



Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 Oslo

Deres referanse:

Vår referanse:
24/269754 - 12

Sted, dato:
Oslo, 29.01.2025

Politidirektoratets høringssvar - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv

Vi viser til Justis- og beredskapsdepartementets høringsbrev av 20. november 2024 om forslag til endringer i politiregisterloven, politiloven, straffeprosessloven, grenseloven og politiregisterforskriften. Etter avtale med departementet har vi fått utsatt høringsfristen til 24. januar 2024. Vi beklager oversittelsen av fristen.

Endringsforslagene gjelder bruk av opplysninger til testing og utvikling av informasjonssystemer innenfor politiregisterlovens og grenselovens virkeområde. I tillegg foreslås forskriftsbestemmelser om PSTs behandling av åpent tilgjengelig informasjon til etterretningsformål etter politiregisterloven ny § 65 a mv.

Politidirektoratet har forelagt høringen for Kripes, Økokrim, Politiets utlendingsenhet (PU), Politiets IT-enhet (PIT) og samtlige politidistrikt. Vi har mottatt svar fra Kripes, PU, PIT og Øst politidistrikt. Svarene fra underliggende enheter følger vedlagt.

Politidirektoratet ønsker endringsforslagene velkommen. Den foreslåtte reguleringen vil klargjøre rettstilstanden på et stadig viktigere område både for politiets digitalisering og for digitalt politiarbeid. Bruk av reelle opplysninger til testing og utvikling vil bidra til å sikre tilstrekkelig kvalitet og sikkerhet i informasjonssystemer som er av stor betydning for politiets kriminalitetsbekjempende virksomhet og oppgaver knyttet til grensekontroll. Underliggende enheter uttaler seg i samme retning.

Nedenfor følger våre kommentarer og endringsforslag strukturert etter de relevante punktene i høringsnotatet. Vi har ingen innspill til de deler av høringen som gjelder PSTs behandling av opplysninger.

Til punkt 2.6.1 og 2.6.3.1 - forholdet mellom personvernforordningen og personverndirektivet

Personvernforordningen kommer ikke til anvendelse på personopplysninger som behandles "*med henblikk på å forebygge, etterforske eller iverksette strafferettslige reaksjoner*", jf. artikkel 2 nr. 2 bokstav d. I henhold til EU-domstolens praksis skal unntaksbestemmelsen i artikkel 2 nr. 2 om saklig virkeområde tolkes strengt. Personvernforordningen skal gjøres til en del av den interne rettsordenen "*som sådan*", jf. EØS-avtalens artikkel 7 bokstav a.

I høringsnotatet punkt 2.6.1 om gjeldende rett heter det at:

Personopplysningsloven gjelder etter § 2 første ledd for all behandling av personopplysninger, med mindre annet er bestemt i eller i medhold av lov. Politiregisterloven er et eksempel på en slik lov, jf. Prop. 56 LS (2017–2018) punkt 4.5.2 der det uttales at: Nasjonale regler som gjennomfører direktiv (EU) 2016/680, vil være et eksempel på slike regler, og reglene vil dermed gå foran bestemmelsene i personopplysningsloven og forordningen. Hvorvidt reglene i personopplysningsloven og forordningen kommer til supplerende anvendelse i disse tilfellene, eller om de er fraveket i sin helhet, må avgjøres på bakgrunn av en tolking av de aktuelle reglene.

Hvorvidt behandling av opplysninger til testing og utvikling av informasjonssystemer som skal brukes til politimessige formål reguleres i sin helhet av politiregisterloven, eller om personopplysningsloven og personvernforordningen helt eller delvis kommer til (supplerende) anvendelse, må dermed bero på en konkret tolkning."

Departementet fremholder videre i høringsnotatet punkt 2.6.3.1 at bruk av opplysninger til testing og utvikling av systemer som skal brukes for politimessige formål, har så nær sammenheng med det opprinnelige formålet at de samme personvernreglene bør gjelde også for denne behandlingen. Departementet påpeker at selv om EU-domstolen i flere saker har uttalt at unntakene i personvernforordningen artikkel 2 nr. 2 skal "*tolkes strengt*", jf. blant annet C-180/21, har dette vært saker hvor det har vært snakk om bruk til formål som skiller seg klarere fra kriminalitetsbekjempelse enn testing og utvikling av informasjonssystemer for politimessige formål. Domstolen har derimot ikke tatt stilling til hvorvidt testing og utvikling av systemer som skal brukes til kriminalitetsbekjempelse faller innenfor personverndirektivets (LED) virkeområde. Departementet mener at testing og utvikling av systemer som skal brukes for politimessige formål, må kunne innfortolkes i formålene med LED artikkel 1 nr. 1 og i politimessige formål, og at LED dermed gjelder for behandlingen. Som følge av dette anser ikke departementet testing og utvikling som et eget eller annet formål enn politimessig formål. Politidirektoratet er enig i dette utgangspunktet.

Det fremgår av LED artikkel 4 nr. 1 at personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål, jf. artikkel 1 nr. 1, og ikke behandles på en måte som er uforenlig med disse formålene. Det følger videre av artikkel 4 nr. 2 at behandling som foretas for et av formålene i artikkel 1 nr. 1, men til et annet formål enn det opprinnelige, skal tillates dersom dette tillates i unionsretten eller nasjonal rett, og behandlingen er nødvendig og forholdsmessig.

LED artikkel 4 er gjennomført i politiregisterloven § 4, som sier at opplysninger som er innhentet for et politimessig formål kan benyttes til andre politimessige formål med mindre det er bestemt i lov eller i medhold av lov at retten er begrenset, i § 5 om nødvendighetskravet, og i § 6 om krav til opplysningenes kvalitet. Det er videre gitt utfyllende bestemmelser i politiregisterforskriften del 2.

Politidirektoratet er kjent med at forholdet mellom politiregisterloven/LED og personvernforordningen er problematisert i Datatilsynets sluttrapport om Politihøgskolens sandkasseprosjekt PrevBOT¹. Vi viser også til vårt innspill av 8. november 2024 til departementets brev av 16. juli 2024 om etterkontroll av personopplysningsloven, hvor

¹ <https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/politihogskolen-sluttrapport-prevbot/>

vi omtaler grensedragningen mellom de to rettsaktene mer generelt. Det er viktig at dette er tydelig vurdert og beskrevet i det videre lovarbeidet.

Til punkt 2.6.3.2 Forslag til lovendringer

Departementet foreslår å utvide politiregisterlovens virkeområde slik at loven også gjelder når opplysninger behandles for testing og utvikling av informasjonssystemer som skal brukes innenfor lovens virkeområde, jf. utkast til politiregisterloven § 3 fjerde ledd nytt annet punktum.

"Utvikling av informasjonssystemer" og avgrensning mot utvikling i straffesak

Kripos uttaler at metodeutvikling som har sitt utgangspunkt i en konkret etterforskning og som skal løse konkrete behov i den aktuelle etterforskningen, ikke kan omfattes av forslaget. Dette ville i så fall bryte med etablerte prosesser og ansvarsforhold for etterforskning. I tillegg ville man ved en slik regulering risikere å "låse" enkeltstående etterforskningsaktiviteter inn i et omfattende godkjenningsregime som kan bidra til at man mister tempo og initiativ i tidskritiske etterforskninger, eksempelvis ved arbeid for å forbigå kryptering under pågående skjult etterforskning.

Politidirektoratet er enig i at det ved vurderingen av bestemmelsens anvendelsesområde må sondres mellom forskjellige utviklingsprosesser. Det er et viktig skille mellom påtalestyrt metodeutvikling som biprodukt av pågående etterforskningsskritt, og øvrig mer planmessig utvikling og testing av informasjonssystemer som forslaget er ment å regulere. For en nærmere begrunnelse av metodeutviklingen og hvordan denne skiller seg fra annen testing og utvikling, viser vi til redegjørelsen i uttalelsen fra Kripos. Vi ber om at departementet klargjør denne avgrensningen i spesialmotivene til den endelige bestemmelsen.

"Innenfor lovens virkeområde"

Politidirektoratet legger, i likhet med PU, til grunn at bestemmelsen er ment å omfatte registre hvor opplysninger behandles dels til politimessige formål og dels til forvaltningsformål, jf. politiregisterforskriften § 1-3 første ledd nr. 3, jf. kapittel 56 om politiets utlendingsregister.

Vi ser samtidig behovet for en avklaring av hvorvidt politiregisterloven § 3 fjerde ledd nytt annet punktum og definisjonen av informasjonssystemer også omfatter systemer som brukes både til forvaltningsformål og politimessige formål, og hvor behandlingen av opplysninger dermed følger både personvernforordningen og LED, men hvor systemet ikke er regulert i politiregisterforskriften del 11.

Et eksempel på informasjonssystem med både forvaltningsmessig og politimessig formål er nytt nasjonalt saksbehandlingssystem REIS som i hovedsak er utviklet for behandling av søknader om fremreisetillatelse etter forordning (EU) 2018/1240 om ETIAS. REIS skal også benyttes når «VIS Designated Authority» (VIS-utpekt myndighet/VDA) behandler treff mellom alfanumeriske eller biometriske opplysninger i søknad om Schengen-visum, D-visum eller oppholdstillatelse opp mot opplysninger registrert i SIS, Europol, Interpol TDAWN, ECRIS-TCN, se artikkel 9a nr. 10 og 22b nr. 9 i VIS endringsforordning.

