. Se også redegjørelsen under punkt 7 om implementering av artikkel 20 for å understøtte PUs oppgaver.

Vi viser til at søk mot CIR for politiet i ankomstfasen og i forbindelse med verifisering og arbeidet med tvangsretur, samsvarer med formålene angitt i forordningene artikkel 2 nr. 1 bokstav b og c, som i henhold til artikkel 20 nr. 5 skal fremgå ved søk. Formålene er forebygge og bekjempe ulovlig innvandring og opprettholde offentlig sikkerhet og den offentlige orden, samt ivareta sikkerheten på medlemsstatenes territorier.

10. Økonomiske og administrative konsekvenser – høringsnotatets pkt. 6

PU finner det vanskelig å gi innspill til dette punktet i høringsnotatet. Det redegjøres for at Stortinget har vedtatt en felles kostnadsramme for informasjonssystemene hvor også kostnader til etterlevelse av interoperabilitetsforordningene inngår. Det informeres også om årlige anslåtte varige driftskostnader for politiet fra 2026. Dette er hovedsakelig knyttet til behov for opplæring, økte ressurser for å håndtere økt arbeidsmengde og drift av IKT-systemene. Høringsnotatet nevner ikke driftsmidler til videre utvikling av IKT-systemene. Det må påregnes at utviklingen går så fort at det også bør beregnes inn.

PU viser til det som vi har bemerket under punkt 3 om at interoperabilitetsforordningen vil føre til en betydelig mengde ny informasjon som skal behandles i den daglige oppgaveløsningen i politiet, primært i enkeltsaker hos grense– og utlendingsmyndigheten, men også i straffesaksbehandlingen. Med IO-forordningene følger også plikt til å rapportere og lage statistikk sentralt til EU, til euLISA og EU-kommisjonen. Vi kan ikke annet se enn at det er svært mange usikkerhetsfaktorer som

gjør det vanskelig å vurdere de økonomiske og administrative konsekvensene av reformen. Det bør tas høyde for denne usikkerheten i det fremtidige budsjettarbeidet.

Når det gjelder opplæring er det en forpliktelse etter forordningene at det skal gis nødvendig opplæring for brukerne av systemene. Det følger av POD rundskriv 2023/003 Informasjon om EUs informasjonssystemer at POD skal utarbeide sentrale planer for nødvendige opplæringstiltak for distriktene og særorganene. Det skal på lokalt nivå gis tilstrekkelig opplæring i informasjonsbehandling, arbeidsprosesser, regelverk og bruk av systemer. Krav til opplæring skal fremkomme i instruksene til hvert enkelt system. Det følger imidlertid av POD rundskrivet at politidistriktene også skal utarbeide egne rutiner som sørger for at kompetansen vedlikeholdes og utvikles. Vi legger til grunn at det også gjelder for særorganene som benytter interoperabilitetsløsningene.

Videre følger det av POD rundskrivet at ansatte som får tilgang til ett eller flere av EUs informasjonssystemer også har et selvstendig ansvar for å sette seg inn i gjeldende regelverk, rundskriv og instrukser. Dette taler med tyngde for at inkorporeringen ikke må skjer i form av en henvisningsbestemmelse i grenseloven og heller ikke at de ulike bestemmelsene gjengis i lov og forskrift med henvisning til artiklene i forordningene. Regelverket blir vanskelig tilgjengelig for brukerne i politiet. Vi viser til våre innspill om lovgivningsteknikk under punkt 4 og bemerker at hensynet til brukervennlighet ved utformingen av bestemmelsene faktisk vil kunne bidra til lavere kostnader.

Et innspill for å ivareta kunnskapen i politiet og ha brukerstøtte til hjelp i den daglige oppgaveutførelsen, vil være å etablere fagmiljøer på tvers i etaten. Det kan også vurderes om det bør opprettes et eget fagforvalterapparat for Interoperabilitet og EUs informasjonssystemer. Kostnader til dette må i så fall vurderes om det inngår i de allerede anslåtte årlige driftskostnadene.

I høringen står det at en "*rekke løsninger i dagens systemer i politier og utlendingsforvaltningen må tilpasses og videreutvikles*". Som nevnt ovenfor ser vi ikke at dette inngår i de årlige driftskostnadene fra 2026. Vi bemerker at løsningene som implementeres må være operasjonelt og fungere i praksis, men det forutsetter at brukerne tidlig involveres i utviklingsarbeidet. Det blir viktig at de ulike aktørene ikke setter i gang med utvikling av forskjellige løsninger, men at det så langt det går utvikles universelle løsninger som kan tas i bruk av de forskjellige aktørene og som lett kan tilpasses søkets behov og tilgangsstyres. Det må lages løsninger som er tilpasset den løsningen saksbehandler bruker som sitt arbeidsverktøy, for eksempel UTSYS. Det må også tilpasses arbeidssituasjonen til den som foretar informasjonsinnhentingen ved at det kan gjennomføres ved arbeidsstasjon til tjenestepersonen, hvor det er flere hjelpemidler tilgjengelig, eller ved en territorialkontroll ved bruk av mobile- eller håndholdte enheter.

Det er uklart om søk mot CIR vil innebære et ekstra opptak av fingeravtrykk, eller om det også kan inngå i noen av dagens systemer. Det er et stort behov for at når det utvikles ny teknologi og systemer som snakker sammen, at man også ser på hvordan de nye systemene skal fungere sammen med dagens løsninger i ulike prosesser hvor identitet skal avklares.

I denne sammenheng nevnes at allerede i 2016 utviklet PU en prototype på en app som forutsetter interoperabilitet, som er ment installert på politiansattes telefoner og som kunne registrere og saksbehandle søkere på stedet bare ved bruk av en mobiltelefon. Politiet vil ha stor nytte av å ta IO-teknologien i bruk. Det å etablere interoperabilitetsløsninger i flere av politiets systemer vil bidra til mer effektive kontroller

på territoriet, men også til å fremskaffe identitet på tredjelandsborgere langt raskere, i flere straffesaker enn i dag.

