POLITIET

Kommunal- og distriktsdepartementet
Postboks 8112 DEP
0032 OSLO

Politidirektoratet

Deres referanse:	Vår referanse:	Dato:
22/6868-1	22/223377 - 78	10.02.2023

Politidirektoratets høringssvar - NOU 2022:11 Ditt personvern - vårt felles ansvar

Politidirektoratet viser til Kommunal- og distriktsdepartementets høringsbrev av 11. november 2022. Høringsfristen er 10. februar 2023.

Politidirektoratet har forelagt høringen for underliggende enheter og har mottatt innspill fra Kripos, Politiets utlendingsenhet (PU), Politiets fellestjenester (PFT), Politihøgskolen, Økokrim og Oslo og Nordland politidistrikt. Mottatte innspill følger vedlagt dette høringssvaret.

Personvernkommisjonens utredning er omfattende, og inneholder en rekke råd og anbefalinger på tvers av ulike samfunnsområder. Sett hen til det omfattende settet med anbefalinger i rapporten vil Politidirektoratet fokusere sine merknader på de deler av utredningen som i størst grad berører politiets virksomhet. Innspillene vil derfor i hovedsak fokusere på NOUens kapittel 7 om personvern i justissektoren. Det vil også knyttes noen merknader til utredningens kapittel 6 og 10, som treffer politiet som en del av offentlig forvaltning. Vi har i våre merknader inntatt henvisninger til innspill vi har mottatt fra underliggende enheter, men oppfordrer samtidig departementet til å gjennomgå disse.

I Juridisk litteratur skilles det gjerne mellom begrepene *personvern* og *personopplysningsvern.* Personvernkommisjonen redegjør kort for dette skillet i utredningens kapittel 3. Politidirektoratet vil bruke begrepet *personvern* når vi i det videre omtaler vern knyttet til behandling av personopplysninger*,* da det er dette begrepet som er etablert i dagligtalen.

Våre merknader vil presenteres etter NOUens oppbygning.

Innledning – den digitale utviklingen sett opp mot politiets samfunnsoppdrag

Politiet er en sentral aktør i arbeidet med å ivareta samfunnets og enkeltmenneskets trygghet og sikkerhet. Politiet bidrar gjennom å forebygge, avdekke og stanse kriminalitet og ved å være i beredskap og håndtere hendelser. Politiet er helt avhengig av innbyggernes tillit for å kunne utøve samfunnsoppdraget, blant annet ved at innbyggerne opplever at politiet er tilgjengelig med hjelp når det trengs.

Den digitale utviklingen skaper nye former for kriminalitet og åpner opp for nye sårbarheter i samfunnet og mot enkeltindivider og grupper. Ettersom teknologien blir mer tilgjengelig og flere oppgaver og samfunnsfunksjoner flyttes over på digitale plattformer, vil kriminalitet utført mot eller ved hjelp av slike bli en stadig større del av det totale kriminalitetsbildet. Kunnskapsutviklingen blant trusselaktører innen digital kriminalitet skjer raskt og verktøy og metoder for å begå digital kriminalitet som tidligere krevde spesialkunnskap, er nå blitt tilnærmet allment tilgjengelig og enkelt å benytte.

I et digitalt utviklingsperspektiv vil det ikke anses særlig hensiktsmessig å opprettholde et gammelt skille mellom ordinær kriminalitet og kriminalitet mot datasystemer og kriminalitet hvor bruk av digitale plattformer har vært avgjørende for å utføre den kriminelle handlingen – politiet må være like mye til stede i det digitale rom som i patrulje i det fysiske rom for å kunne utøve samfunnsoppdraget. Et politi som ikke er i stand til å følge en slik utvikling vil bli passiv i kriminalitetsutviklingen og dermed i kriminalitetsbekjempelsen.

Kriminaliteten er stadig mer grenseoverskridende og utfordringene må adresseres gjennom internasjonale samarbeidsorganer og andre internasjonale fora. Norge er på mange områder bundet opp i internasjonale forpliktelser, ikke minst i EU og med tanke på de rettslige rammene som diskuteres og settes der. Som eksempel kan trekkes frem EUs informasjonssystemer. Innføringen av systemene vil blant annet innebære utvidelse av både formål med behandlinger og også omfanget av personopplysninger som behandles. Forordningene går langt i retning av å sikre at hensynet til kriminalitetsbekjempelse ivaretas.[1]

Den digitaliserte hverdagen utfordrer også politiets måte å arbeide på opp mot andre myndigheter og samarbeidsinstanser. Presset på offentlig sektor vil øke, og en god måte å møte disse kravene på er gjennom inkludering og involvering av samarbeidspartnere. Effektiv forebygging og bekjempelse av kriminalitet fordrer samarbeid med andre myndigheter, næringsliv og frivillige organisasjoner innenfor de fleste polisiære oppgavene. Som også kommisjonen påpeker, er det viktig med et regelverk som legger til rette for nødvendig deling av personopplysninger og som ser de ulike sektorene i sammenheng, dersom det skal være mulig å levere sammenhengende og gode tjenester.

Når kriminaliteten endrer seg, må politiet også endre sin kompetanse og sine arbeidsmetoder. Den teknologiske utviklingen gir nye muligheter som fordrer at politiet har et bevisst og balansert forhold til de ulike hensyn som gjør seg gjeldende, herunder hensynet til personvern og hensynet til kriminalitetsbekjempelse.

Den digitale utviklingen kan utfordre personvernet på flere plan; både gjennom nye former for kriminelle handlinger som retter seg mot den enkeltes personvern og integritet, og gjennom politiets behov for effektive virkemidler for å møte utviklingen i kriminalitetsbildet. Etter Politidirektoratets oppfatning er det ikke nødvendigvis slik at effektiv kriminalitetsbekjempelse i seg selv truer personvernet; effektiv kriminalitetsbekjempelse er også en forutsetning for å beskytte borgerne mot integritetskrenkende og personvernkrenkende kriminalitet. Videre mener direktoratet at hensynet til rettssikkerhet, trygghet og beskyttelse av borgerne mot integritetskrenkende straffbare handlinger tilsier at personvern ikke alltid vil ha forrang ovenfor kriminalitetsbekjempelse. Vi viser for øvrig til våre innspill til utredningens punkt 7.1.2.

[1] For ytterligere omtale av EUs informasjonssystemer, se merknader under punktet om utredningens kapittel 10.

Det vil bli en viktig oppgave for myndighetene fremover å finne en balanse mellom innbyggernes krav til personvern og politiets behov for å være til stede på digitale plattformer og i digitale rom for å sikre innbyggernes trygghet og rettssikkerhet.

I utredningens kapittel 7 har Personvernkommisjonen stort fokus på politiets straffesaksbehandling, som er regulert i straffeprosessloven og politiregisterloven. Politidirektoratet vil understreke at politiets virksomhet omfatter behandling av opplysninger også til en rekke andre formål. Andre politimessige formål enn straffesak (eks. forebygging, ordenstjeneste) er regulert i politiregisterloven, og politiet behandler i tillegg opplysninger til ulike forvaltningsformål og sivil rettspleie, som reguleres av personopplysningsloven/personvernforordningen og ulike særlover.