Ved treff i nevnte systemer skal VIS-utpekt myndighet foreta en vurdering av hvorvidt søkeren utgjør en trussel eller risiko mot offentlig orden og indre sikkerhet i henhold til artikkel 9d og artikkel 9g i endringsforordningen i (EU) 2021/1134, som skal tas i betraktning ved vurdering av om vilkår for Schengen-visum mv. er oppfylt. Slik vi vurderer det, vil denne sikkerhetsvurderingen være av politimessig karakter og ha politimessige formål. Behandlingen av personopplysninger av VIS utpekt myndighet i dette henseende anses derfor å være underlagt LED, som er gjennomført i politiregisterlovgivningen. Behandlingen av visumsøknaden vil for øvrig være underlagt personvernforordningen.

Oppgaven til VIS-utpekt myndighet med å behandle treff er knyttet til behandling av opplysninger fra registre som i dag håndteres ved Kripos (SIS, Europol, Interpol). Hvordan informasjonsutvekslingen mellom VIS-utpekt myndighet og Kripos skal foregå er i dag ikke avklart.

Til punkt 2.6.3.5 Hvilke opplysninger som kan brukes til testing og utvikling og punkt 2.6.3.6 Særlig om opplysninger fra digitale beslag

Opplysninger som er omfattet av politiregisterloven § 8 og opplysninger fra digitale beslag

Departementet foreslår at opplysninger som behandles etter politiregisterloven § 8 (eller § 65) og informasjon fra beslag og utleveringspålegg som ikke inngår i straffesakens dokumenter, ikke skal kunne brukes til testing og utvikling, jf. forslaget til en eksplisitt avgrensning mot disse opplysningene i § 1-5 tredje ledd.

Kripos uttaler at departementet begrunner godt et generelt utgangspunkt om at slike opplysninger ikke skal benyttes til testing og utvikling. Særorganet påpeker imidlertid at den vurdering av nødvendighet, formål og relevans for politiets oppgaveløsning, som må foretas av alle opplysninger som i en innledende fase behandles etter politiregisterloven § 8, vil måtte foretas ved hjelp av digitale hjelpemidler i en eller annen form. Jo større datamengder det er snakk om, jo viktigere vil det være med en effektiv og treffsikker programvare som hjelpemiddel.

På samme måte er politiet avhengig av å ha en optimalt utviklet og testet programvare for med høyest mulig kvalitet å kunne sikre innhold fra databærere som mobiltelefoner og harddisker og for å gjennomgå speilkopier fra slik sikring. I begge tilfeller har det vist seg nødvendig å bruke egenutviklet og innkjøpt programvare i dette arbeidet. Kripos er derfor bekymret for at et generelt forbud mot bruk av personopplysninger til testing og utvikling av slik programvare, i vesentlig grad vil redusere politiets evne til å trekke ut relevante opplysninger fra store datamengder på en mest mulig effektiv og treffsikker måte. Som kjent er bearbeiding av store datamengder i stadig større grad avgjørende for politiets evne til å løse sine oppgaver på flere områder. Slik programvare bør derfor kunne utvikles og testes med utgangspunkt i den type opplysninger programvaren er tenkt brukt på. Bruk av ikke-optimal programvare på dette området vil etter særorganets vurdering representere en større personvernutfordring enn bruk av opplysninger fra materialet til utvikling av optimale løsninger.

Politidirektoratet er enig med Kripos i at det er behov for å gjøre unntak fra forbudet mot bruk av § 8-opplysninger og speilkopier for så vidt gjelder testing og utvikling av informasjonssystemer som er nødvendig for å avklare formålsbestemthet, nødvendighet og relevans, jf. § 8, og for å sikre og gjennomgå beslag eller utleveringspålegg, jf. straffeprosessloven §§ 203 og 210. Vi støtter forslaget fra Kripos til endringer i utkastets § 1-5 tredje ledd.

Til punkt 2.6.3.9 Konsekvensutredninger og forhåndsdrøftinger

Departementet mener at plikten til å rådføre seg med Datatilsynet bør gjelde generelt ved testing og utvikling som kan medføre høy risiko for de registrertes rettigheter og friheter, uavhengig av om behandlingen inngår i et register eller en sammenstilling som nevnt i § 41-2 første ledd. Politidirektoratet er enig i dette. Vi ber departementet vurdere å innta et komma foran det foreslåtte tillegget i § 41 annet ledd første punktum for å tydeliggjøre at det ikke gjelder et slikt krav for at plikten skal komme til anvendelse på testing og utvikling.

Til punkt 2.6.3.10 Særlig om meldeplikt ved testing og utvikling

I høringsnotatet punkt 2.6.3.10 vurderer departementet om politiet bør ilegges en særlig meldeplikt til Datatilsynet for testing og utvikling av informasjonssystemer, men foreslår ikke konkrete regelverksendringer for å innføre en ny meldeplikt. Departementet ber

samtidig om høringsinstansenes syn på hvorvidt en slik meldeplikt bør etableres, og i tilfelle hvordan den kan innrettes.

Kripos uttaler at en eventuell meldeplikt ikke bør bli mer omfattende enn nødvendig, og at en meldeplikt i utgangspunktet først bør vurderes innført dersom det viser seg at Datatilsynet opplever å ikke få tilstrekkelig informasjon gjennom den allerede etablerte muligheten til å kreve opplysninger fra politiet og de foreslåtte ordningene. Politidirektoratet slutter seg til uttalelsen fra Kripos.

Til punkt 2.6.3.11 Personvernkonsekvenser av forslaget

Departementet vurderer i punkt 2.6.3.11 at behandling av opplysninger for testing og utvikling har relativt begrensede konsekvenser for den registrerte. Departementet viser i sin begrunnelse til at testingen og utviklingen ikke vil medføre konsekvenser for den registrertes rettsstilling, at det ikke skal treffes avgjørelser overfor den registrerte, at kravet om den behandlingsansvarliges godkjenning og adgang til å stille nærmere vilkår vil bidra til at behandlingen ikke får større omfang enn nødvendig, samt at kravet om forhåndsdrøftelser vil sørge for at Datatilsynet vil involveres dersom det er snakk om å iverksette testing og utvikling som kan medføre høy risiko.

Siden personvernregelverket gjelder på vanlig måte for test- og utviklingsmiljø, også bestemmelsen om de registrertes rettigheter, vil den registrerte ikke få større rett til innsyn i opplysninger som brukes til testing og utvikling enn det som følger av de alminnelige innsynsreglene i politiregisterloven.

Som påpekt i høringsnotatet punkt 2.6.3.8 vil endringsforslagene medføre tilgang til opplysninger for nye brukergrupper. Den behandlingsansvarlige må vurdere konkret om det skal gis tilgang til opplysninger som underlagt særskilt tilgangsbegrensning til bruk for testing og utvikling. Videre vil forslagene innebære behandling av særlige kategorier opplysninger, herunder opplysninger fra straffesaker. Dette er et moment som taler for at behandlingen kan medføre høy risiko og dermed utløse krav om forhåndsdrøftelser med Datatilsynet. Endringsforslaget vil også innebære behandling av store mengder opplysninger til bruk i maskinlæringsmodeller, samt behandling av ustrukturerte data og ikke-verifiserte opplysninger, jf. høringsnotatet punkt 2.6.3.5.

Departementet viser i sin vurdering til at forslaget ikke innebærer at opplysningene skal utleveres til andre. Politidirektoratet ber om at departementet i det videre lovarbeidet angir nærmere hva som ligger i denne forutsetningen, herunder om dette skal forstås som en begrensning i bruk av reelle personopplysninger til verdikjedetesting, for eksempel eventuell testing av system-til-system-kommunikasjon med andre aktører, eller bruk av eksterne databehandlere ved testing og utvikling og testing og utvikling av skybaserte tjenester.

Til punkt 2.7 Særlig om bruk av informasjon fra skjulte tvangsmidler til testing og utvikling

Departementet foreslår at det i straffeprosessloven § 216 i, som setter rammer for hvilke formål opplysninger fra skjulte tvangsmidler i straffesaker skal kunne brukes til, tilføyes et unntak fra taushetsplikten til bruk av opplysninger for testing og utvikling. I tillegg foreslås det en ny bestemmelse i politiregisterforskriften § 25-4 første ledd om at opplysninger fra kommunikasjonskontroll, romavlytting og dataavlesning som kun er tatt i bruk til testing og utvikling, skal sperres når saken opplysningene er innhentet i er avgjort ved rettskraftig dom eller endelig henleggelsesbeslutning.

Kripos tar til orde for at behovet for den foreslåtte endringen i straffeprosessloven § 216 i bør vurderes på nytt i lys av riksadvokatens brev av 12. november 2024 og at forslaget til forskriftsendringer ikke tas videre. Politidirektoratet viser i sin helhet til uttalelsen fra Kripos på dette punktet.