De administrative og økonomiske forhold ved søkertilgang for Forsvarets, herunder Kystvaktens personell som nevnt under punkt 8, kan PU ikke gi innspill om. Vi nevner bare at tilsvarende som for politiet vil det kreve opplæring, investeringer til utstyr, vedlikehold m.m.

Med hilsen

John Ståle Stamnes
Avdelingsleder

Jon Andreas Johansen
Seksjonsleder

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
Anne Karin Storhaug
Politiadvokat 2

POLITIET
KRIPOS

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:	Vår referanse:	Sted, dato:
23/278860	24/6558 - 2	Oslo, 29.01.2024

Høringssvar - forslag til gjennomføring av interoperabilitetsforordninger

Det vises til høringsbrev fra Justis- og beredskapsdepartementet av 21. desember 2023, samt brev fra Politidirektoratet av 9. januar 2024 med svarfrist til direktoratet innen 29. januar 2024.

Høringen gjelder gjennomføringen av interoperabilitetsforordningene forordning (EU) 2019/817 og (EU) 2019/818 – heretter IO-forordningene, samt etablering av nasjonale hjemler for opptak og bruk av biometriske opplysninger for identifiseringsformål.

Om valg av gjennomføring i norsk rett

De to forordningene er foreslått gjennomført ved inkorporering i grenseloven. Dette følger samme system som gjennomføringen av kildesystemene til interoperabilitet[1]. Kripos har forståelse for at det er utfordrende å innføre forordningene i eksisterende lovverk, og at det av den grunn velges inkorporering som metode for gjennomføring.

Samtidig skaper dette utfordringer, særlig fordi forordningene er omfattende og til dels har et vanskelig tilgjengelig innhold. Både hensynet til de som berøres av regelverket og til brukerne av regelverket tilsier et klart og tilgjengelig regelverk. Kripos kan ikke se at høringsnotatet foretar en fullstendig gjennomgang av de materielle bestemmelsene i forordningene. Departementet nøyer seg med å gi en beskrivelse av hva de ulike kapitlene i forordningene omhandler. Denne tilnærmingen gir liten veiledning for anvendelsen av regelverket, og gjør det vanskelig å tilegne seg formålet med og bakgrunnen for bestemmelsene i forordningene, som da vil gjelde som norsk lov.

Det er positivt at det foreslås å utferdige en egen forskrift som beskriver komponentene i interoperabilitet, samt plasserer behandlingsansvaret for behandling av opplysninger i de ulike komponentene.

---

[1] EES, ETIAS, VIS og Eurodac

KRIPOS
Post: Postboks 2094 Vika, 0125 Oslo / Besøk: Nils Hansens vei 25, 0667 Oslo / (+47) 23 20 80 00
kripos@politiet.no / www.politiet.no / Organisasjonsnummer: 974760827

Om behandling av biometriske opplysninger

Ved gjennomføringen av IO-forordningene utvides muligheten for å sikre rett identitet, samt at det innføres nye hjemler for ID kontroll i forslaget til politiloven § 10 a og § 12 sjette ledd. Dette støtter opp under nasjonal visjon om én person én identitet i nasjonale registre, som igjen bidrar til korrekte og oppdaterte personopplysninger som behandles til politimessige formål og forvaltning.

Med flere tilgjengelige hjemler og verktøy for ID-kontroll er det viktig at slik kontroll utføres systematisk i kontrollsituasjonene. Politiarbeid på stedet innebærer at politipatruljen skal utføre flere oppgaver og herunder etterforskningsskritt. Det pågår et arbeid med utplassering av flere opptaksstasjoner for biometriske opplysninger, såkalte Biometra-stasjoner, der man kan utføre hurtigsøk på fingeravtrykk for å sjekke identitet. Dette utstyret har derimot ikke funksjonalitet for hurtigsøk med ansiktsfoto, som de nye hjemlene åpner for. Dersom politiet skal kunne nyttiggjøre seg de nye hjemlene for id-kontroll fullt ut, krever dette utvikling og utrulling av utstyr.

Kripos vil også understreke at ID-kontroll på stedet ikke erstatter registrering av biometriske opplysninger, såkalt signalering, i straffesak. De nye hjemlene i politiloven forutsetter at opplysningene slettes idet kontrollen er ferdig, og gir ikke mulighet for lagring av den biometri som tas opp på stedet. Som kjent har politiet har store restanser når det gjelder signalering, og det er derfor viktig å understreke betydningen av at biometriske opplysninger fortsatt tas opp for registrering i politiets foto- og fingeravtrykkregister der hjemmelsgrunnlaget for signalering er tilstede. Det er sentralt at dette kommuniseres klart til brukerne, også når nye løsninger for hurtigsøk rulles ut.

Om personvern og behandlingsansvar

Som hovedregel gjelder personopplysningsloven når det behandles opplysninger etter forordningene. Unntak gjelder der opplysninger behandles av politi- og påtalemyndigheten for å forebygge, avdekke, etterforske og rettsforfølge terrorhandlinger og alvorlig kriminalitet. I disse tilfellene kommer LED-direktivet, og dermed politiregisterloven til anvendelse.

Slik Kripos forstår systemet er det ulike brukerprofiler i komponenten European Search Portal (ESP) som avgjør hvilke opplysninger aktuell tjenesteperson gis tilgang til ved søk i ESP. Gitt at tjenestepersoner i politiet håndterer oppgaver som omfatter både forvaltningsvirksomhet og politimessige formål, vil det være viktig at de tekniske løsningene som utvikles for søk i ESP gir god og tydelig veiledning for brukerne slik at de behandler opplysninger i henhold til riktig regelverk. I utgangspunktet skal opplysninger i kildesystemene (EES, ETIAS, VIS og Eurodac) bare være tilgjengelig for forvaltningsmessige formål. Dersom opplysningene skal behandles til politimessige formål må tjenesteperson rette en anmodning til det sentrale aksesspunktet på Kripos. For å sikre at opplysningene ikke innhentes ved direkte søk i ESP – uten at man går veien om det sentrale aksesspunktet - må den tekniske løsningen gi god veiledning slik at det er enkelt å velge rett brukerprofil basert på det aktuelle formålet med søket.

