POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Politiets utlendingsenhet

Deres referanse:	Vår referanse:	Dato:
22/223377-3	22/232479 - 3	12.01.2023

Høring - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport

Politiets utlendingsenhet (PU) viser til oversendelsesbrev av 24. november 2022 fra Politidirektoratet (POD), vedlagt Personvernkommisjonens utredning, NOU2022:11 Ditt personvern – vårt felles ansvar. POD ber om innspill til kommisjonens rapport. Vi viser også til PODs brev av 19. desember 2022. POD har satt høringsfristen til 13. januar 2022. Nedenfor følger tilbakemeldinger og innspill fra PU.

I Innledende bemerkninger

I oversendelsesbrevet viste POD til at det vil bli etablert en arbeidsgruppe som vil peke ut særlige temaer og problemstillinger som politiet bør kommentere på. En oversikt over aktuelle tema og problemstillinger var vedlagt PODs brev av 19. desember 2022. I brevet ble det vist til at arbeidsgruppen, hvor det også deltok representanter fra PU, hadde foretatt en gjennomgang av utredningen og identifisert tema og problemstillinger som det var ønskelig at politiet ga innspill til. Dette gjaldt særlig disse temaene:

- Opplæring, bevisstgjøring og kulturbygging
- Informasjonsdeling på tvers av offentlig forvaltning
- Revidering av politiregisterlov og -forskrift
- Forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom
- Utredning av politiets metodebruk

Videre skisserte arbeidsgruppen hvilke temaer og problemstillinger som særlige traff de ulike politienheter. For PUs del ble det vist til at det særlig var relevant å gi innspill til utredningens punkt 6.4.3.1 om uklare roller og ansvar i samarbeid der det deles personopplysninger.

Personvernkommisjonens utredning er et svært omfattende dokument som tar for seg kompliserte spørsmål og avveininger. Utredningen inneholder vurderinger som krever tid for å modnes og tid til å reflekteres over, for å kunne bidra med hensiktsmessige innspill til konklusjonene i rapporten og forslagene til tiltak. Sett hen til den korte høringsfristen, har vi ikke hatt anledning til å gjennomgå og kommentere i detalj på alle deler av utredningen. PUs tilbakemelding er i all hovedsak knyttet til noen utvalgte tema i utredningens kapittel 7 som

tar for seg personvern i justissektoren. Videre kommenteres også noen forhold i kapittel 6 om personvern i den digitale forvaltning. Vi har også noen generelle kommentarer til utredningen.

II Enkelte generelle kommentarer til utredningen

Om fremstillingen – nyanser og flere perspektiver om sentrale punkter
Kommisjonens utredning er omfattende og inneholder mer enn 140 anbefalinger og tiltak. Den har imidlertid en form og et nivå som gjør det vanskelig å gi innspill. Det er veldig mye i utredningen som er godt fundert og som det er enkelt å være enig i, for eksempel nevnes det som står under punkt 6.4.1.1 om at *"offentlig forvaltning har et særlig ansvar for å ivareta befolkningen tillit og at det krever grundige vurderinger av om formålet med viderebehandling av personopplysninger er forenelig eller ikke med det opprinnelige innsamlingsformålet og hvor stort inngrep viderebehandlingen innebærer*".

Til dette må det likevel bemerkes følgende: Innenfor justissektoren foreligger et omfattende regelverk for behandling av personopplysninger, for eksempel knyttet til politiets registre som reguleres av politiregisterloven med forskrift, i straffeprosessloven, i politiloven og også utlendingsloven. Når det gjelder bestemmelsene om behandling av personopplysninger i utlendingsloven nevnes at det legges til grunn at de er i overenstemmelse med GDPR og personopplysningslovens bestemmelser. Vi viser til at det gjennom flere år pågikk en lovutredning med flere høringsrunder, som resulterte i en egen formålsbestemmelse i utlendingsloven og forskriften om behandling av personopplysninger, samt en særskilt bestemmelse om utlevering av personopplysninger fra DUF (Datasystemet for utlending- og flyktningssaker), til politiet[1].