Regulering av testing og utvikling i grenselovgivningen

Til punkt 2.9.2 Nærmere om behovet

Det bør presiseres i det videre lovarbeidet at den foreslåtte reguleringen gjelder biometriske opplysninger opptatt i grensekontrollen, og ikke biometriske opplysninger fra pass eller lignende dokumenter. Dette vil redusere risikoen for misforståelser.

En praktisk problemstilling er om lovforslaget omfatter situasjonen der man har behov for å kontrollere og teste at utstyret som benyttes i grensekontrollen fungerer korrekt før det benyttes i ordinær drift. Det kan for eksempel være nødvendig å legge fingeravtrykk på opptaksplaten og opptak av ansiktsfoto for å kontrollere at det fungerer optimalt. Formålet, som da vil være å teste kontrollutstyr, dekkes da ikke nødvendigvis av ordlyden i § 22. Dersom denne situasjonen er ment å være dekket av den foreslåtte ordlyden, bør dette fremkomme eksplisitt. Dersom dette ikke anses dekket av bestemmelsen, bør dette inntas. Dette kan eventuelt tas inn som en ny setning i § 22 tredje ledd: *"Slike opplysninger kan også opptas for å teste utstyr som er nødvendig for å gjennomføre grensekontroll."*

I høringsnotatet (side 27 fjerde avsnitt) fremgår det at automatisert ansiktssammenligning vil bli standard metode for undersøkelse av identitet for den personkretsen som er omfattet av EES (tredjelandsborgere). Vi bemerker at det tilsvarende, i tråd med gjeldende regelverk og planlagte rutiner ved innføring av EES, vil bli gjennomført fingeravtrykkssammenligning.

Til punkt 2.9.3 Forslag til endringer

Departementet foreslår en uttrykkelig hjemmel i grenseloven ny § 22 a første ledd for at opplysninger som behandles i forbindelse med grensekontroll kan benyttes til testing og utvikling av informasjonssystemer som brukes for grenseformål. Bestemmelsen er teknologinøytral og gjelder for behandling av opplysninger for det angitte formålet uavhengig av teknisk løsning. Dette inkluderer, men ikke er begrenset til, dagens bruk av Grense- og territorialkontroll-registeret (GTK), register for Forhåndskontroll Sjø (FKS) og register for Forhåndskontroll Land (FKL).

Departementet foreslår at ansiktsfoto og fingeravtrykk opptatt i grensekontrollen kan lagres for en begrenset periode utelukkende for å kunne brukes til testing og utvikling av informasjonssystemer for grensekontrollformål.

Det heter i høringsnotatet at departementet ikke åpner for at opplysninger kan behandles for testing og utvikling etter at de skulle ha vært slettet etter reglene som ga grunnlag for registreringen. Gitt at registrering av biometrisk personinformasjon etter § 22 gjøres for kontroll av reisedokumenter og opplysningene skal slettes når denne kontrollen er gjennomført, er denne formuleringen egnet til å skape uklarheter. Vi viser til at utkastet til § 22 nytt tredje ledd, jf. utkastet til ny § 22a annet ledd, nettopp er en egen hjemmel for at opplysninger kan lagres for bruk til testing og utvikling etter at de ellers skulle ha vært slettet etter reglene som ga grunnlag for registreringen.

Det kan med fordel vurderes å utdype begrepet sensitive opplysninger, evt. særlige kategorier opplysninger, i forskrift for å sikre fleksibilitet og tilpasning til fremtidig teknologiutvikling.

Utvalg av ansiktsfoto og fingeravtrykk

I ny § 22 a er det ikke klare kriterier for hvordan utvalget av ansiktsfoto og fingeravtrykk til testing skal skje. Det kan i større grad fremkomme av forarbeidene at behandlingsansvarlig har et ansvar for at utvalget av personopplysninger til test og utvikling skal bidra til å forhindre bias og diskriminering.

Politidirektoratet gjør oppmerksom på at det på et senere tidspunkt kan bli nødvendig å vurdere behovet for bruk av reelle data til testing og utvikling av systemer som er hjemlet i grenseloven, men som ikke er omfattet av forslaget til endringer i grenseloven § 22 og 22 a. Det er foreløpig ikke avklart om det vil være behov for testing og utvikling med reelle data for systemene som skal muliggjøre nasjonal anvendelse av IO artikkel 20 og 20a (Artikkel 20a innføres ved ikrafttredelse av forordning (EU) 2024/1356 (screeningforordningen)). Etter IO art. 20 og 20a, vil opptak av biometri og søk i CIR etter disse artiklene skje på territoriet med identifiseringsformål (ikke grensekontrollformål).

Til punkt 6 Økonomiske og administrative konsekvenser

Det heter i høringsnotatet at forslaget i seg selv ikke pålegger test- og utviklingsaktiviteter og dermed ikke vil medføre økonomiske og administrative konsekvenser. Testing er imidlertid nødvendig for å gjennomføre og ivareta behandlingsansvarliges plikter etter personvernforordningen til å ivareta integritet, konfidensialitet, tilgjengelighet og riktighet. Se også Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper om IKT-sikkerhet².

Som påpekt av Kripos vil etablering av sporing og analysefunksjonalitet i alle testmiljø hvor det behandles personopplysninger innebære kostnader for politiet. Det samme vil de vilkår som er satt for tillatelser etter forslaget til § 1-5. Slike vil gjerne påløpe andre steder i politiet enn hos den behandlingsansvarlige selv.

Forslag til lov- og forskriftsendringer

Til punkt 7.2 Politiregisterforskriften

I tråd med politiregisterlovgivningens begrepsbruk benyttes "opplysninger" i ny § 1-5. Kripos foreslår at "opplysninger" i den foreslåtte forskriftsbestemmelsen gjennomgående endres til "personopplysninger". Kripos viser til at begrensningene og saksbehandlingsbestemmelsene synes å være utelukkende begrunnet i personvern hensyn og at "personopplysninger" også brukes i andre offentlige organers hjemler for testing og utvikling. Politidirektoratet støtter dette forslaget.

For øvrig viser vi til våre merknader ovenfor til punkt 2.6.3.5 og 2.6.3.9

Til punkt 7.5 Grenseloven

Politidirektoratet foreslår å erstatte "fiktive" opplysninger i forslaget til grenseloven ny § 22 a første ledd med "syntetiske" opplysninger for å sikre samsvar med fagterminologien på dette feltet. For øvrig viser vi til våre merknader ovenfor til punkt 2.9.2.

Vi foreslår videre at begrepet "sensitive opplysninger" i gjeldende grenseloven § 22 første ledd, erstattes med "særlige kategorier av personopplysninger". Dette vil harmonisere bestemmelsen med ordlyden personvernforordningen artikkel 9 nr. 1 og bidra til økt klarhet i lovteksten, jf. også høring av 6. november 2024 om forslag til endringer i grenseloven, utlendingsloven, grenseforskriften og utlendingsforskriften for gjennomføring av forordning (EU) 2024/1717 om endringer i grenseforordningen (EU) 2016/399.

Ordlyden i § gjeldende 22 tredje ledd avgrenser til "ansiktsfoto og fingeravtrykk", noe som er en videreføring av tidligere bestemmelser. Samtidig åpner grenseloven § 15 for å behandle også andre biometriske opplysninger ved gjennomføring av inn- og utreisekontroll, for eksempel iris. Vi har merket oss at det i Prop. 161L (2016-2017) uttrykkelig fremgår at "Det foreslås ingen nye regler for innhenting og lagring av

² <https://nsm.no/getfile.php/1313975-1717589722/NSM/Filer/Dokumenter/Veiledere/NSMs%20Grunnprinsipper%20for%20IKT-sikkerhet%20v2.1.pdf>

biometrisk personinformasjon for grensekontrollformål". Med teknologisk utvikling kan det imidlertid bli nødvendig å inkludere også andre biometriske opplysninger, som irisskanning eller stemmegjenkjenning. Slik bruk vil også kreve testing og utvikling. Vi ser på bakgrunn av dette behovet for å endre § 22 annet ledd slik at bestemmelsens ordlyd ikke avgrenses til spesifikke typer biometriske opplysninger.

Med hilsen

Kristine Langkaas
Seksjonssjef

Gunnvor Hovde
Seniorrådgiver

Dokumentet er elektronisk godkjent uten signatur.

Vedlegg:

Høringsinnspill - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv - Kripos

Brev fra RA - 12.11.2024

Høringsinnspill - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv - Øst politidistrikt

Høringsinnspill - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv - Politiets utlendingsenhet

Høring - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv

Høringsinnspill - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv - Politiets IT-enhet

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:
24/269754

Vår referanse:
24/270771 - 4

Sted, dato:
Oslo, 10.1.2025

Høring - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv

Kripos viser til brev fra Justis- og beredskapsdepartementet av 20. november 2024 om høring av endringer i politiregisterloven og grenseloven mv, samt brev fra Politidirektoratet av 6. desember 2024.

Foreslåtte regler om bruk av opplysninger til test og utvikling av informasjonssystemer innenfor politiregisterlovens virkeområde vil ha stor betydning for Kripos. Det vises særlig til vår rolle som behandlingsansvarlig for de fleste av politiets sentrale registre og vårt (delegerte) ansvar knyttet til behandlingsansvaret for nasjonale, elektroniske straffesaksløsninger, hvor det blant annet inngår å ta stilling til søknader om bruk av opplysninger til test- og utvikling. Som kompetansesenter for norsk politi vil testing og utvikling for øvrig også inngå som en sentral del av den metodeutvikling Kripos er løpende engasjert i.