Å sikre rett identitet på personer som registreres i politiets registre er avgjørende for å sikre oppdaterte opplysninger med tilstrekkelig kvalitet, og med politiloven § 10a og § 12 sjette ledd gis politipatruljen nå en ny metode å sikre rett identitet på.

Når det skal utvikles en teknisk løsning for opptak og søk med biometriske opplysninger etter disse nye bestemmelsene mener Kripos det er sentralt å se på de ulike løsningene politiet har tilgjengelig for identitetsavklaring i sammenheng. I skrivende stund utvikles det en personkontrollapplikasjon med formål å søke opplysninger mot blant annet registrene for pass og id-kort for å fastslå rett identitet på person. Den samme funksjonaliteten har dagens grense- og territorialkontrollapplikasjon, som muliggjør

verifikasjon av identitet i forbindelse med grensekontroll og kontroll på territoriet. Videre er det ved Kripos utviklet funksjonalitet for søk med biometriske sporopplysninger mot opplysninger i passregisteret til bruk ved forebygging og etterforsking av seksuelle overgrep mot barn.

Biometriske opplysninger er en særlig kategori personopplysning både i henhold til GDPR og politiregisterloven, og skal dermed kun behandles etter særskilte vilkår. Når politiet etter hvert har flere ulike muligheter for søk med biometri mot ulike registre, er det viktig at det legges til rette for at tjenesteperson som skal utføre opptak av og søk med biometriske opplysninger settes i stand til å gjøre dette med riktig hjemmel og til rett formål. Med så mange muligheter for behandling av biometriske opplysninger mener Kripos det er sentralt at opplysningene behandles enhetlig og er underlagt de samme krav og vilkår uavhengig av hvilke verktøy som benyttes.

Behandlingsansvaret for opplysninger i forordningenes komponenter følger behandlingsansvaret for opplysningene i kildesystemene. I treffsituasjoner vil ofte opplysninger stamme fra ulike registre ettersom opplysninger mellom registrene skal sammenliknes. Med behandlingsansvar følger også blant annet ansvar for behandling av begjæringer om innsyn, retting, sletting og erstatning i forbindelse med behandling av opplysninger etter interoperabilitetsforordningene. Det fremstår som en krevende oppgave, som vil kreve organisering mellom de behandlingsansvarlige etater, å sikre at behandlingen følger behandlingsansvaret. Det antas at det vil kreve ytterligere regulering eller beskrivelser for å plassere dette ansvaret.

Konkrete innspill til de ulike kapitlene

Til punkt 3.1
I et avsnitt beskrives komponenten shared Biometric Matching Service (sBMS) som *"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)."*

Beskrivelsen er ikke helt korrekt. De ulike EU-systemene vil (fortsatt) ha de biometriske opplysningene, mens det er deres sammenligningstjenester som blir erstattet av sBMS. Altså skal sBMS ha en sentral infrastruktur hvor biometriske maler samles og lagres, og skal erstatte de biometriske sammenligningstjenestene i de sentrale systemene for biometriske opplysninger i EES, VIS, SIS, Eurodac og ECRIS-TCN.

Til punkt 3.3.2
Det er et krav at den enkelte medlemsstat selv skal føre logg over søk i interoperabilitetskomponentene foretatt av personale hos deres myndigheter.

Krav om loggføring av søk må ses i sammenheng med loggføring av opptak (opptak er en forutsetning for søk), og behov for notoritet som følge av dette. Vi mener at det er behov for en bedre avklaring av både hvilke opplysninger som skal loggføres, og hvilke opplysninger som skal slettes og når. En slik avklaring kan for eksempel inntas i lovproposisjonen.

Til punkt 3.3.3
I beskrivelsen av sBMS kommer det ikke fram hvilke biometriske data/opplysninger sammenligningstjenesten skal inneholde. Det bør for ordens skyld presiseres at sBMS vil inneholde ansiktsfoto og/eller fingeravtrykk, slik at det ikke gis inntrykk av at den vil inneholde andre type biometriske opplysninger, som for eksempel DNA. Dette foreslås også presisert i lovproposisjonen.

Til punkt 5.1
Kripos mener det er positivt at det innføres en nasjonal hjemmel for søk i CIR (Central Identity Repository) for identifisering av personer som er ute av stand til å legitimere seg, av levninger etter naturkatastrofe, ulykke eller terrorangrep samt ved brudd på identifikasjonsplikten. Ved brudd på identifikasjonsplikten vil et slikt søk vil gi muligheter for direkte tilgang til opplysninger som ellers ikke er tilgjengelig for direkte søk for politimessige formål.

Når det gjelder kravet om samtykke for opptak av biometriske opplysninger til identifiseringsformål mener Kripos dette i liten grad er begrunnet i høringsnotatet. I punkt 5.1.3 anføres det at en mulighet for opptak av biometriske opplysninger og søk mot CIR vil kunne bidra til å effektivisere politiets arbeid, og til at man vil kunne unngå unødige innbringelser etter politiloven § 8 nr. 3. Dette er Kripos enig i. Vi er derimot ikke ubetinget enig med departementet i at en innbringelse og eventuell tilbakeholdelse i fire timer vil være et mindre belastende tiltak enn at en person må avgi biometriske opplysninger til bruk for et identifikasjonssøk uten å samtykke. Dette standpunktet fra departementet synes i liten grad er begrunnet. En regel som forutsetter samtykke antas klart mindre effektiv i de tilfeller hvor den det gjelder faktisk ikke ønsker å bidra til rett identifisering. Riktig identitet er en viktig forutsetning for forsvarlig behandling av personopplysninger i de systemer som utvikles og benyttes av all offentlig myndighet. De biometriske opplysninger som skal opptas i disse tilfelle skal ikke lagres. I lys av dette stiller vi spørsmål ved om et slikt krav til samtykke er nødvendig, forholdsmessig og formålstjenlig.

Vi savner også en nærmere omtale av hvordan en eventuell samtykkeregel er tenkt implementert og praktisert. Et slikt eventuelt samtykkekrav til id-kontroll etter politiloven må harmoniseres med andre krav til loggføring, notoritet og kvitteringsordninger. Formålet med hjemmelen må være at politiet i praksis kan utføre ID-kontrollene på en enkel, enhetlig og effektiv måte. Det er da viktig å utrede hvordan ID-kontrollprosessene og etterfølgende prosesser skal gjennomføres, og deretter utvikle systemstøtte som sikrer en enhetlig løsning.