Kapittel 6 – Personvern i den digitale forvaltningen

Overordnede tiltak for mer helhetlig tilnærming til personvern i offentlig forvaltning

Kommisjonen etterlyser en nasjonal personvernpolitikk som skal legge føringer for digitaliseringen i samfunnet, og blant annet sørge for at personvern ivaretas i utforming av lovverk. Videre anbefaler kommisjonen større grad av lovregulering på feltet for å styrke forutberegneligheten for innbyggerne og bedre vurderingene rundt behandlingenes lovlighet. I tillegg anbefaler kommisjonen et rådgivende og frittstående organ med det helhetlige ansvaret for personvernets stilling i offentlig forvaltning. Kommisjonen legger til grunn at disse tiltakene vil bidra til en større offentlig samtale om personvern, som inkluderer åpen debatt om grunnleggende verdier, samfunn og demokrati.

Politidirektoratet slutter seg til kommisjonens vurderinger knyttet til viktigheten av en åpen samfunnsdebatt og bevisstgjøringen rundt hvilke personvernaspekter digitaliseringsutviklingen i samfunnet medfører. Direktoratet er opptatt av at ivaretakelsen av personvernhensynene må skje som en integrert del av digitaliseringen av offentlig sektor, og inkluderes i større grad i utviklingen og gjennomføringen av IKT-politikken. Etter vår vurdering vil det derfor være mer hensiktsmessig å tydeliggjøre og eventuelt utvide Digitaliseringsdirektoratets mandat knyttet til ivaretakelse av personvernhensyn, enn å etablere et overordnet personvernansvar for offentlig sektor i et nytt separat fagmiljø.

Direktoratet vil bemerke viktigheten av et enkelt og tydelig regelverk som en forutsetning for etterlevelse. Politiet erfarer at mye av vår ressursbruk på personvernfeltet går med til å tolke og avklare krav i regelverket, og det er vår vurdering at tydeligere avklaringer om praktisk anvendelse på ulike fagområder/konkrete problemstillinger vil bidra til styrket personvern i praksis. Mange offentlige virksomheter treffes av de samme problemstillingene, og bedre samordning av arbeidet på tvers av offentlig sektor ville kunne redusere den totale ressursbruken for offentlig sektor og føre til bedre og mer enhetlig etterlevelse totalt sett. Eksempelvis har Schrems II-dommen medført omfattende ressursbruk både knyttet til rettslig tolkning, vurderinger knyttet til aktuelle leverandører, og ikke minst policy-vurderinger knyttet til hvordan IT-utviklingen i de enkelte virksomhetene skal forholde seg til den aktuelle rettstilstanden. Et organ med overordnet ansvar for personvernfeltet vil kunne gi nyttig bidrag til felles avklaringer i slike spørsmål, både i form av å lede prosesser for avklaring, utrede og avklare gjeldende rett, utforme beste praksis på praktiske problemstillinger, eventuelt gi autorative avklaringer innen sitt tillagte kompetanseområde, eller initierer slike avklaringer hos rette vedkommende.

Direktoratet viser til Kripos' merknader i vedlagte høringssvar på side 2 og referansen til Justisdepartementets utkast til veileder om taushetsplikt, opplysningsplikt og opplysningsrett i

forvaltningen. Dette er eksempel på utredninger som, når den er ferdigstilt, vil bidra til å avklare sammenhengen mellom disse pliktene/rettighetene og på den måten er praktisk viktig for offentlig sektors oppfyllelse av målet om økt etterlevelse av de ulike lovkravene og forventningene til forvaltningen (om f.eks. informasjonsdeling).

Tydeligere avklaring av ulike problemstillinger/beste praksis vil også være lettere å kommunisere internt i virksomhetene. Dette vil igjen gjøre arbeid med kompetansehevning og bevisstgjøring om behandlingen av opplysninger enklere, og lette virksomhetenes arbeid med etterlevelse og gjennomføring av lovpålagte vurderinger.

Politidirektoratet har merket seg kommisjonens anbefaling om større grad av lovregulering på feltet, og har forståelse for kommisjonens standpunkt om at dette vil bidra til større åpenhet og demokratisk kontroll rundt behandlingen av personopplysninger i offentlig forvaltning. Vi bemerker viktigheten av at lovgivningen utformes på en måte som ivaretar hensynet til teknologinøytralt og digitaliseringsvennlig lovverk. Se nærmere om dette under våre merknader til utredningens punkt 7.4.2 *Implementering av politidirektivet i politiregisterloven.* Politidirektoratet støtter videre kommisjonens anbefaling om at personvernkonsekvensvurderingene tillegges større fokus i lovgivningsprosessen og ved øvrige politiske initiativ. Det er vår erfaring at personvernaspekter med fordel kan vurderes og kommuniseres tydeligere i utrednings- og lovgivningsprosesser, og at dette vil bidra til tydeligere forventningsavklaringer knyttet til for eksempel tverretatlige samarbeidsinitiativ både hos befolkningen og på politisk nivå.

6.3.5 Vurdering av forenlighet

Profilering og bruk av maskinlæring, samt bruk av personopplysninger til testing og utvikling av IT-løsninger vil normalt forutsette at allerede innsamlede personopplysninger viderebehandles til nye formål. For å kunne behandle personopplysningene til andre formål enn de opprinnelig ble innsamlet for, må det vurderes om de nye formålene er forenlig med de opprinnelige innsamlingsformålene.

I utredningen påpeker Personvernkommisjonen at forenlighetsvurderinger kan være vanskelige og uttaler i den forbindelse at:

> det er viktig å avklare hva slags videre bruk av personopplysninger i offentlig forvaltning som vil være akseptabel, samt hvem som kan/bør foreta disse vurderingene. Det er uklart om det er nok at hvert enkelt forvaltningsorgan som behandlingsansvarlig gjør disse vurderingene, eller om de bør gjøres av lovgiver.

Etter personvernforordningen artikkel 6 nr. 4 er utgangspunktet at bruk av personopplysninger til utvikling og test av IT-systemer, som opprinnelig ble innsamlet for andre formål, ikke er forenlig, men at det etter konkrete vurderinger likevel kan være aktuelt. Politidirektoratet er enig med kommisjonen i at vurderinger av forenlighet kan være svært krevende og at det kan knytte seg usikkerhet til hva som er akseptabelt når det gjelder viderebehandling til nye formål. Vi viser her til at både Skatteetaten, Tolletaten og NAV i sin lovgivning har fått regulert den rettslige adgangen til å bruke personopplysninger ved utvikling og testing av IT-systemer.

Etter direktoratet syn kan det at enkelte etater får lovhjemmel for slik bruk, mens andre ikke har det, være egnet til å skape usikkerhet om hva som er gjeldende rettstilstand. Dersom det er ønskelig å avklare hva slags videre bruk i offentlig forvaltning som vil være akseptabel

mener direktoratet at det ved en eventuell lovregulering bør vurderes om dette kan gjøres generelt, fremfor at det reguleres spesifikt for enkelte offentlige etater.

6.4.3 Deling av personopplysninger mellom forvaltningsorganer

Politidirektoratet er enig med Personvernkommisjonen i at det kan være hensiktsmessig at ansvarsfordelingen i samarbeid mellom forvaltningsorganer lov- eller forskriftsfestes. Det vises til kommisjonens anbefaling om større grad av lov- eller forskriftsfesting av ansvarsfordeling i utredningens punkt 6.4.3.1, samt anbefaling om at det nasjonale handlingsrommet til å skape klarhet i ansvarsforhold bør benyttes aktivt i utredningens punkt 10.3.4.