Kripos ønsker forslagene velkomne. Et regelverk vil klargjøre rettstilstanden på et stadig viktigere område både for politiets digitalisering og for digitalt politiarbeid. Bruk av identifiserbare opplysninger i test og utvikling vil bidra til kvaliteten i løsninger av stor betydning for kriminalitetsbekjempelsen og politiets øvrige oppgaveløsning.

Kripos stiller seg bak de faktiske beskrivelsene i høringsnotatet av politiets virksomhet, utviklingsarbeid og behov. Som departementet peker på vil bestemmelsene omfatte en rekke forskjellige typetilfeller av test og utvikling, hvor ulike hensyn gjør seg gjeldende med varierende styrke. Departementet avgrenser virkeområdet for bestemmelsene mot innmelding og korrigering av feil i programvaren. Kripos støtter dette. Til de øvrige typetilfellene som vil oppstå har vi enkelte særlige kommentarer.

Utvikling i etterforskning

Ved Kripas, og antakelig i andre deler av politiet, deltar utviklere etter behov som del av en etterforskning. Disse utvikler verktøy, gjerne mindre og spesialiserte, for å løse konkrete behov i den aktuelle etterforskning. Det kan for eksempel dreie seg om verktøy for å gjøre opplysninger i spesielle dataformater tilgjengelige for etterforskere i en for dem forståelig form. Denne virksomheten skiller seg ikke fra andre situasjoner hvor spesialister bidrar med sin kompetanse inn i en etterforskning. Virksomheten vil på vanlig måte være underlagt etterforskningsledelsen, herunder påtalefaglig etterforskningsledelse.

Slik *metodeutvikling i sak* skiller seg vesentlig fra den testing og utvikling som forslaget søker å regulere:

- Formålet med utviklingen er ikke metodeutvikling i seg selv, men å bidra til å oppklare saken. At det kan resultere i en ny eller forbedret metode er et mer eller mindre tilfeldig overskuddsprodukt.
- Ansvarsforholdene er som i etterforskning for øvrig; det er påtalefaglig etterforskningsledelse som står ansvarlig for at virksomheten drives i henhold til gjeldende regelverk.
- Utvikler er integrert i etterforskningen.
- Utviklers leveranser er gjerne små og spesialiserte verktøy tilpasset den enkelte sak, men slik at disse kan gjenbrukes der samme problemstilling oppstår i en senere etterforskning.
- Utviklingen skjer saksnært, og er som utgangspunkt kun basert på opplysninger som er en del av aktuell etterforskning.

For Kripas synes det klart at denne type metodeutvikling, som har sitt utgangspunkt i et konkret etterforskningsformål, ikke kan omfattes av foreslått regelverk. Det vil i så fall bryter med etablerte prosesser og ansvarsforhold for etterforskning. Man risikerer i tillegg å "låse" enkeltstående etterforskningsaktiviteter inn i et omfattende godkjenningsregime, hvilket kan bidra til at man mister tempo og initiativ i tidskritiske etterforskninger, eksempelvis ved arbeid for å forbigå kryptering under pågående skjult etterforskning.

Kripas foreslår derfor at det i merknadene til endelig forslag tydelig avgrenses mot test og utvikling som skjer som etterforskning av konkret straffesak. Etter vår oppfatning vil en slik avgrensning i lite omfang påvirke den test og utvikling som forslaget har som formål å regulere.

Opplysninger omfattet av politiregisterloven § 8 og beslaglagte opplysninger som ikke inngår i sakens dokumenter

Kripas synes departementet begrunner godt et generelt utgangspunkt om at opplysninger omfattet av politiregisterloven § 8 og opplysninger som ikke inngår i sakens dokumenter ikke skal benyttes til test og utvikling.

Kripas vil imidlertid påpeke at den vurdering av opplysningers relevans og betydning for politiets oppgaveløsning, som må foretas for alle opplysninger som innledningsvis behandles etter politiregisterloven § 8, vil måtte gjøres ved hjelp av digitale hjelpemidler i en eller annen form. Jo større datamengder det er snakk om å vurdere, jo viktigere vil det være med en effektiv og treffsikker programvare som hjelpemiddel.

På samme måte er politiet avhengig av optimalt utviklet og testet programvare for med høyest mulig kvalitet å kunne sikre innhold fra databærere (som mobiltelefoner og

harddisker) og for å gjennomgå speilkopier fra slik sikring. I begge tilfeller har det vist seg nødvendig å bruke både egenutviklet og innkjøpt programvare i arbeidet. Kripos er derfor bekymret for at et generelt forbud mot bruk av personopplysninger til test og utvikling av slik programvare vil vesentlig redusere politiets evne til å trekke ut relevante opplysninger fra store datamengder på en mest mulig effektiv og treffsikker måte. Bearbeiding av store datamengder er som kjent i stadig større grad avgjørende for politiets evne til å løse sine oppgaver på flere områder. Slik programvare bør derfor kunne utvikles og testes med utgangspunkt i den type opplysninger programvaren er tenkt brukt på. Bruk av ikke-optimal programvare på dette området vil etter vår vurdering representere en større personvernutfordring enn bruk av opplysninger fra materialet til utvikling av optimale løsninger.

Med dette som utgangspunkt ønsker Kripos at det gjøres et unntak - for testing og utvikling av slike systemer - fra den regel som er foreslått i forskriften § 1-5 tredje ledd. Et forslag til formulering fremgår nedenfor i våre merknader til § 1-5.

Opplysninger innhentet gjennom kommunikasjonskontroll, romavlytting og dataavlesning

Departementet foreslår endring av straffeprosessloven § 216 i, ved at test og utvikling tilføyes som unntak fra taushetsplikten. Videre foreslås det endringer i politiregisterforskriften § 25-4 første ledd om at opplysninger fra kommunikasjonskontroll, romavlytting og dataavlesning som kun er tatt til bruk til testing og utvikling skal sperres når saken opplysningene er innhentet i er avgjort ved rettskraftig dom eller endelig henleggelsesbeslutning.

Kripos viser til brev 12. november 2024 fra riksadvokaten, vedlagt her. I brevet punkt 2 tredje avsnitt skriver Riksadvokatembetet at "(...) § 216 i er en bestemmelse om taushetsplikt, som dermed kun regulerer i hvilken utstrekning opplysningene kan brukes utad og ikke legger begrensninger på politiets interne bruk". Dette utgangspunktet, som også følger av forarbeider til straffeprosessloven, ligger til grunn for embetets videre føringer i nevnte brev. Kripos finner det derfor uklart hva departementet legger til grunn når det uttales på side 22 i høringsnotatet at bestemmelsen også "innebærer en regulering av hvilke formål opplysningene skal brukes til", og at nevnte bestemmelser har karakter av formålsbegrensninger.

Legger man riksadvokatens utgangspunkt til grunn vil det etter vår oppfatning ikke være like stort behov for endring i straffeprosessloven for å hjemle bruk av denne type opplysninger til test og utvikling internt i politiet. I så fall vil foreslått § 216 i første ledd tredje punktum bokstav l måtte leses som et unntak fra taushetsplikten vis-à-vis bruk utenfor politiet, hvilket vi oppfatter å være i strid med departementets intensjon. Vi foreslår derfor at behovet for lovendring vurderes på ny i lys av riksadvokatens brev.

Når det gjelder forslaget i § 25-4 om sperring av opplysninger til test og utvikling fremstår dette for Kripos som lite praktikabelt og også vanskelig forenelig med føringene i ovennevnte brev fra riksadvokaten. Rent praktisk vil opplysninger fra kommunikasjonskontroll, romavlytting og dataavlesning merkes idet de overføres til bruk for andre interne politiformål. Merking kan imidlertid ikke gjøres slik at opplysningene senere maskinelt kan skilles ut og sperres i systemene de overføres til. En slik løsning er derfor ikke gjennomførbar i dagens politisystemer og vil i så fall forutsette etablering av manuelle prosesser som etter Kripos' vurdering ikke står i rimelig forhold til de personvernfordeler man vil oppnå. Snarere tvert imot. En slik regel vil i praksis stenge for testing og utvikling på et område hvor optimal programvare er sentralt for at denne type opplysninger kan behandles med høy kvalitet. Kripos kan heller ikke se at foreslått

regel er umiddelbart forenelig med det utgangspunkt riksadvokaten legger til grunn i ovennevnte brev. For Kripos synes embetets klare utgangspunkt å være at forskriften § 25-4 omhandler innhentingssaken og at lovens systematikk er at denne ikke skal påvirke behandling av opplysninger overført derfra til andre formål. Kripos foreslår følgelig at forslaget om endringer i § 25-4 ikke tas videre.

Særlig merknader til politiregisterforskriften § 1-5

I tråd med politiregisterlovgivningens systematikk brukes "opplysninger" i den foreslåtte bestemmelsen om test og utvikling, ikke "personopplysninger". Begrensningene og saksbehandlingsreglene som foreslås synes imidlertid utelukkende å være motivert av personvern hensyn. Også de tilsvarende hjemlene fra andre samfunnsområder som gjennomgås i høringsnotatet gjelder for behandling av personopplysninger.