Til forslaget til politiloven § 10 a

For å tydeliggjøre formålet med den nye bestemmelsen foreslås det å endre overskriften til "*Opptak av biometriske opplysninger for identifiseringsformål*".

For å sikre et best mulig grunnlag for å få treff på registrerte biometriske opplysninger i nasjonale registre mener Kripos at bestemmelsen – i tillegg til søk i politiets foto- og fingeravtrykkregister - også bør omfatte søk mot registrene for pass og id-kort, samt mot utlendingsdatabasen. Dersom man velger å åpne for biometriopptak til bruk for identifiseringsformål innen de rammer som oppstilles i ny § 10a, er det sentralt at de biometriske opplysningene utnyttes så effektivt som mulig for nettopp slikt identifiseringsformål. Søket bør da ikke begrenses til kun politiets foto- og fingeravtrykkregister, men også omfatte de andre sentrale, nasjonale registre med identifiseringsformål, i særlig grad registrene for pass- og id-kort, samt utlendingsregisteret. Vi kan ikke se at en begrensning til foto- og fingeravtrykksregistret er nærmere begrunnet i høringsnotatet, og mener bestemmelsen bør utvides til også å hjemle søk mot registrene for pass og id-kort.

Til forslaget til forskrift om interoperabilitet

I forslaget til § 2 *Tilgang til felles identitetsregister* foreslår vi å endre ordet "*innhentes*" til "*opptas*" i første ledd andre setning. I § 2 andre ledd foreslås det tilsvarende å endre ordet "*innhentet*" til "*tatt opp*". Det gjenspeiler terminologien i politiloven § 10 a.

I forslaget til § 3 *Behandlingsansvar* bør det fremkomme at UDI er behandlingsansvarlig for opplysninger etter returforordningen, jf. SIS-loven § 4.

Med hilsen

Kristin Ottesen Kvigne

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
Eyvind Aavatsmark Berg
saksbehandler

POLITIET

Møre og Romsdal politidistrikt

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:	Vår referanse:	Sted, dato:
23/278860	24/6991 - 2	Ålesund, 30.01.2024

Høring - Forslag til gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer mm

"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

Innledning....1
Pkt. 4.1– Inkorporering i Grenseloven av 2021....1
Pkt. 4.2 - Forslag om ny forskrift om interoperabilitet....3
Pkt. 4.4.2 – Tilgang til søk i CIR for Kystvakten....3
Pkt. 5.1.3 - Krav om samtykke....5

Innledning

Det vises til epost av 12. januar om innspill til høringssvar om inkorporasjon av EUs forordninger om interoperabilitet.
Møre og Romsdal Politidistrikt har i denne forbindelse valgt ut fire punkter å kommentere på. Momenter som ikke omhandles i dette innspillet må derfor anses som støttet ut fra en helhetsvurdering.

MØRE OG ROMSDAL POLITIDISTRIKT
Post: Postboks 1353 Sentrum, 6001 Ålesund / Besøk: Nedre Strandgate 50, 6001 Ålesund / (+47) 70 11 87 00
post.moreogromsdal@politiet.no / www.politiet.no / Organisasjonsnummer: 974764113

Pkt. 4.1– Inkorporering i Grenseloven av 2021

Departementet anfører i dette punkt et forslag om at forordningene gjennomføres i norsk rett ved inkorporasjon, i form av en henvisningsbestemmelse som gjør forordningene til norsk lov uten omskrivninger. Dette foreslås innført i eksisterende Grenselov paragraf 8.

Det anses at det er både fordeler og ulemper med dette. Fordelen vil være at det ved senere endringer og oppdateringer av Interoperabilitetsforordningen, ikke vil være behov for å endre norsk regelverk da inkorporeringen vil vise til det til enhver tid gjeldende regelverk.

Det anses at denne fordelen blir overskygget av det faktum at et slikt verktøy med stor sannsynlighet vil forbli ukjent for majoriteten i politiet. Mulighetene som eksisterer i dette systemet både med tanke på arbeidet til operative mannskaper, etterforskere og etterretning, vil bli mindre kjent og dermed ikke utnyttet som tilsiktet. Systemet vil dermed for Norsk politi, ikke bli det verktøyet man ønsker å innføre for å oppnå måloppnåelse som beskrevet i forordningens Art. 2 bokstav (c), (f) og (g).

Bakgrunnen for denne antakelsen er mange års erfaring med at majoriteten i Politietaten, både polititjenestemenn og tjenestemenn i påtalemyndigheten faktisk ikke kjenner til verktøyene og mulighetene som eksisterer gjennom benyttelse av lovverk og muligheter i utlendingslov, grenselov og ellers på utlendingsfeltet pr. i dag og faktisk ikke benytter seg av disse. Dersom man legger et verktøy, som må anses som et enormt fremskritt og mulighet for alle som arbeider med oppgaver som på et tidspunkt medfører behov for korrekt identifisering av personer, inn under regelverk som i hovedsak benyttes av grense og utlendingsforvaltning, vil det dessverre bli gjemt og usynlig. Regelverket og mulighetene som ligger i søkemulighetene vil ikke anses som relevant og kjennskapen vil forbli for de spesielt interesserte.

Den beste måten å gjøre dette på, vil være å etablere en egen Interoperabilitets lov og heller vise til denne i annet lovverk. På denne måten blir det en lov juristene må forholde seg til selv om de ikke arbeider på et utlendingsfaglig område. Behovet for å kjenne til en lov som åpner for muligheter vedr. identifisering vil appellere til flere da den åpner muligheten for tiltak i operativt arbeid, i etterforskning og i etterretningssammenheng. Av åpenbare grunner vil denne loven uansett være kjent for mannskaper innenfor grensekontroll og utlendingskontroll.

Når det gjelder tilgjengeligheten for andre etater legges det til grunn at som egen lov, vil den også bli langt mer tilgjengelig og anvendbar for andre etater som har en oppgave inn mot identitetskontroll, ved at den ikke vil oppfattes så tett og eksklusivt knyttes til grensekontrollarbeid og politiet.