Ifølge personvernforordningen artikkel 4 nr. 7 er "behandlingsansvarlig" den som bestemmer formålet med behandlingen og hvilke midler som skal benyttes. Politidirektoratet er enig i at det, særlig i komplekse organisasjoner, som større forvaltningshierarkier, og ved behandlinger som involverer flere offentlig myndigheter, kan oppstå tvil om hvem som regnes som behandlingsansvarlig ut fra personvernforordningens definisjon, og at lovgiver i slike tilfeller bør benytte seg av adgangen til å fastsette behandlingsansvaret i nasjonal rett. Det vises til at behandlingsansvarlig er pliktsubjektet etter personvernforordningen og personopplysningsloven og at det derfor er viktig at det går klart frem hvem dette er.

Økt samhandling mellom offentlige etater, med ulike regelsett som regulerer behandlingen av opplysninger, kan medføre et landskap det er vanskelig å navigere i. I tillegg til personvernforordningen må politiet også forholde seg til politiregisterloven og politiregisterforskriften, noe som skaper ekstra utfordringer i samarbeid med andre offentlige etater. Som påpekt i vårt høringssvar av 3. oktober 2018 til Personvernkommisjonens mandat, oppstår det – i tillegg til spørsmålet om hvem som har behandlingsansvar – flere til dels vanskelige problemstillinger når flere offentlige etater inngår i et samarbeid, som tilsier en regulering.[2] Eksempler på problemstillinger er: hvilket regelsett må legges til grunn; hvordan skal opplysninger utveksles; hva kan opplysninger som sammenstilles fra flere ulike enheter til et nytt kunnskapsgrunnlag brukes til; eller tilfeller der avgiverorganet har hjemmel til å utlevere, men mottakerorganet mangler behandlingsgrunnlag for å behandle mottatte opplysninger. Vi viser her til forskriftshjemmelen i forvaltningsloven ny § 13 g om adgang til å gi bestemmelser om informasjonsdeling for å utføre oppgaver som er lagt til avgiver- eller mottagerorganet, og annen behandling av taushetsbelagte opplysninger (i kraft 1. juli 2021), og forskrift om deling av taushetsbelagte opplysninger og behandling av personopplysninger i det tverretatlige samarbeidet mot arbeidslivskriminalitet (a-kriminformasjonsforskriften), som er fastsatt ved kgl.res. 17. juni 2022 med hjemmel i denne bestemmelsen.

Som eksempel på et rettsområde hvor den nasjonale adgangen til å skape klarhet i hvem som er ansvarlig for etterlevelse av personvernregelverket bør benyttes, kan nevnes EUs Interoperabilitetsforordninger (IO) som oppretter rammer for å sikre driftskompatibilitet mellom inn- og utreisesystemet (EES), visuminformasjonssystemet (VIS), det europeiske systemet for fremreisetillatelse (ETIAS), fingeravtrykkregisteret Eurodac, og Schengen-informasjonssystemet (SIS), jf. artikkel 1 nr. 2.[3] Denne rammen omfatter følgende driftskompatibilitetskomponenter: en europeisk søkeportal (ESP), en biometrisk

[2] Politidirektoratets høringssvar – Personvernkommisjonen – innspill til mandat, vår referanse 201803252-11.
[3] Forordning (EU) 2019/818 av 20. mai 2019 om fastsettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer vedrørende politisamarbeid og rettslig samarbeid, asyl og migrasjon og Forordning (EU) 2019/817 av 20. mai 2019 om fastsettelse av en ramme for interoperabilitet mellom EU-informasjonssystemer vedrørende grenser og visum.

sammenligningstjeneste (felles BMS), et felles identitetsregistrer (CIR) og en fleridentitetsdetektor (MID).

Interoperabilitet (IO) er et EU-initiativ som skal legge til rette for samhandling (interoperabilitet) mellom EUs informasjonssystemer. Forordningene gir forholdsvis komplekse regler om behandlingsansvar for medlemsstatenes ulike myndigheter, som dels følger behandlingsansvaret for de underliggende systemene, dels fastsetter behandlingsansvar for registrering av opplysninger i de ulike IO-komponentene. Dette gjør at nasjonal regulering av behandlingsansvar er nødvendig for å sikre tilstrekkelig klarhet i ansvarsforholdene og legge til rette for en lojal etterlevelse av EU-regelverket.

Et annet område hvor det hadde vært ønskelig med en tydeligere regulering av behandlingsansvaret er det tverretatlige samarbeidet mot arbeidslivskriminalitet. Dette samarbeidet er regulert av forskrift om deling av taushetsbelagte opplysninger og behandling av personopplysninger m.m. i det tverretatlige samarbeidet mot arbeidslivskriminalitet (a-kriminformasjonsforskriften), gitt med hjemmel i forvaltningsloven § 13 g. Forskriftens § 8 om behandlingsansvar overlater til hovedaktørene som inngår i samarbeidet å "sørge for at det etableres en ordning for ivaretakelse av behandlingsansvaret."

For øvrig viser vi til uttalelsen fra Kripos, som i sitt høringssvar nyanserer behovet for regulering av ansvarsforhold. Vi viser videre direktoratets omtale av regulering av behandlingsansvar i politiregisterloven under våre innspill til utredningens punkt 7.4.2.

6.4.5 Profilering til kontrollformål

Personvernkommisjonen anerkjenner at det finnes legitime grunner til å forhindre, kontrollere og avdekke misbruk av offentlige ordninger og at avanserte dataanalyser og profilering både kan være et hensiktsmessig og nødvendig virkemiddel i den sammenheng. Kommisjonen mener at profilering ved bruk av maskinlæring som har til formål å avdekke ulovligheter alltid bør sees som en inngripende behandling og peker i den forbindelse på faren for utglidning fra beslutningsstøtte til beslutning.

Politidirektoratet er enig i kommisjonens tilnærming.

6.4.6 Offentlige aktører og store teknologiselskaper

Personvernkommisjonen mener offentlige virksomheter må gjøre grundige vurderinger av om de skal benytte sosiale medier for å gi informasjon og kommunisere med innbyggerne. Videre uttaler kommisjonen at sosiale medier ikke bør brukes i konkret enkeltsaksbehandling.

Politidirektoratet støtter kommisjonens uttalelse på dette punktet. Som også kommisjonen peker på vil ulike virksomheter kunne ha ulike behov når det gjelder å være til stede i sosiale medier, blant annet for å nå ut til befolkningen for å kunne utføre sitt samfunnsoppdrag. Dette gjør seg gjeldende for politiet som har som primæroppgave å skape trygghet og bekjempe kriminalitet. Politiet har også en rekke forvaltningsoppgaver. Innbyggerne trenger informasjon og dialog om begge deler, og politiet har et behov for å informere innbyggerne om vårt arbeid. Direktoratet viser i den forbindelse til Kripos sine merknader i vedlagt høringssvar på side 3, hvor de redegjør for arbeid knyttet til politiets åpne tilstedeværelse på internett og tiltaket "Sikker chat for nettpatruljene".

Direktoratet anerkjenner viktigheten av at det foreligger grundige vurderinger av politiets bruk av sosiale medier, og at det eksisterer gode rutiner og retningslinjer som sikrer at politiet i sin

tilstedeværelse på sosiale medier etterlever de til enhver tid gjeldende regelverk, herunder at politiet ivaretar krav til personvern og taushetsplikt.