Siden også personopplysninger er definert i politiregisterloven § 2, synes det derfor nærliggende å knytte begrensninger og saksbehandlingsregler til dette begrepet også i § 1-5, mens tilgangsreglene i § 8-2 bør knyttes til "opplysninger" som foreslått i høringsnotatet. På denne måten vil politiet og påtalemyndigheten få noe større anledning til å teste og utvikle på bakgrunn av opplysninger som ikke er personopplysninger – og som da heller ikke vil gripe inn i personvernet på samme måte.

Som nevnt over ser Kripos også behov for - i noen avgrensede sammenhenger - å kunne teste og utvikle med utgangspunkt i opplysninger omfattet av politiregisterloven § 8 og opplysninger hentet fra digitale beslag. Etter dette foreslår Kripos følgende (kursiverte) justeringer i § 1-5:

§ 1-5 Testing og utvikling av informasjonssystemer

Personopplysninger kan bare behandles til testing og utvikling av informasjonssystemer dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger.
Personopplysningene skal ikke brukes til testing og utvikling lenger enn nødvendig.

Behandling av *personopplysninger* til testing og utvikling skal godkjennes av den behandlingsansvarlige. Den behandlingsansvarlige kan stille nærmere krav til behandlingen, herunder til behandlingens varighet, hvilke typer opplysninger som skal brukes og omfanget av behandlingen. Kravene skal dokumenteres.

Personopplysninger som behandles etter *politiregisterloven* §§ 8 og 65 kan ikke behandles til testing og utvikling. *Personopplysninger* som innhentet ved beslag eller utleveringspålegg, jf. straffeprosessloven §§ 203 og 210, kan bare behandles til testing og utvikling dersom de inngår i straffesakens dokumenter. *Behandling nevnt i første og andre punktum kan likevel skje for testing og utvikling av informasjonssystemer nødvendige for å avklare formålsbestemthet, nødvendighet og relevans jf. politiregisterloven § 8 eller for testing og utvikling av informasjonssystemer nødvendige for å sikre og gjennomgå beslag eller utleveringspålegg, jf. straffeprosessloven §§ 203 og 210.*

Dersom behandling til testing og utvikling skjer atskilt fra annen behandling, skal *personopplysningene* slettes når de ikke lenger er nødvendig for testing og utvikling, og senest samtidig med at de slettes i det registeret vedkommende er registrert. *Personopplysningene* skal tilintetgjøres.

Økonomiske og administrative konsekvenser

Etablering av sporing og analysefunksjonalitet i alle testmiljø hvor det behandles personopplysninger vil innebære kostnader for politiet. Det samme vil de vilkår som er satt for tillatelser etter forslaget til § 1-5. Slike vil gjerne påløpe andre steder i politiet enn hos den behandlingsansvarlige selv.

Departementet ber særlig om høringsinstansenes syn på etablering av meldeplikt til Datatilsynet. Datatilsynet har etter politiregisterlov og -forskrift vidtgående muligheter til å kreve opplysninger fra politiet. Tilsynet orienteres i tillegg også gjennom mer uformelle og regelmessige møter. Departementet foreslår en utvidet ordning med forhåndsdrøftelser ved høy risiko. Fra Kripas' side er man opptatt av at en eventuell meldeordning ikke blir mer omfattende og ressurskrevende enn nødvendig. Vårt utgangspunkt er at en meldeplikt først bør vurderes innført dersom det viser seg at Datatilsynet ikke opplever å få tilstrekkelig informasjon gjennom de etablerte og foreslåtte ordninger.

Med hilsen

Ketil Haukaas

assisterende sjef Kripas

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:

Jarle Langeland
seniorrådgiver



RIKSADVOKATEN

Troms og Finnmark statsadvokatembeter
Postboks 2503
9267 TROMSØ

Deres referanse:

Vår referanse:

Dato:

24/2759 - 1 / EKY001

12.11.2024

Behandling i kriminaletterretningsregisteret (Indicia) av opplysninger innhentet ved bruk av skjulte tvangsmidler – forholdet til politiregisterloven § 50 tredje ledd mv.

1. Bakgrunn og problemstilling

Det vises til brev 14. september d.å. fra Troms og Finnmark statsadvokatembeter samt til brev 6. s.m. fra Troms politidistrikt. Brevene er foranlediget av tilsynsrapport 15. mai 2023 fra Kontrollutvalget for kommunikasjonskontroll, der Troms politidistrikt ble pålagt å forelegge for riksadvokaten «spørsmålet om politiregisterloven § 50 tredje ledd 'stenge[r] for å bruke opplysninger innhentet ved skjult metodebruk i Indicia'». Riksadvokaten slutter seg i det vesentlige til politiets og statsadvokatens vurderinger, men finner likevel grunn til å foreta en selvstendig gjennomgang og drøftelse av problemstillingen og de underliggende spørsmål den reiser.

Indicia er politiets datasystem for kriminaletterretning. Hjemmel for behandling av opplysninger i Indicia, er straffeprosessloven og politiregisterloven. Nærmere regler om kriminaletterretningsregisteret er gitt i politiregisterloven § 11, jf. § 5 nr. 2 og politiregisterforskriften kapittel 47, som også har regler om sperring og sletting, jf. §§ 47-13 og 47-14, jf. politiregisterloven §§ 50 og 51. I den grad opplysninger fra kommunikasjonskontroll (KK), romavlytting (RA) og dataavlesing (DA) overføres til kriminaletterretningsregisteret, oppstår spørsmål om forholdet til den særlige sperreregelen som gjelder for slike opplysninger, jf. politiregisterloven § 50 tredje ledd.

Spørsmålet om hvilke regler som gjelder for sletting og sperring, henger nært sammen med adgangen til å benytte opplysninger fra KK, RA og DA til andre formål enn forfølgning av det forhold som begrunnet kontrollen, jf. straffeprosessloven § 216 i. Riksadvokaten vil derfor først redegjøre for grunnlaget for å benytte slike opplysninger til etterretningsformål, herunder i form av registrering i kriminaletterretningsregisteret (punkt 2). Deretter drøftes forholdet til politiregisterloven § 50 tredje ledd (punkt 3). Til sist behandles enkelte relaterte spørsmål om utlevering av opplysninger og forholdet til politiets forvaltningsvirksomhet, samt om informasjonssikkerhet og ansvarsforhold (punkt 4).

2. Forholdet til straffeprosessloven § 216 i

Rammene for bruk av opplysninger som stammer fra KK følger først og fremst av straffeprosessloven § 216 i, som gjelder tilsvarende for opplysninger fra RA og DA, jf. § 216 m siste ledd og § 217 o siste ledd. Utgangspunktet er at opplysninger fra KK, RA og DA er underlagt streng taushetsplikt og bare kan benyttes i den utstrekning det følger av § 216 i første ledd tredje punktum bokstavene a til k.

Etterretning er ikke nevnt blant formålene som gir grunnlag for unntak fra taushetsplikten. Etter riksadvokatens vurdering må bestemmelsen likevel forstås slik at den som et klart utgangspunkt ikke er til hinder at opplysninger fra KK, RA og DA, benyttes til etterretningsformål. Dette gjelder enten det er tale om etterretning som ledd i etterforskning eller i polisært øyemed. Om sontringen vises det til riksadvokatens rundskriv nr. 3/1999, punkt II nr. 3.

Hvis det er tale om etterretning som ledd i etterforskning, følger det av § 216 i første ledd tredje punktum bokstav a, at slik bruk er lovlig, idet det vil være tale om bruk «som ledd i etterforskningen av et straffbart forhold». Grensen mot polisært etterretning er imidlertid ikke avgjørende i denne sammenheng, idet § 216 i er en bestemmelse om taushetsplikt, som dermed kun regulerer i hvilken utstrekning opplysningene kan brukes utad og ikke legger begrensninger på politiets interne bruk. Dette er også uttrykkelig forutsatt i lovens forarbeider. Utover forarbeidshenvisningene som er nevnt i brevet fra Troms politidistrikt, vises det til Ot.prp. nr. 64 (1998–99), merknadene til § 216 i, side 161–162, der det uttales:

«Tredje punktum er et unntak fra taushetsplikten i første og annet punktum. Bestemmelsen regulerer derfor bare i hvilken utstrekning opplysningene kan brukes utad – ved at de [meddeles] til andre. Bestemmelsen legger ikke begrensninger på politiets adgang til å bruke overskuddsinformasjon til å avverge straffbare handlinger så lenge dette kan skje uten at opplysningene meddeles til andre.

Politiet kan dermed på bakgrunn av overskuddsinformasjon foreta taktiske disposisjoner for å avverge en forseelse eller en forbrytelse som bare kan medføre bot. Politiet får for eksempel på bakgrunn av kommunikasjonskontroll kjennskap til at to unggutter avtaler å kappkjøre på en nærmere bestemt veistrekning en bestemt dag. Taushetsplikten er da ikke til hinder for at politiet kjører med uniformert bil på denne veistrekningen på det aktuelle tidspunktet.»