De av oss som er brennende opptatt av fagfeltet kan gjerne mene noe annet, men faktum er at i distriktene er de fleste tjenestemenn fokusert på det de gjør til daglig, og dersom noe anses som utenfor deres tjenesteområde, er det ikke kutyme for å utforske muligheten dette gir. Bakgrunnen for dette er somregel usikkerhet og manglende kjennskap og informasjon. Usikkerhet og manglende kjennskap til muligheter vil medføre at tiltak ikke gjøres og at personer derfor ikke identifiseres. Dette er i mange tilfeller av frykt for å kontrollere eller innbringe personen unødig. En slik handling vil medføre mindre tilgjengelig operativ kapasitet på gata i en periode. I frykt for at egen manglende kompetanse skal medføre en ulempe for en reisende, er det ikke ukjent at en usikker betjent velger å overse et avvik i den tro at avviket skyldes at tjenestepersonen selv har gjort en feil.

Ved å gjøre dette til en egen lov vil langt flere jurister bli oppmerksomme på muligheten, informere om og etterspørre tiltak, både i kontrollsituasjonen og i avhørssammenheng. Dersom jourhavende kontaktes i en situasjon hvor en person nekter å samarbeid vil det være avgjørende og betydelig mer effektivt og en sikring av rettssikkerheten dersom disse kjenner til muligheten til å oppta biometri og gjennomføre søk i CIR med biometri eller alfanumerisk informasjon i kombinasjon med reisedokument informasjon. Dette vil medføre en raskere dimittering av personer politiet ikke har grunnlag for å kontrollere ytterligere.

I enkelte tilfeller vil den kontrollerte ikke være i stand til å samarbeide og i andre tilfeller vil den kontrollerte nekte å samarbeid eller sågar motarbeide politiet. Dette medfører at Jourhavende jurist må ha kjennskap til dette regelverket for å vite hva som kan gjøres og hvilke muligheter man da har til å avklare rett identitet.

I en ideell verden burde ikke lovens plassering ha noen betydning, men vi kan vel fastslå at denne verden ikke er ideell.

MRPD foreslår å etablere en egen Interoperabilitets lov fremfor inkorporering i grenseloven.

Pkt. 4.2 - Forslag om ny forskrift om interoperabilitet

Det foreslås ny forskrift om interoperabilitet mellom felleseuropeiske informasjonssystemer for grensepassering, utlendingsforvaltning og politisamarbeid, dette foreslås gjort med hjemmel i Grenseloven § 25 nr. 12 og ny nr. 13.

Slik MRPD ser det, vil denne forskriften medføre regulering i flere lover og forskrifter av samme område. Handlinger og tiltak som er vist til i høringsnotatet er tiltenkt regulert i en slik forskrift vil også være omhandlet i annet lovverk. Dette fremstår som dobbeltarbeid som kan medføre usikkerhet om hva som er hjemmel for det enkelte tiltak på et senere tidspunkt. Man vil i en slik situasjon også kunne erfare at når lover og forskrifter endres og oppdateres, vil det medføre usikkerhet dersom ikke alle lovendringer gjøres samtidig.

Fagfeltet grensekontroll har en del erfaring med et fragmentert regelverk, hvor lovregler, rundskriv og annen informasjon til tider står i strid til hverandre og hva som er rett til tider er vanskelig å fastslå for politiet.

MRPD anbefaler at forslaget om å opprette en egen interoperabilitetsforskrift slettes.

Pkt. 4.4.2 – Tilgang til søk i CIR for Kystvakten

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.

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 vises i denne sammenheng til Artikkel 2 i Interoperabilitets forordningen, som blant annet oppgir at målet med forordningen er forbedre formålstjenligheten og effektiviteten av inn- og

utreisekontrollen ved de ytre grensene, forbedre gjennomføring av den felles visumpolitikken og bidra til å forebygge, avsløre og etterforske terrorhandlinger og andre alvorlige straffbare forhold.

Forsvaret, herunder Kystvakten, er en del av grensemyndigheten, jf. grenseloven § 6. Norge benytter i dag forsvaret, representert ved Garnison Sør Varanger (GSV) langs vår yttergrense land til å gjennomføre yttergrensekontroll og overvåkning. På lik linje benyttes forsvaret ved Kystvakten til å ha oppsyn og gjennomføre kontroll på vegne av politiet for Norge og resten av Schengen landene ved vår yttergrense sjø. Det er åpenbart at tilgang til søk i CIR vil effektivisere og styrke GSV sin kontroll ved landegrensen dersom de påtreffer personer i grensenære områder. Kystvakten vil også, med en slik søkemulighet i CIR, oppleve å bli styrket og deres arbeid effektivisert og gjort mer treffsikkert.

Dette vil også gjelde for alt det arbeidet Kystvakten med bakgrunn i samarbeidsavtale mellom politidirektøren og sjef Forsvarets operative hovedkvarter vedrørende Kystvaktens kontroll på Schengen yttergrense av 11. mai 2011, bistår politiet med når de deltar ved utlendingskontroll på territoriet i medhold av utlendingsloven § 21.

Kystvakten håndterer 21 lover og forskrifter på vegne av andre myndigheter. Kontrollvirksomheten skjer normalt til sjøs uten tilstedeværelse av politiet. I denne forbindelse utføres det både operativt arbeid i kontrollsituasjoner hvor personer anholdes, pågripes, anmeldes og fraktes til en politilokasjon. En slik innbringelse, jf. politiloven § 8, eller pågripelse, jf. straffeprosessloven § 173 annet ledd, kan for Kystvaktens fartøyer medføre flere timers seilingstid.

Kystvakten er en etablert samarbeidsaktør i redningsoperasjoner som er følge av f.eks. ulykker og terrorhandlinger, både på land og til vanns. I denne forbindelse vil tilgang til mulighet for rask identifisering av passasjerer og mannskap være av stor betydning. Et tilfelle hvor omfanget av politiets behov for bistand fra Forsvaret kan være særlig stort er havari til sjøs av større fisketråler, cargo fartøy eller i verstefall et cruiseskip med flere tusen utenlandske passasjerer ombord.