6.4.7 Informasjonssikkerhet

Personvernkommisjonen peker på at brudd på informasjonssikkerhet i løsninger som behandler personopplysninger også vil kunne medføre brudd på personopplysningssikkerheten, og at tiltak for å forbedre informasjonssikkerheten dermed ofte også vil kunne bidra til økt personopplysningssikkerhet.

Politidirektoratet er kjent med at Digitaliseringsdirektoratet tidligere har innhentet innspill på et initiativ om felles sikkerhet i forvaltningen fra fagmyndigheter, tilsyn og departementer. Politidirektoratet forstår kommisjonens forslag som en støtte til dette initiativet – Felles sikkerhet i forvaltingen - og et forslag om at tiltaket blir prioritert og sentralt finansiert. Politidirektoratet vil i den forbindelse bemerke at det allerede finnes flere veiledere og støttemateriell som er tilgjengelig for bruk i offentlig sektor. Det kan være utfordrende å holde oversikt over disse, da de kommer fra flere ulike aktører. Politidirektoratet er enig med kommisjonen i at en felles referanseramme (norm) for offentlige virksomheter, vil kunne være hensiktsmessig, og støtter kommisjonens forslag om at tiltaket bør finansieres sentralt. Særlig vil etablering av basisnivåer med sikkerhets- og personvernstiltak være et godt bidrag til etablering av mer felles sikkerhet på tvers i forvaltningen og et mer effektivt arbeid med informasjonssikkerhet, som også beskrives som et mål for tiltaket. Dette er noe også politiet vil kunne dra nytte av i ledelsessystemet for sikkerhet i etaten og ved utvikling av nye løsninger.

Direktoratet vil bemerke at det for å sikre realisering av initiativet vil være behov for å synliggjøre hvilke økonomiske og administrative konsekvenser initiativet vil innebære.

Kapittel 7 – Personvern i justissektoren

7.1.2 Personvern i justissektoren – en rettssikkerhetsgaranti

I utredningens punkt 7.1.2 vurderer kommisjonen forholdet mellom personvern og kriminalitetsbekjempelse.

Kommisjonen trekker frem politiregisterlovens formålsbestemmelse, § 1, og uttalelser i lovens forarbeider om at hensynet til personvernet i utgangspunktet må vike der det ikke lar seg gjøre å forene hensynet til personvern og hensynet til kriminalitetsbekjempelse. Kommisjonen skriver:

> Når interesser står mot hverandre, kan ikke utgangspunktet være at personvernet alltid må vike. Dersom personvernkrenkelsen som følge av et tiltak er tilstrekkelig alvorlig, må konklusjonen etter Personvernkommisjonens oppfatning være den motsatte; kriminalitetsbekjempelsen skal vike.

Politidirektoratet mener, i likhet med Kripos, at utsagnet i forarbeidene ikke kan tolkes bokstavelig med den mening at personvernet *alltid* skal vike. Politiregisterloven skal ivareta begge hensyn. Som også PU, Kripos og Nordland politidistrikt tar til orde for, mener direktoratet at det må legges opp til en forholdsmessighetsvurdering som veier de to hensynene mot hverandre i tråd med dagens regulering i politiregisterforskriften § 1-1, jf. § 4-2. Aktuelle momenter i forholdsmessighetsvurderingen er formålet med behandlingen, hvilke

opplysninger som skal behandles, typen kriminalitet, herunder alvorlighetsgrad og antall personer som vil ha tilgang til opplysningene, jf. forskriftens § 4-2 første ledd.

Et inngrep som vurderes som forholdsmessig i tråd med forskriftens § 1 og § 4-2, kan i enkelte tilfeller innebære at hensynet til personvernet vil måtte vike. Det vises til at en av politiets hovedoppgaver er kriminalitetsbekjempelse, og at hensynet til gjennomføring av denne oppgaven nødvendigvis vil måtte veie tungt i forholdsmessighetsvurderingen.

Som vi også påpekte i vårt høringssvar av 3. oktober 2018 til Personvernkommisjonens mandat mener Politidirektoratet at:

> det *ikke* er slik at effektiv kriminalitetsbekjempelse i sin natur er en trussel mot personvernet. Politiets evne til kriminalitetsbekjempelse vil på gitte områder også være helt nødvendig for å bevare og styrke personvernet og den reelle retten til privatliv.[4]

Kommisjonen uttaler selv i utredningens punkt 7.1.2 at "[i] flere sammenhenger vil en tilstrekkelig kriminalitetsbekjempelse utvilsomt være en forutsetning for godt personvern." Det er statens hovedoppgave å beskytte sine innbyggere, ikke bare mot ytre fiender, også mot alvorlig kriminalitet. Kriminalitetsbekjempelse er også vern av grunnleggende rettigheter og friheter for borgerne. Det er godt personvern at kriminalitet blir oppklart og det er godt personvern å hindre at innbyggerne utsettes for alvorlig kriminalitet, for eksempel vil forebygging og etterforsking av ID-tyverier, nettovergrep mot barn, ulovlig deling av bilder og digital kriminalitet rettet mot eldre bidra til å beskytte personvernet til den enkelte borger. Det er en viktig dimensjon som i mange sammenhenger kan bli underkommunisert. For eksempel rammer terrorhandlinger og annen alvorlig kriminalitet begått av ekstreme miljøer i stor grad det sivile samfunn, og virkningen av slike handlinger går lengre enn tap av menneskeliv og materielle verdier gjennom den frykt og utrygghet som skapes. Slik alvorlig kriminalitet bør da møtes både med polisiære og rettslige midler som er til rådighet i en rettsstat, og med forebyggende tiltak som en rekke aktører kan utføre i samfunnet, både offentlige og private.

Det er således et sterkt behov for å diskutere hvordan hensynet til personvern skal balanseres opp mot hensynet til kriminalitetsbekjempelse. For all kriminalitetsbekjempelse er det krav til at det gjøres en nødvendighets- og forholdsmessighetsvurdering før inngrep besluttes og retten til privatliv vil da hensyntas. Økte personvernrettigheter for den enkelte til å kunne utøve digital aktivitet, eller hvor denne aktiviteten skjer på digitale arenaer hvor det ikke vil være mulig å få tilgang for polisiære formål grunnet kryptering og anonymisering, vil måtte medføre en økt aksept av risiko for kriminalitet i samfunnet. Det vil da innebære en diskusjon hvor flere gode formål må ses opp mot hverandre.

7.3.4 Politiske føringer – utvidelser av politimyndighetenes inngrepsmuligheter

Personvernkommisjonen uttaler at politiske føringer for europeisk politisamarbeid gjennom EUROPOL kan skape personvernutfordringer, og viser til at European Data Protection Supervisor (EDPS) har avdekket at EUROPOL mottar store mengder personopplysninger fra politiet i medlemsland og at disse opplysningene ofte er i strid med personvernregelverket.

Politidirektoratet er enig med kommisjonen om at det er viktig at norske myndigheter sikrer at personvernet til norske innbyggere blir ivaretatt når politiet overfører opplysninger til EUROPOL og i andre sammenhenger hvor det utveksles informasjon mellom politimyndigheter.

[4] Politidirektoratets høringssvar – Personvernkommisjonen – innspill til mandat, vår referanse 201803252-11.