Videre vises det til Prop. 61 L (2016–2017) side 3–4:

«Bestemmelsen setter bare begrensninger i adgangen til å bruke opplysningene utad, ved at de meddeles andre. Bestemmelsen legger dermed ikke begrensninger på politiets adgang til å bruke informasjonen dersom dette kan skje uten at [den] videreformidles til andre.»

Se likeledes Bruce og Haugland, *Skjulte tvangsmidler* (2. utgave), punkt 14.4 (side 298), der det imidlertid uttales at «[e]n grense må trolig trekkes ved deling til bruk i politiets forvaltningsmessige virksomhet».

Spørsmålet om adgangen til bruk i politiets forvaltningsvirksomhet er aktuelt i denne sammenheng, fordi politiregisterforskriften § 47-8 første ledd åpner for tilgang til kriminaletterretningsregisteret i den utstrekning det er nødvendig for utøvelsen av politiets forvaltningsvirksomhet. Bruk av overskuddsinformasjon i forvaltningsøyemed er nærmere omhandlet i Ot.prp. nr. 64 (1998–99), punkt 8.9.4:

«Departementet er enig med Metodeutvalget i at overskuddsinformasjon ikke bør kunne brukes til forvaltningsgjøremål. Departementet vil heller ikke foreslå en slik unntaksregel som utvalget går inn for. Det er store betenkeligheter knyttet til lagring av opplysningene. Og hvis det, som utvalget foreslår, ikke skal skje noen lagring, forsvinner mye av poenget med å kunne bruke overskuddsinformasjonen. Informasjonen er dessuten ofte usikker. Rettssikkerhetshensyn taler derfor for at adgangen avskjæres helt. Departementet viser her til de motforestillinger som Metodeutvalget selv har gjort gjeldende og til Advokatforeningens høringsuttalelse.»

I punkt 8.9.4.1 i proposisjonen, fremgår det at Metodeutvalget mente at det burde gjøres unntak ved at det «åpnes en adgang til å bruke overskuddsinformasjon fra kommunikasjonskontroll i saker om overtredelse av straffeloven kapittel 8 eller 9 ved klarering og autorisering av personer som skal jobbe med sikkerhetsklarert materiale». Dette fikk imidlertid ikke tilslutning av departementet, jf. det som er gjengitt over («[d]epartementet vil heller ikke foreslå en slik unntaksregel som utvalget går inn for»), samt følgende uttalelse i merknadene til § 216 i, på side 162:

«Departementet går ikke inn for at overskuddsinformasjon skal kunne brukes ved personkontroll, slik Metodeutvalget foreslår (se 8.9.4)»

Etter riksadvokatens syn er det imidlertid noe uklart om uttalelsene om bruk i forvaltningsøyemed også omfatter rent intern bruk. I lys av de generelle uttalelsene om at taushetsplikten ikke er til hinder for bruk så lenge opplysningene ikke meddeles utad, ville det vært naturlig at det ble sagt uttrykkelig dersom det hadde vært meningen også å begrense den interne bruken. Dette gjelder desto mer ettersom taushetsplikt i alminnelighet ikke er til hinder for at opplysninger deles internt, herunder til bruk i politiets forvaltningsvirksomhet, så lenge det foreligger tjenstlig behov, se politiregisterloven §§ 21 og 29, jf. også Ot.prp. nr. 108 (2008–2009), punkt 11.6.1, der rettstilstanden forut for politiregisterloven beskrives slik:

«Den interne informasjonsflyten i politiet og påtalemyndigheten er regulert i henholdsvis politiloven § 24 fjerde ledd og straffeprosessloven § 61c nr. 3, og begge gjenspeiler prinsippet om at det ikke finnes begrensninger i adgangen til å utveksle opplysninger innad i politiet. Selv om ordlyden i bestemmelsene ikke er identiske, slår begge bestemmelsene fast at taushetsplikten ikke er til hinder for at opplysninger blir gjort kjent for andre tjenestemenn i politiet og påtalemyndigheten dersom tjenstemessig behov tilsier det. Bestemmelsene skiller heller ikke mellom politiets ulike oppgaver, noe som innebærer at opplysninger som er innhentet i forbindelse med politiets kriminalitetsbekjempende virksomhet kan gjøres tilgjengelig for politiets forvaltningsvirksomhet.»

Når uttalelsene i Ot.prp. nr. 64 (1998–99) sammenholdes med de nevnte rettslige utgangspunktene, antar riksadvokaten at det ikke er grunnlag for å tolke taushetsplikten etter § 216 i på en slik måte at den er til hinder for å benytte overskuddsmateriale fra KK, RA og DA i politiets forvaltningsvirksomhet, så lenge det er tale om rent intern bruk. En annen sak er at bruk i forvaltningsøyemed ofte vil forutsette at opplysningene kan utleveres, for eksempel til en part i forvaltningssaken, og i så fall må det være klart at opplysningene ikke kan brukes.

På denne bakgrunn legger riksadvokaten til grunn at taushetsplikten etter straffeprosessloven § 216 i ikke er til hinder for registrering i kriminaletterretningsregisteret, så lenge opplysningene ikke meddeles utad. Begrensningene i adgangen til utlevering og forholdet til bruk i politiets forvaltningsvirksomhet, omtales nærmere i punkt 4.

3. Forholdet til politiregisterloven § 50 tredje ledd

Spørsmålet er så hvilke regler om oppbevaring, sletting og sperring som gjelder i tilfeller der opplysninger fra KK, RA eller DA overføres fra saken opplysningene er innhentet i (innhentingssaken) til bruk i en annen sak eller for øvrig til et annet formål (sekundærsaken), herunder særlig hvilke regler som gjelder ved overføring til kriminaletterretningsregisteret.

Utgangspunktet er at opplysninger innhentet ved KK, RA og DA, og som ikke er brukt i saken, skal sperres når saken er endelig avgjort, jf. straffeprosessloven §§ 216 g første ledd, 216 m siste ledd og § 216 o siste ledd, jf. politiregisterloven § 50 tredje ledd første punktum, som lyder:

«Opplysninger innhentet ved kommunikasjonskontroll som ikke er brukt i saken, skal sperres når saken er avgjort ved rettskraftig dom eller endelig henleggelsesbeslutning.»

Som det fremgår, gjelder sperreplikten kun for «opplysninger ... som *ikke* er brukt i saken». Hva som skal skje med opplysninger som *er* brukt i saken, sier bestemmelsen ikke noe om, men det følger forutsetningsvis at slike opplysninger ikke skal sperres, jf. også Prop. 4 (2019–2020), merknadene til § 50, side 25–26:

«Etter første punktum skal opplysninger som er «brukt i saken» ikke sperres. Under etterforskningen vil enkelte opplysninger fra kommunikasjonskontroll i praksis bli brukt og inngå i flere av straffesakens dokumenter (eksempelvis avhørsrapporter, rettsbøker, påtegningsdokumenter m.v.). Formuleringen «brukt i saken» innebærer at disse dokumentene følger hovedregelen i politiregisterforskriften § 25-3, og ikke skal sperres. Et krav om sperring av slike dokumenter ville resultert i tilfeldige utslag av sperringsregelen for sentrale dokumenter under etterforskningen, og også vært meget ressurskrevende.»

Sperreplikten avhenger altså av om opplysningene er brukt til det formål de er innhentet, eller ikke. Det er opplysninger som ikke er brukt – overskuddsmaterialet – som skal sperres. For opplysninger som *er* brukt i straffesak, gjelder de alminnelige reglene for oppbevaring av straffesaksdokumenter.

Det som er sagt så langt gjelder innhentingssaken. Forholdet mellom sperring i innhentingssaken og adgangen til å overføre opplysninger til andre formål, er nærmere regulert i politiregisterforskriften § 25-4 første ledd, som lyder:

«Før sperring etter politiregisterloven § 50 tredje ledd finner sted, kan opplysninger overføres og brukes til andre formål innenfor rammen av straffeprosessloven § 216i. Politiregisterloven § 50 tredje ledd gjelder også for opplysninger som er overført etter første punktum.»

Det følger av det som er sagt i punkt 2 at registrering i kriminaletterretningsregisteret, etter riksadvokatens oppfatning, i utgangspunktet ligger «innenfor rammen av straffeprosessloven § 216i». Så langt dette rekkes, klargjør første punktum at det er adgang til å overføre opplysninger fra innhentingssaken før sperring etter § 50 tredje ledd. Forskriften kan imidlertid ikke forstås slik at den også gir rettslig grunnlag for sekundærbruken. Overføring forutsetter dermed at den videre bruken har et selvstendig behandlingsgrunnlag, jf. nærmere nedenfor.

Annet punktum slår fast at politiregisterloven § 50 tredje ledd «gjelder også for opplysninger som er overført etter første punktum». Troms politidistrikt tolker dette som en «*presisering om at sperring skal skje i innhentingssaken ... selv om opplysningene har blitt overført og tatt i bruk under et annet formål. Altså at slette/sperreplikten i innhentingssaken ikke suspenderes som følge av at opplysningene er overført*» (uthevet her).