Forholdsmessighetshensyn tilsier at det bør gis tilgang også for *Kystvakten* til søk i CIR for identifiseringsformål iht. artikkel 20. Slik søketilgang kan være tilstrekkelig til at personen kan dimitteres eller løslates på stedet, og at vedkommendes videre seilas kan fortsette i henhold til plan. I tillegg tilsier hensynet til Kystvaktens generelle effektivitet i kontrollvirksomheten for øvrig en slik løsning.

I all etterforskning er det viktig for rettssikkerheten at Kystvakten på lik linje med Politiet, ved gjennomføring av intervju eller avhør forsikrer seg om at de snakker med rett person. I denne forbindelse er en identitetskontroll helt avgjørende. I slike situasjoner kan Kystvakten på lik linje med politiet komme opp i situasjonen at det reises tvil om identiteten som er oppgitt og Kystvakten på lik linje med politiet kan oppleve at den anholdte personen ikke samarbeider.
Da Kystvakten i slike situasjoner er å anse som politiets forlengede arm, vil det være naturlig at de også har tilgjengelig de virkemidler politiet har i samme situasjon. Det vurderes som kontraproduktivt å begrense en myndighet som faller inn under målgruppen i forordningens fortale nr. 1, 15, 25, 28, m.fl.

Enkelte tiltak er forbeholdt politiet, men et virkemiddel som er ment å effektivisere identitetskontrollen og tilgjengeliggjøre informasjon innhentet fra andre systemer for å understøtte nettopp identifisering og verifisering av rett identitet og legalitet av opphold og inn-/utreise ansees naturlig å kunne benytte seg av.

Slik MRPD har oppfattet det, vil Kystvakten på sikt gis mulighet til å gjennomføre grensekontroll og registrering i EES systemet. Dette fordrer tilgang til andre EUIS systemer også, og i denne sammenheng fremstår det enda mer uforståelig at Kystvakten skulle unntas tilgang til søk i CIR på lik linje med politiet under utøvelse av sine oppgaver, som gjøres på vegne av politiet.

I tillegg til et åpenbart behov for tilgangen av oppgavestyrte hensyn, vil en slik tilgang for Kystvakten forhindre at personer som anholdes, kontrolleres eller er gjenstand for etterforskning, utsettes for ytterligere ulempe ved å måtte tåle anholdelse og påfølgende innbringelse for å fraktes til lokasjon hvor politiet befinner seg for å gjennomføre ID kontroll og opptak av biometri for søk i CIR. Man vil dermed slippe tidkrevende transportoppdrag for kystvakten ved at disse vil kunne utføre denne kontrollen på egenhånd. Dette vil være i tråd med forordningens formål om effektivisering og det vil også sikre ivaretakelse av enkeltpersoners rettigheter på en bedre måte enn en innbringelse for å avklare identitet vil være. Det legges til grunn at dette vil være i tråd med generell rettsoppfatning i befolkningen og en måte å unngå unødig bruk av forsvarets ressurser.

MRPD foreslår at Kystvakten også gis mulighet til å oppta biometrisk informasjon i hensikt å gjennomføre søk mot CIR.

Pkt. 5.1.3 - Krav om samtykke

Departementet foreslår i høringsnotatet en ny bestemmelse i Politiloven §§ 10a og 12. Dette gjøres for å imøtekomme IO forordningens bestemmelse i Art. 20 om nasjonal hjemmel for innhenting av biometrisk informasjon for sammenlikningsformål. Dette er etter MRPD sin mening et meget godt forslag som i all hovedsak støttes.

Det som i denne sammenheng stilles et spørsmål ved, er forslaget om at opptak av biometrisk informasjon skal betinges av et informert samtykke.

Informert samtykke og nedtegning

Møre og Romsdal politidistrikt har følgende kommentarer til dette. Første tilfelle er hvor kontrollert person ikke er i stand til å samarbeide eller hjelpe til med egen identifisering, da kan man i de fleste tilfeller legge til grunn at en slik mulighet for identifisering vil være kjærkommen, og samtykke er enkelt å få.

Andre tilfeller er i situasjoner hvor personen har uttalt at å samarbeide med politiet om avklaring av egen identitet ikke er ønskelig. Det fremstår da kunstig å skulle be om samtykke og samarbeid av personen som nettopp har tydelig gjort det klart at samarbeid for å avklare egen identitet ikke er aktuelt. Når man da fortsetter samtalen med å spørre om samtykke til å la politiet oppta biometrisk informasjon i den hensikt å avklare vedkommendes identitet, kan dette fremstå som provoserende og som om politiet ikke registrerer og tar hensyn til det vedkommende nettopp har sagt.

For at samtykke skal være informert, må formålet med innhentingen og benyttelsen av biometrisk informasjon forklares på en slik måte at vedkommende forstår hva som skal skje, hvordan informasjonen innhentes, hvorfor og evt. konsekvensen av dette. Det er ikke usannsynlig at dette må formidles med tolk og at vedkommende må motta informasjonen skriftlig. Dette utgjør både en kostnad, det tar tid å vente på tolk og deretter gjennomføre samtalen med tolken og den kontrollerte. Det påfallende med kravet om samtykke, er da som nevnt at det er jo akkurat dette den kontrollerte personen har uttalt at ikke er aktuelt å samarbeide om.

Det fremgår videre at et muntlig samtykke umiddelbart skal nedtegnes av politiet.

Dersom informasjonen skal nedtegnes, må dette oppbevares, enten i original eller digitalt. Et samtykke skal også kunne trekkes tilbake, dette kan bli vanskelig i praksis.

Å kreve samtykke i en slik situasjon vil fremstå som en byråkratisk hemsko som medfører tidkrevende merarbeid for politietaten ved utførelse av en oppgave som er ment å effektivisere politiets arbeid, eksemplifisert ved de praktiske forholdene som er vist til over og som må tas hensyn til.

Ikke krav i forordningen

Ved gjennomgang av IO forordningene, vises det til at dette ikke er et tiltak som anbefales i interoperabilitetsforordningen, hverken som del av fortalen eller innlemmet i artiklene i forordningene.