Direktoratet viser i den forbindelse til Kripos sine merknader i vedlagt høringssvar på side 4, hvor de redegjør for arbeid med fastsettelse av retningslinjer og utlevering av opplysninger til utlandet i internasjonalt politisamarbeid.

7.4.2 Vurderinger av personvernkonsekvenser i myndighetsutøvelsen

Personvernkommisjonen diskuterer i punkt 7.4.2 utfordringer i justissektoren knyttet til uklare hjemler, bruk av åpne kilder, formålsutglidning og deling av data mellom politiet og andre myndigheter.

Implementering av politidirektivet i politiregisterloven

Politidirektoratet støtter Personvernkommisjonens syn om at det er behov for en ny vurdering av om alle bestemmelsene i politidirektivet (LED)[5] skal implementeres i politiregisterloven. Vi mener at både artikkel 4 om personvernprinsippene, artikkel 10 bokstav c om bruk av særlige kategorier opplysninger som den registrerte selv har offentliggjort, artikkel 11 om automatiske avgjørelser og profilering og artikkel 20 om krav til innebygd personvern bør gjennomføres i politiregisterloven. I tillegg mener vi at politiregisterlovgivningens bestemmelser om internkontroll og informasjonssikkerhet, som bygger på tilsvarende bestemmelser i gammel personopplysningslov, bør harmoniseres med og følge metodikken i politidirektivet og personvernforordningen.

For øvrig viser vi til den utførlige gjennomgangen av hvilke bestemmelser i direktivet som bør gjennomføres i politiregisterloven i uttalelsen fra Oslo politidistrikt. Kripos og PU har i sine høringssvar også sluttet seg til at det er behov for en harmonisering av politidirektivet og politiregisterloven.

Når det gjelder hvem som bør forestå vurderingen og det nærmere omfanget av denne, mener Oslo politidistrikt at det bør opprettes et eget utvalg for å vurdere i hvilken grad forpliktelsene i henholdsvis politidirektivet og Europarådskonvensjonen er tilfredsstillende gjennomført i politiregisterloven med forskrift, men også i øvrig i sektorlovgivning som politiloven og straffeprosessloven. Politidirektoratet er enig i dette.

Politidirektoratet støtter, i likhet med Oslo politidistrikt, Kripos og PU, kommisjonens vurdering av at politiregisterloven bør forenkles og forbedres. Behovet for en modernisering av politiregisterlovgivningen blir stadig mer fremtredende i lys av den teknologiske utviklingen og behovet for å digitalisere politiets tjenester. Vi viser i den forbindelse til Digitaliseringsdirektoratets veileder for *Digitaliseringsvennlig regelverk.* Etter Politidirektoratets vurdering fremstår politiregisterlov og -forskrift som lite digitaliseringsvennlig og vi mener at regelverket gjør det mer krevende for politiet å digitalisere sine tjenester. Digitalisering er en nødvendig forutsetning for at politiet skal kunne ivareta sitt samfunnsoppdrag. Regelverket fremstår i dag som unødvendig detaljert og fragmentert og oppleves av rettsanvenderne som lite tilgjengelig og brukervennlig, noe som i seg selv er et hinder for etterlevelse og god ivaretakelse av personvern i praksis. For øvrig viser vi til vårt høringssvar av 15. desember 2016 til endringer i politiregisterloven og politiregisterforskriften – implementering av direktiv (EU) 2016/680, hvor vi uttalte at:

> Etter direktoratets vurdering er det et behov for en mer helhetlig evaluering av politiregisterloven med forskrift uavhengig av nye EU-krav på dette feltet. De praktiske erfaringene med anvendelsen av loven og forskriften etter ikrafttredelsen har avdekket

[5] Direktiv 2016/680, (politidirektivet).

> behov for klargjøring og forenkling på en rekke punkter for å gjøre regelverket mer brukervennlig. Også den tekniske utviklingen og det stadig større innslaget av tverrfaglig samarbeid med andre etater, medfører behov for å vurdere revisjon av regelverket.[6]

Videre vises også til vårt høringssvar av 3. oktober 2018 til Personvernkommisjonens mandat, hvor vi påpekte behovet for en evaluering og revisjon av politiregisterloven med tilhørende forskrift:

> Dagens regelverk er komplisert og vanskelig å navigere i og det kan stilles spørsmål ved om et komplisert og fragmentert lovverket [sic] gir økt personvern i praksis. Særlig politiregisterforskriften er svært detaljert og fragmentarisk bygget opp. Ved utformingen av reglene ble det i stor grad tatt utgangspunkt i gjeldende registre og IKT-systemer på tidspunktet reglene ble utformet. […] Etter Politidirektoratets oppfatning er gjeldende politiregisterforskrift bygget på en "analog" tankegang og er krevende å anvende i dette perspektivet.[7]

Oslo politidistrikt har på side 7 i sitt høringssvar tatt til orde for at det er behov for en revurdering av kriteriene for plassering av behandlingsansvar lavt i hierarkiet i politi- og lensmannsetaten. Det vises til at bakgrunnen for plassering av behandlingsansvar lavt i hierarkiet i politiregisterloven med forskrift baserer seg på prinsipper om at behandlingsansvaret bør plasseres så nært behandlingen som mulig og at den behandlingsansvarlige bør ha reell innflytelse på den behandlingen som skjer.

Politidirektoratet er enig i at det er behov for å gjennomgå reguleringen av behandlingsansvaret i politi- og påtalemyndighet. Gjeldende regulering er særlig en utfordring der behandlingsansvaret er lagt lokalt til den enkelte politimester/særorgansjef, mens Politidirektoratet/Politiets IT-enhet utvikler og beslutter felles IT-løsninger og gir føringer for bruken. På straffesaksområdet er videre riksadvokaten faglig overordnet og gir føringer for behandlingen av opplysninger blant annet ved å behandle klager fra de registrerte knyttet til straffesaksløsningene.

Den behandlingsansvarlige har ansvar for at behandlingen av personopplysninger følger regelverket, inkludert både personopplysningssikkerheten og den faktiske behandlingen. En politimester vil i praksis ikke ha samme reelle innflytelse på alle disse aspektene, jf. for eksempel hvordan informasjonssikkerhet og personvern er ivaretatt i felles IT-løsninger. Lovverket bør i større grad tydeliggjøre hvilke organ som har ansvar for de ulike delene av behandlingsansvaret slik at det er i samsvar med den reelle innflytelsen, og direktoratet anbefaler en regelverksgjennomgang med sikte på å klargjøre innholdet i behandlingsansvaret og hvorvidt det i realiteten er et felles/delt ansvar mellom ulike organ innen politi- og påtalemyndigheten.

Bruk av åpne kilder
Personvernkommisjonen mener bruk av åpne kilder på internett kan skape særskilte personvernutfordringer.

---

[6] Politidirektoratets høringsuttalelse til endringer i politiregisterloven og politiregisterforskriften som følge av implementeringen av EU-direktiv 2016/680, vår referanse 201604312-9.
[7] Politidirektoratets høringssvar – Personvernkommisjonen – innspill til mandat, vår referanse 201803252-11.

I likhet med Kripos, PU og Nordland politidistrikt støtter ikke Politidirektoratet kommisjonens vurderinger om bruk av åpne og tilgjengelige kilder på internett. Direktoratet viser til Nordland politidistrikts og Kripos sine merknader i vedlagte høringssvar på henholdsvis side 2 og 6.