Riksadvokaten er enig i at dette er en plausibel fortolkning. En slik presisering er riktignok overflødig, ettersom sperreplikten i innhentingssaken er uttrykkelig regulert av politiregisterloven § 50 tredje ledd, jf. over, men forståelsen har støtte i forarbeidene, jf. Prop. 4 L (2019–2020), punkt 5.1.4:

«I forskriften vil det bli presisert at reglene om sperring og sletting også skal komme til anvendelse når opplysningene kan behandles videre etter straffeprosessloven § 216 i. Sperring av opplysningene i innhentingssaken skal imidlertid ikke påvirke den videre behandlingen av opplysninger som allerede er overført til andre formål.»

Uttalelsen trekker temmelig klart i retning av at det er sperreplikten i innhentingssaken som er tema, og som presiseres i forskriften § 25-4 første ledd annet punktum.

Spørsmålet om hvilke regler som styrer den videre behandlingen i sekundærsaken, er så vidt en kan se ikke uttrykkelig løst, verken i politiregisterloven eller politiregisterforskriften. Det er imidlertid klart at «[s]perring av opplysningene i innhentingssaken [ikke] skal ... påvirke den videre behandlingen av opplysninger som allerede er overført til andre formål», jf. ovennevnte forarbeidsuttalelse. Dette må forstås slik at den videre behandlingen i sekundærsaken skal vurderes løsrevet fra innhentingssaken.

Gitt at sekundærbruken skal vurderes for seg, synes det nærliggende å ta utgangspunkt i at reglene i politiregisterloven om oppbevaring, sletting og sperring, kommer til anvendelse på vanlig måte. Dette innebærer blant annet at det må foreligge et behandlingsgrunnlag. De sentrale bestemmelsene i denne sammenheng er politiregisterloven § 4, jf. § 11, jf. § 5 nr. 2.

Det vises særlig til § 4, som slår fast at «[o]pplysninger kan behandles til det formålet de er innhentet for *eller til andre politimessige formål, med mindre det er bestemt i lov eller i medhold av lov at retten til behandling er begrenset ...*» (uthevet her). Behandling i kriminaletterretningsregisteret er klart nok et «politimessig formål». Straffeprosessloven § 216 i innebærer i utgangspunktet at «retten til behandling er begrenset», men riksadvokaten mener altså at bestemmelsen ikke begrenser adgangen til registrering i kriminaletterretningsregisteret, så lenge opplysningene ikke meddeles utad. Andre lovbestemte begrensninger foreligger så vidt vites ikke. De grunnleggende kravene til formålsbestemthet, jf. § 4, er dermed oppfylt, og det nærmere grunnlaget for behandling i kriminaletterretningsregisteret følger som nevnt over av § 11, jf. § 5 nr. 2, jf. politiregisterforskriften kapittel 47.

Hvilke regler som gjelder for sletting og sperring er ikke opplagt, men i utgangspunktet er det ingenting ved ordlyden i politiregisterloven § 50 tredje ledd som står i veien for også å anvende bestemmelsen når opplysninger fra KK, RA og DA er overført til et sekundært formål. Etter riksadvokatens syn vil dette også som hovedregel ha gode grunner for seg, for å sikre sammenheng i regelverket og unngå at overføring til andre formål undergraver de hensyn sperreplikten i § 50 tredje ledd skal ivareta. Riksadvokaten antar således at § 50 tredje ledd i utgangspunktet også kommer til anvendelse på materiale i sekundærsaken. Hvor langt dette utgangspunktet rekker, beror på fortolkning.

Bestemmelsen synes uten videre anvendelig ved overføring til bruk i annen straffesak, jf. straffeprosessloven § 216 i første ledd tredje punktum bokstavene c eller d. Dersom det i slike tilfeller overføres flere opplysninger enn det som faktisk blir brukt, gir det fullgod mening at opplysningene som «ikke er brukt i saken», altså overskuddsmaterialet, skal sperres i tråd med § 50 tredje ledd, mens opplysningene som blir brukt, oppbevares på linje med de øvrige straffesaksdokumentene, på samme måte som i innhentingssaken.

Ordlyden passer imidlertid ikke like godt ved overføring til enkelte andre formål. Dette gjelder blant annet ved overføring til kriminaletterretningsregisteret, som i hovedsak omhandler registrering «utenfor den enkelte straffesak», jf. politiregisterloven § 11 jf. § 5 nr. 2. Sperreplikt med utgangspunkt i vilkårene «brukt i saken» og «avgjort ved rettskraftig dom eller endelig henleggelsesbeslutning», synes i en slik sammenheng lite treffende.

En kunne se for seg en løsning der bestemmelsen likevel anvendes så langt den passer. I grove trekk kunne dette innebære at opplysninger som overføres, men ikke blir brukt til det aktuelle formål, skal sperres, mens opplysninger som blir brukt til formålet, skal anses «brukt i saken» og dermed – i tråd med det som gjelder i straffesak – følge reglene for oppbevaring, sletting og sperring på vedkommende område. At opplysninger som er brukt, skal oppbevares etter reglene på det aktuelle området, er lagt til grunn i riksadvokatens brev 31. august 2022 om sletting og sperring av materiale fra kommunikasjonskontroll mv. i eldre saker, jf. side 2 siste avsnitt.

En slik tilnærming kan nok ha gode grunner for seg i enkelte tilfeller, men i relasjon til kriminaletterretningsregisteret, antar riksadvokaten at lite vil være vunnet ved en slik løsning.

Sentralt i så måte er at såfremt vilkårene for registrering i kriminaletterretningsregisteret er oppfylt, vil overføring og registrering i seg selv antagelig innebære at opplysningene må anses «brukt» til formålet. Med andre ord vil det – forutsatt lovlig registrering – ikke foreligge noe overskuddsmateriale som det gir mening å sperre etter prinsippet i politiregisterloven § 50 tredje ledd.

I den grad det overføres opplysninger som viser seg ikke å fylle vilkårene for registrering eller for øvrig ikke å bli brukt til etterretningsformål, må det være klart at opplysningene ikke kan oppbevares, utover det som er nødvendig for å avklare registreringsspørsmålet. Dette vil imidlertid uansett følge av den alternative bestemmelsen om sletting og sperring, jf. politiregisterloven § 50 første ledd, som fastslår at «[o]pplysninger skal ikke lagres lenger enn det som er nødvendig for formålet med behandlingen». Riksadvokaten har således vanskelig for å se at en tilpasset anvendelse av politiregisterloven § 50 tredje ledd, i den sammenheng det her er tale om, vil gi et mer betryggende eller strengere regime enn det som følger av § 50 første ledd.

Etter en samlet vurdering antar riksadvokaten at det i relasjon til kriminaletterretningsregisteret ikke er grunnlag for anvendelse av § 50 tredje ledd, som beskrevet over, og at spørsmål om sletting og sperring av opplysninger som stammer fra KK, RA, eller DA i stedet skal vurderes etter de alminnelige reglene om oppbevaring, sletting og sperring som gjelder for registeret, herunder politiregisterloven § 50 første ledd. Det synes uansett klart at sperreplikten som gjelder for innhentingssaken, er uten betydning, jf. det som er sagt over om at spørsmålet om sperring i sekundærsaken skal vurderes for seg.

Riksadvokaten legger etter dette til grunn at politiregisterloven § 50 tredje ledd ikke er til hinder for at opplysninger fra KK, RA og DA registreres i kriminaletterretningsregisteret.

4. Særlig om utlevering av opplysninger, forholdet til politiets forvaltningsvirksomhet, krav til informasjonssikkerhet og ansvarsforhold

Som nevnt i punkt 2, gjelder etter straffeprosessloven § 216 i streng taushetsplikt for opplysninger fra KK, RA og DA. Riksadvokaten legger til grunn at § 216 i går foran reglene om *utlevering og innsyn* som ellers gjelder for opplysninger i kriminaletterretningsregisteret, jf. politiregisterforskriften § 47-8 til § 47-11, jf. også Høyesteretts avgjørelse HR-2020-1263-A. Opplysninger i kriminaletterretningsregisteret som stammer fra KK, RA og DA, kan følgelig bare utleveres innenfor rammene av § 216 i første ledd tredje punktum bokstavene a–k. Dette må også gjelde i relasjon til politiregisterforskriften § 47-8 første ledd om tilgang til kriminaletterretningsregisteret som ledd i utøvelsen av politiets *forvaltningsvirksomhet*. I den grad det ikke allerede foreligger, må det etableres rutiner for tilgangsbegrensninger og merking (med distribusjonskoder mv.) av opplysninger fra KK, RA og DA, slik at utlevering og bruk i strid med straffeprosessloven § 216 i, forhindres.