Kommisjonen kunne på flere punkter ha begrunnet sine anbefalinger og konklusjoner mer utførlig. Som eksempel nevnes et så sentralt tema som deling av opplysninger, og det mener vi er tilfelle for vurderingene under følgende punkter:

- Punkt 7.4.2.2 om "nedkjølingseffekt" på grunn av justissektorens søk i åpne kilder på nett.
- Punkt 7.1.2 om forholdet mellom personvern og kriminalitetsbekjempelse
- Konklusjonen under punkt 7.4.5.3 hvor kommisjonen anbefaler et generelt forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon offentlige rom

Om utviklingen i EU som vil føre til store endringer innenfor justissektoren
Regelverksutviklingen innenfor EU og Schengenområdet knyttet til grense- og utlendingsfeltet og utviklingen av EUs informasjonssystemer er ikke i særlig grad nevnt utredningen. Utviklingen i EU vil innebære store endringer for behandling av personopplysninger innenfor justissektoren i Norge. Vi viser til at de nye rettsaktene innebærer at formål med behandlingen utvides, det blir flere personopplysninger som skal registreres, utvidet plikt til deling av informasjon, samt tekniske løsninger for samhandling og utveksling av informasjon mellom systemene (interoperabilitet). Disse forordningene er Norge bundet av gjennom EØS-avtalen og vår tilslutning til Schengenavtalen. Med enkelte unntak er det ingen "valgfri øvelse" for norske myndigheter å implementere regelverket i nasjonal rett.

[1] Utlendingsloven § 83a jf. forskriften § 17-7a og utlendingsloven § 84a

Vi er imidlertid enig med kommisjonens vurderinger under kapittel 10 om regelkompleksitet og nasjonalt handlingsrom når det gjelder å gjøre EUs regelverk bedre tilgjengelig og klarere i nasjonal rett ved implementeringen av rettsakter fra EU. Språket i EUs forordninger er tungt, omstendelig og formuleringene er lite tilpasset vanlig norsk språkbruk. Dette gjør rettsreglene vanskelig å forstå. Det er krevende å anvende rettsreglene i praksis og utilgjengeligheten gjør det vanskelig for innbyggerne å være orientert om sin rettsstilling. Lovgivningsteknikken i forbindelse med implementering bør forbedres og PU er enig i at det bør vurderes tiltak for å forbedre lovtekster uten å endre innhold.

Om Del 1 – personvern, rettslige rammeverk og teknologiske drivkrefter – begrepet personvern

Noen av fremstillingene i denne delen av rapporten fremstår ikke hensiktsmessig for å forstå utfordringene i offentlig sektor. PU mener blant annet at det med fordel bør kunne gis en bedre og oppdatert definisjon av selve begrepet *personvern*, utover at det vises til forklaringen som gis i Schartum, D.W. (2020). Kommisjonen uttaler at de legger denne forståelsen til grunn i sin utredning. Den relativt enkle forståelsen av begrepet personvern er etter vår vurdering lite egnet til å kunne finne løsninger på alle utfordringene offentlige etater står i og vil møte fremover.

Ivaretakelse av personvern handler om kunnskap om behandling av personopplysninger*,* fordi et moderne samfunn ikke kan fungere uten behandling av personopplysninger. Det enkle og selvfølgelige utgangspunkt som alle i offentlig virksomhet må ha bevissthet om, er at all behandling av personopplysninger krever hjemmel i lov.

III Kommentarer til enkelte kapitler og forslag til tiltak

6.4.3 Deling av personopplysninger mellom forvaltningsorganer

Kommisjonen viser til at offentlige organers behov for å utveksle opplysninger på tvers av virksomheter for å løse oppgaver ofte vil innebære at personopplysninger blir videreformidlet til formål som ikke er forenelig med det opprinnelige innsamlingsformålet. Etter vår vurdering burde kommisjonen ha underbygget denne påstanden med data og eksempler. I tillegg mener vi at kommisjonen burde ha redegjort mer for hva som ligger i uforenelige formål, og på den måten fått belyst hvilke rammer som personvernforordningen setter for gjenbruk av opplysninger.

Deling av opplysninger har også en nær rettslig og faktisk sammenheng med reglene om taushetsplikt. Vi mener at taushetspliktsreglene i større grad burde vært nevnt i vurderingene til kommisjonen. I den sammenheng ville det vært interessant om kommisjonen hadde knyttet noen kommentarer til de vurderinger som ble gjort i kapittel 19 om taushetsplikt og informasjonsutveksling i *Ny forvaltningslov NOU 2019:5*.