Fortalens pkt. 30 oppgir at medlemsstatene bør fastsette fullmakten til innhenting og opptakelse av biometrisk opplysninger under en identitetskontroll av person i nasjonal rett. Det antas at Politilovens nye bestemmelse i § 10a vil være dekkende for dette formålet. Det vises ikke til noe behov for samtykke fra den kontrollerte for innhenting av biometrisk informasjon.

IO Forordningens art. 20 krever ikke innhenting av samtykke, men viser til at prosedyren skal innledes i personens nærvær og som det fremgår av fortalens pkt. 28 angis det at fingeravtrykk skal opptas med teknikk for direkteskanning. Det er i denne forbindelse ikke snakk om opptak av biometrisk informasjon eller alfanumerisk informasjon for lagring, dette er en kontroll av den inngitte informasjon som benyttes for å kontrollere om den stemmer overens med den lagrede informasjonen. Å måtte avgi biometrisk informasjon er en påregnelig og forventet konsekvens av å avgi slik informasjon i første omgang.

Det vises her til at ved innreise på Schengenområdet vil det jfr. Forordning (EU) 2017/2225 Annex V Part B bokstav (J) være grunnlag for bortvisning fra riket dersom tredjelandsborger nekter å avgi biometrisk informasjon i situasjoner hvor dette er påkrevd. Bakgrunnen for å avgi denne er å kontrollere om rett person reiser inn, oppholder seg på Schengenterritoriet og deretter forlater i henhold til reglene som gjelder for oppholdet på medlemslandenes territorium.

Som det fremgår av IO forordningens fortale pkt. 25 skal også CIR forenkle og effektivisere tilgang for myndigheter med ansvar for å forebygge, avsløre etterforske terrorhandlinger eller andre alvorlige straffbare forhold til de EU-informasjonssystemer som ikke er opprettet utelukkende med det formål å forebygge, avsløre eller etterforske alvorlig kriminalitet. Dersom man innfører en hindring for opptakelse av slik informasjon nasjonalt vil dette være et hinder for den forventede virkning av systemet.

Det vises til høringsnotatets pkt. 5.1.3 hvor det anføres at opptak av biometri og søk i register for å avklare og verifisere en identitet vil være langt mindre inngripende for en person enn innbringelse. I en tidskritisk situasjon hvor avklaring av en persons identitet er av største viktighet i forbindelse med kontroll av person mistenkt for grov og alvorlig kriminalitet og eller terrorisme, vil et krav om samtykke eller innbringelse dersom vedkommende nekter samtykke, legge beslag på politiressurser man i situasjonen burde anvende bedre. Å kreve samtykke i en slik situasjon fremstår som ubegripelig og som et hindrer for politiet å gjøre nytte av mulighetene gitt ved forordningens art. 20. Som nevnt tidligere fremstår det heller ikke som om dette var hensikten med bestemmelsen fra EU sin side.

Ujevnt maktforhold

Slik MRPD ser dette, vil et slikt behov for samtykke medføre at situasjonen blir noe den i utgangspunktet ikke er. Man befinner seg i en situasjon hvor statens maktapparat representert med somregel minimum to uniformerte betjenter, setter personen som kontrolleres i en situasjon hvor vedkommende under politiets påsyn, blir pålagt å umiddelbart velge mellom å samtykke til innhenting av biometrisk informasjon eller bli innbrakt til politistasjonen i inntil 4 timer. Altså å avgjøre mellom 2 for vedkommende uønskede handlinger.

Det som da fremstår som mer unaturlig er at man gjennom forslaget til ny politilov § 10a kan foreta seg handlinger som er langt mer inngripende uten samtykke for å gjennomføre identitetskontrollen. Innenfor Norsk forvaltningsrett har en også et prinsipp om "*fra det mer til det mindre*" der hvor man uten krav om samtykke kan foreta noe som er mer inngripende vil det være naturlig at man har tilsvarende adgang til å foreta noe som er mindre inngripende. Å bruke det mildeste inngrepet burde her være et naturlig valg da vi ikke bør gripe inn med strengere midler enn nødvendig, "*mildeste inngrepsprinsippet*".

Som departementet selv sier i eget høringsnotat under pkt. 5.1.3:" *Departementet erkjenner at det kan stilles spørsmål ved hvor frivillig samtykket er i en situasjon der alternativet er å bli innbrakt*". Det må vær på det rene at noe gyldig lovlig samtykke, kan umulig foreligg i en slik situasjon hvor maktforholdet er så skjevt.

Ivaretakelse av rettigheter og personvern

Det vises innledningsvis til at Interoperabilitetsforordningen allerede tar høyde for personvern gjennom anvendelse av GDPR regelverk og LED regelverk. Det er i tillegg i forordningen gitt egne artikler som påpeker viktigheten av informasjonssikkerhet og overholdelse av personlige rettigheter i forbindelse med registrering, retting og sletting av informasjon i systemet.

Som det fremgår av forordningens Art. 22 nr. 2.: "*Dersom svar på et søk i CIR viser at det finnes opplysninger om den personen i et av EU systemene som er del av Interoperabilitet pakken, må det anmodes om tilgang til denne informasjonen på vilkår etter fremgangsmåte i respektive rettslige instrumenter for slik tilgang".*

Dette viser at forordningen er skrevet med hensyn på ivaretakelse av rettigheter og retten til personvern. Det er ingen åpen tilgang til informasjon, selv for de som er gitt tilgang med henvisning til tjenstlig behov. Når man i norsk rett skal legge på et krav om samtykke utover det som er vurdert som nødvendig gjennom forordningene, kan man erfare at effektiviteten og muligheten som gis ved forordningens Art. 20, ofres.

MRPD sitt forslag er at hjemmelen i Politiloven for innhenting av biometrisk informasjon for søk og sammenlikning med CIR, utformes uten krav om samtykke. At politiet ønsker å sammenlikne den biometriske og alfanumerisk informasjon med det en person tidligere har avgitt vil bli forstått ansett som et forventet tiltak fra kontrollmyndighetens side. Et samtykke avgitt i en kontrollsituasjon som kan oppfattes som kritikkverdig, vil reise flere spørsmål enn svar og vil som nevnt gjøre situasjonen til noe den ikke er.