Politidirektoratet anerkjenner at det digitale rom er et viktig middel for å sikre ytringsfrihet, herunder for borgernes kommunikasjon og livsutfoldelse. Som også påpekt innledningsvis i vårt høringssvar skaper den digitale utviklingen nye former for kriminalitet og kriminalitet utført ved hjelp av digitale plattformer vil bli en stadig større del av det totale kriminalitetsbildet. Trusselaktører benytter seg av digitale plattformer for å sammenstille og systematisere opplysninger som igjen benyttes til å begå kriminelle handlinger. Dersom politiet skal være i stand til å følge kriminalitetsutviklingen vil politiet også måtte være til stede i det digitale rom og behandle personopplysninger.

Direktoratet vil bemerke viktigheten av at det til enhver tid gjeldende regelsett for innhenting og lagring overholdes, herunder gjennomføring av vurderinger av nødvendighet, forholdsmessighet og formålsbestemthet. Så lenge de til enhver tid gjeldende regler for innhenting og lagring overholdes har direktoratet vanskelig for å se hvordan politiets behandling av nevnte opplysninger skiller seg fra bruk av andre kilder for informasjonsinnhenting.

Kommisjonen anfører at politiets mulighet til å bruke opplysninger som er innhentet på nett til etterforskningsformål kan føre til at personer legger bånd på hva de sier og gjør i frykt for negative konsekvenser. Direktoratet er enig med Kripos og PU om at det er ønskelig med mer kunnskap om den reelle påvirkningen slik innsamling og lagring har på ytringsfriheten, før en eventuell nedkjølingseffekt på ytringsfriheten tillegges vekt i debatten.

Oslo politidistrikt etterlyser en vurdering av politidirektivet i forbindelse med redegjørelsen om bruk av åpne kilder. Distriktet peker på at LED artikkel 10 bokstav c gir grunnlag for behandling av særlige kategorier personopplysninger der det er *åpenbart* at den registrerte har offentliggjort opplysningene. Politidirektoratet er enig i Oslo politidistrikts merknader og viser til vedlagt høringssvar på side 2.

Masseinnsamling av opplysninger
I tilknytning til omtalen av bruk av åpne kilder uttaler kommisjonen at:

> dersom det igangsettes tiltak som innebærer masseinnsamling av personopplysninger for nærmere angitte formål, er det viktig at metoder for dataseparasjon følges for å sikre at data kun benyttes til formål lovgiver har vurdert det nødvendig for.

Politidirektoratet kan ikke se at kommisjonen har redegjort for hva de legger i begrepet "masseinnsamling", og etterlyser kommisjonens forståelse av begrepet som utgangspunkt for anbefalingen. For øvrig støtter direktoratet kommisjonens uttalelse om viktigheten av tiltak for å sikre at data behandles til nødvendige formål, hvor dataseparasjon vil være et av flere aktuelle tiltak.

Formålsutglidning i forbindelse med politiets myndighetsutøvelse
For oversiktens skyld ønsker Politidirektoratet å synliggjøre at politiet er gitt en viss adgang til å behandle personopplysninger til andre politimessige formål enn det de er innhentet til, jf. politiregisterloven § 4. Det følger av lovens forarbeider at "[d]ette innebærer for eksempel at opplysninger som er innhentet i forbindelse med etterforskning kan brukes til politiets

kriminalitetsforebyggende arbeid."[8] Slik bruk forutsetter tjenestemessig behov, jf. politiregisterloven § 21.

7.4.3 Åpenhet om politiets metodebruk

Personvernkommisjonen anbefaler at det nedsettes et utvalg for å utrede metodebruk i justissektoren. Videre anbefaler kommisjonen i punkt 7.4.8 at utvalget også skal vurdere om Kommunikasjonsutvalgets mandat bør utvides til å omfatte kontroll med andre av politiets metoder enn kommunikasjonskontroll, romavlytting og dataavlesning. Politidirektoratet anerkjenner at det kan være behov for å se sammenhengen av ulike hjemler og konsekvenser av eventuelle utvidelser av politimyndighetenes hjemler som har kommet til over tid, herunder personvernkonsekvenser.

Politidirektoratet mener at før det eventuelt nedsettes et slikt utvalg, som også skal se på Kommunikasjonskontrollutvalgets mandat, bør en se hen til de mange utredninger og lovprosesser som ligger til grunn for den regelverksutviklingen som har funnet sted. Dersom anbefalingen om å nedsette et utvalg realiseres, mener Politidirektoratet at det nedsatte utvalget også bør vurdere eventuell utvidelse av kontrollområdet for Kommunikasjonskontrollutvalget til andre av politiets metoder, samt kriminalitetsutfordringer både for samfunnet, grupper og enkeltindivider.

7.4.4 Domstolskontroll

Personvernkommisjonen mener det bør vurderes om dagens domstolskontroll av politiets tiltak bør utvides. Videre mener kommisjonen at det bør innføres et tillegg i straffeprosessloven § 170a som sikrer en vurdering av at den samlede bruken av ulike etterforskningsmetoder ikke blir et uforholdsmessig inngrep.

Politidirektoratet er enig med kommisjonen om viktigheten av en effektiv og reell domstolskontroll, men vil likevel bemerke at hensynet til effektiv og reell domstolskontroll må holdes opp mot behovet for effektiv og reell kriminalitetsbekjempelse i politiet. Direktoratet støtter kommisjonens uttalelse om at forholdsmessighetsvurderinger ved bruk av tvangsmidler må vurderes opp mot øvrig benyttet tvangsmiddelbruk, og at det av den grunn kan være hensiktsmessig å innføre et tillegg i straffeprosessloven § 170a som foreslått. Politidirektoratet ser imidlertid behov for at det i forbindelse med et eventuelt videre lovarbeid redegjøres nærmere for hvordan hensynet til personvern skal vektlegges i denne sammenheng i forskjellige straffesaker.

Direktoratet viser for øvrig til Kripos' merknader i vedlagte høringssvar på side 8.

7.4.5 Bruk av ny teknologi i justissektoren

Kommersielle analyseverktøy for bruk i justissektoren

Personvernkommisjonen trekker frem viktigheten av åpenhet for å sikre muligheter med kontroll med anskaffelser i justissektoren. Kommisjonen peker også på viktigheten av åpenhet knyttet til behandling av personopplysninger andre steder i utredningen, herunder kapittel 12. Direktoratet er enig med kommisjonen om at åpenhet er viktig både for å sikre kontroll med anskaffelser av potensielt inngripende verktøy, men også som en forutsetning for tilfredsstillende demokratisk deltakelse, personvern og rettssikkerhet. Politidirektoratet vil likevel bemerke at politiet i noen tilfeller er avhengig av å holde noen kapasiteter og metoder skjult for å kunne utføre tjenesten med en tilstrekkelig grad av operasjonssikkerhet. Dette

[8] Ot.prp.nr.108 (2008-2009), punkt 21.2.

hensynet til begrenset åpenhet må ivaretas. Vi viser for øvrig til Kripos' merknader i vedlagte høringssvar på side 8.

Utfordringer ved bruk av maskinlæringsmodeller i justissektoren
Politidirektoratet er enig med kommisjonen om at det må gjennomføres gode forhåndsvurderinger og sikre dokumentasjon før en tar i bruk maskinlæringssystemer. Dette for å sikre ansvarlig bruk av slike systemer, unngå feilkilder som potensielt kan ha alvorlige konsekvenser for enkeltindivider og sikre muligheter for etterprøvbarhet.