Som et eksempel på uforenelige formål viser kommisjonen til tilfeller hvor UDI mottar informasjon fra politiet om brudd på straffeloven eller utlendingsloven. Vi mener at dette ikke er et godt eksempel, selv om man sikkert isolert sett kan si at det dreier seg om uforenelig formål. Personvernforordningen artikkel 10 regulerer behandling av personopplysninger om straffedommer og lovovertredelser. Den krever ikke at det fastsettes nasjonale lovbestemmelser for behandling av personopplysninger om straffbare forhold under en offentlig myndighets kontroll. Utlendingsmyndighetenes behandling av opplysninger om

straffedommer og lovovertredelser trenger altså ingen nærmere regulering i loven etter forordningen, jf. Prop. 59 L (2017-2018) punkt 4.3.3. For ordens skyld er det inntatt en henvising til personvernforordningens artikkel 10 i utlendingsloven § 83a.

Ellers er vi enig med kommisjonen i at større samarbeid mellom forvaltningsorganer bør føre til ekstra årvåkenhet. Kommisjonen mener at slike samarbeid i større grad bør lov- eller forskriftsfestes. Vi er ikke direkte uenig i dette, men behovet for dette må vurderes konkret i hvert enkelt tilfelle, herunder må det vurderes om det vil være tilstrekkelig at samarbeidet reguleres i utvekslingsavtaler eller lignende.

I utredningens punkt 6.4.3.1 bemerker kommisjonen at det ved deling av opplysninger på tvers av organer er en utfordring at det oppstår usikkerhet rundt ansvarsforholdene mellom samarbeidende organer. Vi kan ikke utelukke at det kan oppstå en viss usikkerhet om ansvar og roller ved deling på tvers av organer. Likevel er vår erfaring ofte den motsatte: At forvaltningsorganer blir ekstra bevisst på nettopp roller og ansvar, herunder det eksisterende rettslige grunnlaget for utlevering av opplysninger, når man vurderer deling til andre organer.

7.1.2 Personvern i justissektoren – en rettssikkerhetsgaranti

Personvernkommisjonen mener at dersom personvernkrenkelsen som følge av et tiltak er tilstrekkelig alvorlig, må konklusjonen være at kriminalitetsbekjempelsen skal vike.

PU er her uenig i personvernkommisjonens konklusjon og savner også en mer nyansert vurdering og bedre begrunnelse i utredningen. Vi stiller spørsmål ved bruken av ordet personvernkrenkelse i denne sammenhengen. For det første, dersom det er det hjemmel i lov for et tiltak for å forebygge og bekjempe kriminalitet, blir det korrekt å hevde at det foreligger en personvernkrenkelse? Forutsetter ikke krenkelsen at det foreligger et lovbrudd? For det andre, dersom kommisjonen oppstiller at personvernkrenkelse foreligger selv om det ikke skjer noe lovbrudd, burde det under dette punktet bli gitt noen konkrete eksempler på hva kommisjonen mener med personvernkrenkelse.

PU synes det er vanskelig å følge kommisjonens logikk og argumentasjon under dette punktet, herunder at kommisjon er uenig i merknadene til politiregisterloven § 1 (lovens formål); nemlig at lovens utgangspunkt er at hensynet til personvern må vike i de tilfellene der hensynet til kriminalitetsbekjempelse og hensynet til personvern ikke kan forenes. Kommisjonen standpunkt er noe uheldig, særlig sett hen til at det følger av forarbeidene til politiregisterloven at det skal skje en forholdsmessighetsavveining, og det fremgår av loven at det skal skje en vurdering av nødvendighet.

PU synes det er betenkelig at kommisjonen mener at hensynet til personvern må veie tyngst selv om saken dreier seg om helse, liv eller død. Det er ikke enkelt å se hvordan det kan være rettskildemessig dekning for et slikt standpunkt, heller ikke at det finnes støtte for et slikt standpunkt i de menneskerettighetskonvensjoner som Norge er bundet av. Kommisjonen bør gi eksempler på hva som kan være alvorlige personvernkrenkelser som ikke kan skje, når det dreier seg om å oppklare og iretteføre for domstolen alvorlige forbrytelser som drap, terrorisme og internasjonal organisert kriminalitet.