Med hilsen

Frank Knudtzon
Politioverbetjent

Mathias Häber
Politiadvokat

Dokumentet er elektronisk godkjent uten signatur.

8

POLITIET

Norwegian Police

Innlandet Politidistrikt

Til: Politidirektoratet
Fra: Innlandet Politidistrikt
Kopi til:
Saksbehandler: Ronny Samsonstuen

Dato: 29.01.24

Høringssvar: Forslag til gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer mm – Innlandet politidistrikt

Innlandet politidistrikt har følgende betraktninger til lovforslaget:

Inkorporasjon i grenseloven § 8, 1 ledd:

Det fremstår som noe forenklet å inkorporere en såpass stor endring som IO er i en allerede eksisterende lovgiving. For SIS ble det utarbeidet egen lov og det virker litt underlig at forankringen til IO også burde reguleres i egen lovgivning; altså en IO-lov.

Det bes derfor om at dette vurderes på nytt.

IO-forordningen artikkel 20, 2 ledd:

Under punkt 4.4.1 om identifiseringsformål heter det: *" Søk er ikke tillat for identifisering av barn under 12 år, med mindre det er til barnets beste".*

Alderskravet fremstår som noe ulogisk da det er nettopp identifisering som er formålet med kontrollen. Dette vil trolig skape problemer ved gjennomføring og virke mot sin hensikt hvis man tenker på situasjoner der man mistenker for eksempel barnebortføring. Det er heller ikke ytterligere konkretisert hva som menes med barnets beste så langt vi kan se.

Det er også en åpenbar utfordring å skulle avgjøre om en person er over eller under 12 år. Det må poengteres at hele formålet med kontrollen er å identifisere en person som mangler reisedokumenter eller få verifisert reisedokumenter. En konsekvens av dette kan være at grensekontrollørene også lar være å gjennomføre en identifisering av personer over 12 år når de er usikre på alder.

DISTRIKT/SÆRORGAN
Post: Adresse, Pb. 0000, NO-0000 Sted / Besøk: Adresse, NO-0000 Sted / (+47) 00 00 00 00
politi@politiet.no / www.politiet.no / 000 000 000

Politiloven § 10 a:

Under punkt 5.1.3 som gjelder opptak av biometriske opplysninger ved brudd på identifikasjonsplikten sier høringsnotatet at søk i CIR må være på bakgrunn av et samtykke.

Dette fremstår som uheldig etter vårt syn. Det man søker etter er informasjon som er avgitt frivillig og formålet er å klargjøre identitet. Søket blir heller ikke lagret. Alternativet er at personen blir innbragt til en politistasjon etter politiloven § 8, 1 nr. 3. Dette må være et større inngrep ovenfor den kontrollerte enn å avgi biometri på stedet. Dette mener vi må tillegges avgjørende vekt i denne sammenheng.

Det fremgår også av høringsnotatet at et samtykke skal nedtegnes av politiet på stedet eller være skriftlig. Dette fremstår for oss som vanskelig gjennomførbart i praktisk bruk. Skal man for eksempel opplyse om at hvis man ikke samtykker vil man bli innbragt til nærmeste politistasjon? Hvis man skal det kan man jo stille spørsmål om hvor frivillig et slikt samtykke egentlig er.

Til slutt vil vi påpeke at et velfungerende EUIS er avhengig av at medlemsstatene har tilnærmet lik forståelse av regelverket. Har man i arbeidet med denne lovendringen sett til andre medlemsstaters regelverk? Dette gjelder særlig med tanke på samtykke ved brudd på identifiseringsplikten og alderskravet på 12 år.

Med hilsen

Ronny Samsonstuen
Prosjektleder EUIS/politioverbetjent
Innlandet politidistrikt

POLITIET

Finnmark politidistrikt

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:	Vår referanse:	Sted, dato:
23/278860 - 3	24/6628 - 2	Kirkenes, 29.01.2024

Høring - Forslag til gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer mm

Vi viser til høringsbrev fra Politidirektoratet sendt 9. januar 2024 vedrørende forslag til gjennomføring av forordning (EU) 2019/817 og (EU) 2019/818 om interoperabilitet mellom felleseuropeiske informasjonssystemer mm.

Finnmark politidistrikt har følgende innspill til høringsnotatets forslag hva gjelder bruk av felles identitetsregister (CIR) i straffesak:

I høringsnotatet vises det til at bruk av søkeadgangen forutsetter hjemmel i medlemslandenes nasjonale lovgivning. Forordningens artikkel 22 regulerer søk i det felles identitetsregisteret med det formål å forebygge, avsløre eller etterforske terrorhandlinger eller andre alvorlige straffbare forhold.

Høringsnotatet viser til straffeprosessloven § 160, politiregisterloven § 13 og påtaleinstruksen kapittel 11 i relasjon til politiets søk i felles identitetsregister (CIR) for identifiseringsformål, men vurderer ikke forordningenes artikkel 22, og politiets og påtalemyndighetens adgang etter nasjonal lovgivning til bruk av det felles identitetsregisteret (CIR) under etterforskning og iretteføring av straffbare forhold.

Finnmark politidistrikt mener det må belyses hvorvidt dagens norske regelverk hjemler bruk av det felles identitetsregisteret (CIR) i straffesak. Dersom dagens norske regelverk ikke hjemler bruk av det felles identitetsregisteret (CIR) i straffesak, bør det utredes hvorvidt regelverket bør endres for å komme i samsvar med forordningene. Dersom det vurderes å være behov for endringer i norsk regelverk for bruk av felles identitetsregister (CIR) i straffesak, bør relevante hjemler inntas i eller i medhold av straffeprosessloven, framfor i forskrift med hjemmel i grenseloven.

FINNMARK POLITIDISTRIKT
Post: Postboks 501, 9917 Kirkenes / Besøk: Rådhussvingen 1, 9900 Kirkenes / (+47) 78 97 20 00
post.finnmark@politiet.no / www.politiet.no / Organisasjonsnummer: 984000049

Med hilsen

Ellen Katrine Hætta
Politimester i Finnmark

Dokumentet er elektronisk godkjent uten signatur.