Direktoratet viser før øvrig til Kripos sine merknader i vedlagt høringssvar på side 8, hvor det redegjøres kort for hva som anses relevant for politiet i dag, samt hva som vil kunne tillates etter dagens regelverk (politiregisterlov).

Bruk av kunstig intelligens og utfordringer ved bruk av store datamengder
Politidirektoratet er enig med Personvernkommisjonen i at nasjonale hjemler for bruk av maskinlæring må sikre tilstrekkelig åpenhet og rettssikkerhet for de(n) registrerte, slik kommisjonen uttaler i utredningens punkt 6.4.4. Direktoratet er videre positive til at menneskerettighetsvurderinger bør ligge til grunn der systemene som brukes kan ha betydelig innvirkning på innbyggernes liv. Det er viktig at regulering av maskinlæringssystemer ikke bidrar til å forsterke maktubalansen mellom offentlig myndigheter og innbyggerne.

Kommisjonen anbefaler et generelt forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom.

Politidirektoratet er kjent med at Europakommisjonens forslag til KI-forordning ligger til behandling i Europaparlamentet og Rådet.[9] I forslaget til KI-forordning er det ikke foreslått et totalforbud mot teknologien. Det er foreslått noen snevre unntak for politiets bruk av slik teknologi, blant annet for å bekjempe alvorlig kriminalitet. Forslaget er imidlertid kritisert fra flere hold. European Data Protection Board (EDPB) og EDPS har blant annet i sin *'Joint Opinion on the European Commission's Proposal for a Regulation laying down harmonised rules on artificial intelligence'* anbefalt et totalforbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom.[10] Det er derfor fortsatt knyttet usikkerhet til den endelige regulering av denne teknologien.

Politidirektoratet vil bemerke at vi legger til grunn samme forståelse av begrepet 'ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom' som i forslaget til KI-forordning (fortalepunkt 8 og 9), slik at det omfatter KI-systemer som har til formål å identifisere fysiske personer på avstand. Vi forutsetter derfor at forslaget om et forbud for eksempel ikke vil omfatte bruk av ansiktsgjenkjenningsteknologi på nettovergrepsvideoer eller som ledd i grensekontroll på flyplasser.

Kripos, PU og Oslo politidistrikt har alle kommentert anbefalingen i sine høringssvar. Der gis det uttrykk for skepsis til et generelt forbud. Det pekes blant annet på at forsvarlig bruk av ansiktsgjenkjenningsteknologi er viktig for politiets arbeid i dag og at det er viktig å skille mellom ulike former for bruk av ansiktsgjenkjenning. Politidirektoratet er enig i dette. Direktoratet er videre enig med Kripos i at norske myndigheter ikke bør unngå å benytte seg

[9] Proposal for a regulation of the European Parliament of the Council laying down harmonised rules on artificial intelligence, 21. April 2021.
[10] EDPB-EDPS, Joint Opinion 5/2021, on the European Commission's Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

av det handlingsrommet som eventuelt vil følge av unntakene i den foreslåtte KI-forordningen med tanke på den alvorligste kriminaliteten som retter seg mot liv og helse.

Oslo politidistrikt har i sitt høringssvar foreslått at utredning av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon bør inngå som del av mandatet til Personvernkommisjonens foreslåtte metodeutvalg i utredningens punkt 7.4.3. Dersom det opprettes et slikt utvalg er Politidirektoratet enig i dette.

7.4.6 Personvernkompetanse

Personvernkommisjonen fremholder i utredningens punkt 7.4.2.4 og 7.4.6 at politiet ikke i tilstrekkelig grad har vektlagt å øke medarbeidernes bevissthet rundt personvern, samt at personvernkompetanse og -kultur må forankres i ledelsen i politiet. Videre anbefaler kommisjonen at personvernkompetansen i enhetene for digitalt politiarbeid (DPA) i politidistriktene bør styrkes.

Politidirektoratet er enig med kommisjonen i at det er et lederansvar å sørge for at ansatte har tilstrekkelig personvernkompetanse, samt at etablering av en god personvernkultur er en forutsetning for systematisk, varig og god ivaretakelse av personvernet.

Politietaten er en stor og kompleks organisasjon, der behandlingsansvar tilligger ulike enheter, avhengig av hvilket regelverk som regulerer behandlingen av personopplysningene. Dette fordrer at politiet har et bevisst forhold til håndtering av personopplysninger, samt at man arbeider kontinuerlig for å tydeliggjøre roller og ansvar og etablere enhetlige prosesser og praksis på tvers av enhetene i etaten.

Som det fremgår av rapporten, er det bygget et personvernfaglig miljø i Kripos. Det er videre etablert et personvernfaglig miljø i Politidirektoratet, samt et nettverksforum for personvernrådgivere fra enhetene i etaten, som aktivt bidrar i det daglige personvern-arbeidet. Vi er enig med Kripos, når de uttaler følgende i sitt høringssvar:

> Personvern i politiet har gått igjennom en betydelig utvikling siden ikrafttredelsen av politiregisterloven og politiregisterforskriften i 2013, og det etterfølgende SPOR-programmet. Utviklingen er ikke avsluttet, og det er flere initiativ både i regi av Politidirektoratet og Kripos for å styrke personvernet i politiet ytterligere.

Hva gjelder behandling av personopplysninger etter personvernforordningen, ble det i direktoratet etablert et sentralt GDPR-prosjekt, som i perioden 2018-2021 gjennomførte en rekke tiltak for enhetlig innføring av ny personopplysningslov i 2018 i etaten, herunder tiltak for å øke kompetanse og bevissthet om personvern.

Som Kripos bemerker i sitt høringssvar, er grunnopplæring i personvern obligatorisk for alle nyansatte i politiet, gjennom e-læringskurs. Det samme gjelder for nye ledere, som gjennomfører et utvidet kurs innen personvern. Vi viser for øvrig til vedlagte uttalelser fra Kripos og PU om økt bevissthet om og opplæring i personvern i politiet.

Politidirektoratet erfarer en økende bevissthet rundt personvern i etaten, i ulike ledd av organisasjonen. Dette gjenspeiles blant annet i økt bevissthet om og rapportering av brudd på personopplysningssikkerheten (avvik), internt og til Datatilsynet. Samtidig vil direktoratet påpeke at bevissthet og kompetanse ikke er tilstrekkelig for etterlevelse av personvernlovgivningen i en kompleks etat som politiet. I tillegg til videre arbeid med tilpasset

opplæring tilpasset ulike roller, er det nødvendig med kontinuerlig arbeid med å forbedre internkontroll og rutiner for hvordan personvern skal ivaretas i ulike prosesser. Som vi også har fremhevet i våre merknader til utredningens punkt 7.4.2 *Implementering av politidirektivet i politiregisterloven* mener direktoratet at et enkelt og tilgjengelig regelverk er en forutsetning for godt personvern. Dagens regelverk er fragmentert, detaljert, til dels overlappende og utydelig, noe som gjør anvendelsen av regelverket vanskelig for rettsanvenderne.