7.4.2.1 Implementere av politidirektivet i politiregisterloven

Kommisjonen uttaler at etter deres syn er *"politiregisterloven et eksempel der loven ikke oppstiller tilstrekkelig konkrete krav og føringer for behandling av personopplysninger.* Det vises bl.a. til at det kan skape utfordringer at behandlingsgrunnlag ikke gjenfinnes i politiregisterloven. Vi er enig i at dette er en svakhet ved politiregisterloven. I all hovedsak er behandlingsgrunnlagene regulert for det enkelte politiregister i politiregisterforskrifens kapittel 44-60. Manglende lovregulering av dette kan bidra til å skape usikkerhet. For eksempel oppstår det et spørsmål om det er anledning til å behandle opplysninger som er innenfor lovens virkeområde, og som gjøres i samsvar med kravene i lovens kapittel 2, når behandlingen ikke treffer noen av behandlingsgrunnlagene som er regulert i forskriften. Etter vår vurdering bør det derfor inntas bestemmelser om behandlingsgrunnlag i politiregisterloven.

Kommisjonen mener at det er behov for at politiregisterloven harmoniseres med EU-retten. Flere av kravene i EUs politidirektiv er ikke eksplisitt gjennomført i politiregisterloven. Dette gjelder bl.a. for bestemmelser relatert til automatiske beslutningsprosesser, innebygd personvern, personvernprinsipper og bruk av opplysninger som den registrerte har offentliggjort. Sistnevnte er regulert i direktivets artikkel 10 bokstav c, og er etter kommisjonens vurdering et praktisk viktig grunnlag for behandling av opplysninger fra åpne kilder. Vi slutter oss til kommisjonens vurderinger. Det vil være en klar fordel om de nevnte personvernkravene fra direktivet inntas uttrykkelig i norsk rett.

7.4.2.2 Bruk av åpne kilder

Kommisjonen redegjør i utredningens punkt 7.4.2.2 for bruk av åpne kilder som en innhentingsmetode. De viser til at dette er en lovlig metode så lenge innhentingen har en saklig grunn og er forholdsmessig. Det er Grunnloven og EMK art. 8 som setter yttergrenser for metodebruken. Om innhentingen griper inn i vernet etter EMK art. 8, må tiltaket også ha hjemmel i lov. Vi slutter oss til kommisjonens vurdering av det rettslige grunnlaget for bruk av åpne kilder som innhentingsmetode.

Vi er enig med kommisjonen når de skriver at det er viktig at politiet har en høy bevissthet om personvernimplikasjonene ved bruk av åpne kilder. Kommisjonen bruker en del plass på å uttrykke en bekymring for at bruk av åpne kilder kan ha nedkjølingseffekter ved at befolkningen ikke vil uttrykke seg like fritt i frykt for at det kan få negative konsekvenser. Bekymringen om nedkjølingseffekter kunne med fordel vært ytterligere nyansert. Her mener vi at kommisjonen burde innhentet ytterligere erfaringsgrunnlag, for eksempel om den samlede bruk av denne metoden.

7.4.2.5 Deling av opplysninger mellom politiet og andre myndigheter

Kommisjonen viser til en del av bestemmelser i politiregisterloven som åpner for at politiet kan dele opplysninger med eksterne. De presiser at det er avgjørende at mottaker har et dekkende behandlingsgrunnlag for den videre behandlingen, noe som ikke alltid er tilfelle, for eksempel ved deling av opplysninger til vekterbransjen. Vi er enig med kommisjonen i at det er viktig at det foreligger et harmonisert regelverk ved deling av opplysninger, slik at man påser at mottaker har et behandlingsgrunnlag før opplysninger deles. Det er imidlertid viktig at vurderingen av om mottaker har et behandlingsgrunnlag ikke bare vurderes etter særlovgivningen, men også etter mer generell lovgivning som for eksempel forvaltningsloven og personopplysningsloven.

Kommisjonen viser også til at det er utfordrende at en del av utleveringshjemlene i politiregisterloven forutsetter at politiet skal vurdere relevansen av opplysningene etter mottakers regelverk. Det er sikkert riktig at dette kan by på utfordringer. Likevel er det ikke noe i veien for at politiet kan innhente opplysninger om forhold hos, herunder om regelverket til, mottakeren. Da vil man blant annet få kontrollert at mottaker har et eget selvstendig behandlingsgrunnlag for den videre håndteringen av opplysningene.