7.4.7 Systemer og verktøy for å ivareta personvernet

Håndtering av digitale beslag og overskuddsinformasjon
Personvernkommisjonen redegjør for problemstillinger knyttet til å filtrere bort overskuddsinformasjon ved beslag av digitale lagringsenheter og anbefaler at norske myndigheter bør innhente erfaringer fra andre land om ordninger for å filtrere bort slik informasjon.

Politidirektoratet tiltrer, og viser til, Kripos sin redegjørelse på dette punktet i vedlagt høringssvar på side 10. Vi vil samtidig understreke betydningen av at det til enhver tid er gode rutiner, og etablert kultur, for etterlevelse av regelverk knyttet til håndtering av beslag, herunder elektronisk beslag, og overskuddsinformasjon.

Utlevering av dokumenter til advokater
Personvernkommisjonen anbefaler at det bør etableres en samhandlingsplattform for dokumentutlevering i justissektoren. Kommisjonen trekker blant annet frem utfordringer knyttet til kontroll med bruk av kopier og tilbakelevering av dokumenter, som bidrar til å øke risikoen for at personopplysninger kommer på avveie. Kommisjonen anbefaler derfor at plattformen gir tilgang til dokumenter uten å gi nedlastingsmuligheter. Politidirektoratet støtter, i likhet med Oslo politidistrikt og Kripos, kommisjonens anbefaling og viser for øvrig til Oslo politidistrikt og Kripos sine merknader i vedlagt høringssvar, henholdsvis på side 3 og 11.

Kommisjonen foreslår at Justisdepartementet bør etablere en norm for IKT-sikkerhet og investere tyngre fremover ved bestilling/kravsetting og utvikling av løsninger som tilfredsstiller kravene til innebygd personvern. Politidirektoratet oppfatter det som noe uklart hva kommisjonen legger i norm for IKT-sikkerhet.

I helse- og omsorgssektoren er det til sammenligning etablert en bransjenorm for informasjonssikkerhet og personvern (Normen). Normen beskriver både organisatoriske og tekniske tiltak som anses egnet for å oppnå tilfredsstillende informasjonssikkerhet og personvern i sektoren. Den som samhandler med en virksomhet som har forpliktet seg til å innrette seg etter kravene i en slik bransjenorm, skal kunne være trygg på at virksomheten har etablert egnede organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern.

Politidirektoratet mener at formålet med etableringen av en slik norm må være å beskytte informasjonen og personvernet, og at det vil være uheldig dersom en etablering av en norm i justissektoren var avgrenset til tekniske tiltak. Den bør derfor ikke avgrenses til IKT-sikkerhet, men omhandle både informasjonssikkerhet og personvern. En slik norm vil kunne være hensiktsmessig, da informasjonssikkerhet knyttet til dokumentutveksling med politiet har betydning for samfunnets tillit til ivaretakelse av borgernes personvern. Ved utarbeidelse av en slik bransjenorm, bør det ses hen til en eventuell felles norm for informasjonssikkerhet i offentlig sektor, som foreslått i utredningens punkt 6.4.7.

Politidirektoratet støtter forlaget om at det bør investeres tyngre i at krav til innebygd personvern er tilfredsstilt ved bestilling/kravsetting og utvikling av løsninger. Dette innebærer at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning, slik at blant annet opplysningenes konfidensialitet og integritet ivaretas. Innebygd personvern vil være et bidrag til bedre styring og kontroll med informasjonssikkerheten i de digitale løsningene, og ikke minst bedre informasjonssikkerhet ved den senere bruken av løsningene i etaten. Når personvernet er godt integrert i de digitale løsningene, vil det være færre muligheter for feil bruk eller informasjonssikkerhetsbrudd. En slik tyngre investering vil imidlertid kreve økt ressursbruk, både i form av kompetanse fra ulike fagområder og investering av økonomiske midler.

Kapittel 10 – Regelkompleksitet og nasjonalt handlingsrom

Generelle merknader til kapittel 10

Kommisjonen drøfter under punkt 10 hvordan norske myndigheter kan bruke det nasjonale handlingsrommet som personvernforordningen og EØS-avtalen gir, og gjennom dette legge til rette for lojal etterlevelse av internasjonalt regelverk og imøtekomme særlige norske behov for klarhet og sammenheng i den rettslige reguleringen.

Europa og Norge står overfor økende utfordringer knyttet til grenseoverskridende kriminalitet med et økt trusselbilde knyttet til terror, fremmedkrigere og alvorlig kriminalitet som ID-misbruk, ulovlig migrasjon og menneskehandel.

For å møte disse utfordringene har EU besluttet å styrke samarbeidet på Schengenområdet. Dette innebærer nye krav til grensekontroll og særlig økt informasjonsutveksling på tvers av landene i Europa. Som PU påpeker vil de nye rettsaktene innebære 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).

PU viser til at de nye løsningene fra EU vil innebære en innsamling av biometriske data på brorparten av tredjelandsborgere som reiser inn til Schengen, og at 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. Kommisjonen behandler ikke implementeringen av EUs informasjonssystemer særskilt hverken i utredningens punkt 7 om justissektoren eller punkt 10 om regelkompleksitet og nasjonalt handlingsrom. Politidirektoratet anser, som også PU, at dette er en mangel ved utredningen. Som vi tidligere har nevnt vil innføringen av systemene innebære en utvidelse av både formål med behandlinger og også omfanget av personopplysninger som behandles. Forordningene går langt i å regulere en omfattende behandling og utveksling av personopplysninger for å ivareta hensyn til kontroll og kriminalitetsbekjempelse.

EU-forordningene er gjennomgående innført i norsk rett ved inkorporasjon, det vil si at de gjøres gjeldende som norsk lov uten omskrivninger. Departementet gir imidlertid ikke en fullstendig gjennomgang av det materielle innholdet i rettsaktene i høringsnotatene, men konsentrerer seg om å peke på regelverksendringene som kreves for å gjennomføre forordningene i norsk rett. Dette innebærer at høringsnotatet som forarbeider gir liten veiledning i anvendelsen av regelverket. I tillegg kommer at forordningenes struktur, språkform og tekniske detaljnivå er avvikende fra norsk lovgivningsteknikk, noe som gjør

regelverket vanskelig tilgjengelig både for de som skal anvende forordningene og de som søker informasjon om innholdet i rettsaktene. Vi mener at denne tilnærmingen er uheldig og at man ut fra hensynet til klarhet og sammenheng i regelverket burde gitt en mer utførlig gjennomgang av forordningene i forarbeidene, og eventuelt mer utfyllende regler i forbindelse med inkorporeringen i norsk rett.

Vi viser for øvrig til PU sine merknader i vedlagt høringsuttalelse, side 2 og 3.

Med hilsen

Håkon Skulstad
assisterende direktør

Kristine Langkaas
seksjonssjef

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
Rådgiver Kristin Munthe-Kaas

Vedlegg:
Avgitt høringssvar - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport - Økokrim
Høringsinnspill - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport - Politiets utlendingsenhet
Høringsinnspill - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport - Oslo politidistrikt
Høringsinnspill - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport - Kripos
Høringsinnspill - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport - Nordland politidistrikt
Høringsinnspill - NOU 2022:11 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport - Politihøgskolen
Høringsinnspill - NOU 202211 Ditt personvern - vårt felles ansvar - Personvernkommisjonens rapport - Politiets fellestjenester

Kopi:

Justis- og beredskapsdepartementet	Postboks 8005 Dep	0030	Oslo