7.4.6 Personvernkompetanse

Kommisjonen trekker frem at de ikke kan se en tilstrekkelig økning av bevissthet rundt personvern blant medarbeidere i politiet. PU har en noen annen opplevelse. Det er en økt bevissthet om personvern i organisasjonen, både blant ledere, tjenestepersoner og andre ansatte. Det er flere årsaker til det. Særlig viser til utarbeidelsen av nytt internt instruksverk som i større grad inkluderer personvernmessige forhold, og også intern opplæring om instruksene. Vi viser også til etableringen av personvernrådgiver (PVR)-stillingen i 2018, implementering av GDPR i etaten og obligatorisk opplæring i personvern. Lederne skal sørge for at alle deres ansatte har fullført relevant personvernopplæring, blant annet om GDPR. Erfaringen er at ansatte i større grad melder ifra om avvik og mulige regelbrudd og at de i større grad enn før tar kontakt med kontaktpersoner innen personvern, som PVR og informasjonssikkerhetsleder. Det jobbes også kontinuerlig med opplæring av personvernkonsekvensvurderinger i alle ledd av organisasjonen. Målet er å sørge for at de som behandler personopplysningene skal kunne utføre korrekte vurderinger før opplysningene behandles.

Vi har merket oss at kommisjonen viser til uttalelser fra Kripos om at *"det er ønskelig med 100% dedikerte personvernressurser i politidistriktene".* Det er likevel viktig at det ikke skjer en fullstendig oppsplitting mellom fagmiljøene i politiet og de som arbeider med personvern. Det er viktig at de som jobber med personvern i politiet har tilstrekkelig nærhet til og kunnskap om politiets fagfelt. Dette er beste måten å sikre at relevante og riktige personvernvurderinger blir foretatt på rett sted og til rett tid.

7.4.5.3 Utfordringer ved bruk av store datamengder

Personvernkommisjonen anbefaler et generelt forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom, jf. også vurderingen av dette i utredningens punkt 5.2.3.2. Kommisjonens anbefaling om forbud vil imidlertid også ramme de tilfeller hvor politiet gjør målrettede undersøkelser i historiske data, og hvor man forsøker å identifisere eller finne en mistenkt person. Det er ikke vanskelig å se for seg saker relatert alvorlig kriminalitet hvor et slikt absolutt forbud kan få uheldige konsekvenser. Tilsvarende kan også gjelde for grensekontrolloppgaver.

7.5 Personvernkommisjonens anbefalinger oppsummert

Vi mener at det er en svakhet ved utredningen om justissektoren at EUIS-programmet, og det nye regelverket med tilhørende løsninger som nå kommer fra EU på grense- og utlendingsfeltet, ikke er nevnt, jf. også våre innledende kommentarer om dette. De nye løsningene fra EU vil innebære en innsamling av biometriske data på brorparten av tredjelandsborgere som reiser inn til Schengen. Dette vil være en stor endring innen

justissektoren både når det gjelder omfanget av innsamlede data og muligheten for å søke på tvers av registre.

For øvrig har vi merket oss at kommisjonen setter digitalisering og personvern opp mot hverandre, uten at de i særlig grad belyser sider av digitaliseringen som vil bidra til et bedre personvern. Her kan det bl.a. vises til utviklingen av nye IT-løsninger som ivaretar personvernprinsipper på en helt annen måte enn gamle systemer med et teknisk etterslep og hvor det er vanskelig å få bygget inn gjeldende personvernkrav. Vi mener også at arbeidet med å tilgjengeliggjøre opplysninger på mobile arbeidsflater, som er i tråd med metodikken om å utføre politiarbeid på stedet, kunne vært nevnt i utredningen. Bruk av mobile arbeidsflatene vil bl.a. bidra til å sikre en bedre kvalitet på opplysningene som behandles.

Med hilsen

Eli Fryjordet
Assisterende Sjef PU

Jon Andreas Backlund Johansen
Fungerende seksjonsleder

Dokumentet er elektronisk godkjent uten signatur.