Registrering i Indicia reiser også spørsmål om *informasjonssikkerhet og systemkrav*. Opplysninger fra KK, RA og DA skal oppbevares etter reglene i beskyttelsesinstruksen, jf. kommunikasjonskontrollforskriften § 7 annet ledd og § 9 annet ledd. Beskyttelsesinstruksen § 12 oppstiller særlige krav til informasjonssikkerhet mv. Politidirektoratet har opplyst at

Indicia antas å tilfredsstille de materielle kravene til informasjonssikkerhet, herunder kravet til «forsvarlig sikkerhetsnivå» etter virksomhetssikkerhetsforskriften § 49 første ledd. Det mangler imidlertid formell godkjenning etter beskyttelsesinstruksen § 12, jf. virksomhetssikkerhetsforskriften §§ 50 og 51. Sistnevnte forskrift § 50 annet ledd krever at «informasjonssystemer som skal behandle sikkerhetsgradert informasjon, er godkjent før de tas i bruk». Gradering etter beskyttelsesinstruksen innebærer ikke at opplysningene er «sikkerhetsgradert», men etter beskyttelsesinstruksen § 12 annet ledd skal «[d]okumenter gradert etter instruksen ... følge reglene for dokumenter gradert BEGRENSET». Dette må antagelig innebære at også kravet om godkjenning før systemet tas i bruk, gjelder tilsvarende. Etter det riksadvokaten forstår, har Politidirektoratet godkjenningsmyndighet, jf. virksomhetssikkerhetsforskriften § 51 annet ledd.

Ettersom Indicia ikke fullt ut er i tråd med kravene etter beskyttelsesinstruksen § 12, forutsettes det at opplysninger fra KK mv. ikke registreres i Indicia før opplysningene eventuelt er nedgradert etter beskyttelsesinstruksen § 5. Samtidig er riksadvokaten klar over at det i praksis er et behov for å benytte Indicia også forut for nedgradering, og en vil følge dette nærmere opp i dialog med Politidirektoratet.

Avslutningsvis understrekes det at det hører under *politimesterens ansvar* å sørge for at opplysninger som innhentes ved KK, RA og DA behandles i tråd med gjeldende regelverk, herunder at opplysninger blir sperret når de ikke lenger skal oppbevares etter reglene i politiregisterloven § 50 tredje ledd, se blant annet kommunikasjonskontrollforskriften § 9 siste ledd. Det forutsettes at politimesteren organiserer virksomheten på en slik måte at påtalemyndigheten i politiet kan øve effektiv kontroll med behandlingen av opplysninger som stammer fra KK, RA og DA, herunder uavhengig av om opplysninger overføres fra innhentingssaken til andre formål.

Dette brevet inneholder ikke gradert informasjon og sendes derfor som ordinær post.

Kopi sendes de øvrige statsadvokatembetene samt til politidistriktene og særorganene, Politidirektoratet og Kontrollutvalget for kommunikasjonskontroll, til orientering.

Runar Torgersen
førstestatsadvokat

Esben Kyhring
førstestatsadvokat

Dokumentet er elektronisk godkjent og har derfor ingen signatur

Gjenpart

Agder politidistrikt

Agder

statsadvokatembeter

Det nasjonale

statsadvokatembetet

Finnmark politidistrikt

Hedmark og Oppland

statsadvokatembeter

Hordaland, Sogn og

Fjordane

statsadvokatembeter

Innlandet politidistrikt

Kontrollutvalget for

kommunikasjonskontroll

Kripos

Møre og Romsdal

politidistrikt

Møre og Romsdal

statsadvokatembeter

Nordland politidistrikt

Nordland

statsadvokatembeter

Oslo politidistrikt

Oslo statsadvokatembeter

Politidirektoratet

Politiets sikkerhetstjeneste

Rogaland

statsadvokatembeter

Sør-Vest politidistrikt

Sør-Øst politidistrikt

Troms politidistrikt

Trøndelag politidistrikt

Trøndelag

statsadvokatembeter

Vest politidistrikt

Vestfold, Telemark og

Buskerud

statsadvokatembeter

Økokrim

Øst politidistrikt

Mottakere

Troms og Finnmark
statsadvokatembeter

KOP1



Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:
24/269754-5

Vår referanse:
24/283281 - 5

Sted, dato:
Ski, 10.01.2025

Svar på høring - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv

Det vises til brev 6. desember 2024, med oversendelse av Justis- og beredskapsdepartementets høringsbrev av 20. november 2024 med vedlegg. PODs frist for uttalelse, 8. januar d.å., er etter avtale utsatt til 10. d.s.

Øst politidistrikt støtter vurderingen i høringsbrevet av politiets behov for å kunne benytte reelle data til utvikling og test av teknologiske løsninger. Vi er videre enige i at det bør gis klare hjemler for behandling av opplysninger til slike formål, både for å sikre politiets behov for teknologisk utvikling, og for å gi klare rammer i forhold til de registrertes rettigheter.

Distriktet støtter i all hovedsak forslagene til lov- og forskriftsendringer i høringsbrevet.

Endringer i politiregisterloven

Forslaget til endringer i politiregisterloven er etter vår vurdering hensiktsmessige og fornuftige.

Vi slutter oss til forlaget om forhåndsdrøfting med Datatilsynet ved testing og utvikling som kan medføre høy risiko for de registrertes rettigheter og friheter. Distriktets fagmiljø i innenfor kommunikasjonskontroll mv., mener imidlertid at det er lite hensiktsmessig å ha et særskilt krav om forhåndsdrøftelser med Datatilsynet ved bruk av opplysninger fra skjulte tvangsmidler til testing og utvikling, og støtter derfor ikke foreslått endring i Politiregisterforskriften §§ 41-2 og 41-3. Det foreslås ev. vurdert om det i stedet bør innhentes godkjenning fra høyere påtalemyndighet før slike opplysninger tas i bruk til testing/utvikling. Det kan videre vurderes om bruk av data fra skjulte tvangsmidler til test/utvikling bør protokollføres og innrapporteres særskilt til riksadvokaten, på tilsvarende måte som ved bruk av kommunikasjonskontroll, romavlytting og dataavlesing.

Med virkning fra 1. mars 2024 delegerte politidistriktene det daglige ansvaret for å oppfylle plikter knyttet til behandlingsansvaret for nasjonale, elektroniske straffesaksløsninger til Kripos. Beslutninger om bruk av opplysninger fra nasjonale straffesaksløsninger til IT-utvikling, herunder til test, utvikling og maskinlæring er omfattet av delegasjonen. Vi legger derfor til grunn at politidistriktene ikke vil ha ansvar for de beslutninger som er lagt til behandlingsansvarlig etter de foreslåtte bestemmelsene om bruk av opplysninger til test og utvikling i politiregisterloven.

PSTs behandling av åpen informasjon

Distriktet har ikke bemerkninger til forskriftsregulering av PSTs behandling av åpent tilgjengelig informasjon.

Endringer i grenseloven

Distriktet støtter foreslåtte endringer i grenseloven, og ingen bemerkninger til selve lovteksten.

Det fremgår imidlertid i høringsnotatet pkt. 2.9.3.2 siste avsnitt at:

"... opplysningene ifølge Politidirektoratet [skal] behandles i en aidentifisert form, det vil si at alfanumeriske opplysninger (som navn) fjernes slik at personen ikke er direkte identifiserbar."

Personopplysningloven og GDPR kommer ikke til anvendelse på anonymiserte opplysninger. Opplysningene (ansiktsfoto og fingeravtrykk) vil etter vårt syn fortsatt være å anse som personopplysninger selv om opplysningene ikke er knyttet til navn eller fødselsnummer. Personer som registreres vil med rimelige midler kunne identifiseres, i alle fall i de tilfeller vedkommende tidligere er registrert hos politiet. Det vises til fortalen i personvernforordningen pkt. 26 hvor det framgår:

"Personopplysninger som er blitt pseudonymisert, og som kan knyttes til en fysisk person ved hjelp av tilleggsopplysninger, bør anses som opplysninger om en identifiserbar fysisk person."

Vi legger derfor til grunn at de som legges inn i databasen med foto og fingeravtrykk, vil ha krav på svar om hvorvidt de er registrert, hvilke opplysninger som er registrert og hvilke handlinger som er foretatt, etter reglene i GDPR art. 15. Velges "aidentifisert" lagring av data, bør det etter vårt syn sikres tekniske løsninger for å gjenopprette koblingen mellom foto/fingeravtrykk og navn i tilfeller der innsynsbegjæring mottas, slik at de registrertes rettigheter til innsyn mm. etter GDPR kan etterleves på en praktisk og effektiv måte.

Med hilsen

Mona Elin Hertenberg

Politiinspektør

Dokumentet er elektronisk godkjent uten signatur.

Kopi:

Elisabeth Grytten

Hilde Oline Olsen

Per Helge Skjoldager

Kvendseth



Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:
24/269754-5

Vår referanse:
24/282684 - 3

Sted, dato:
Oslo, 09.01.2025

Høring - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv Innspill fra Politiets utlendingsenhet

Innledning

Politiets utlendingsenhet viser til brev av 06.12.24 fra POD med vedlagt høringsnotat fra Justis- og beredskapsdepartementet datert 20.11.24. Frist for å komme med innspill ble satt til 08.01.25. PU var 02.01.25 i kontakt med Politirektoratet og fikk utsatt frist til 10.01.25.

Høringen gjelder lovfesting av bruk av opplysninger til testing og utvikling av informasjonssystemer innenfor politiregisterlovens og grenselovens virkeområde. Det er foreslått endringer i politiregisterlov og forskrift, grenseloven, politiloven og straffeprosessloven. Svarfristen til POD er satt til 08.01.25.

Vi støtter departementets forslag. Det er viktig at politiets adgang til å benytte reelle data til testing og utvikling lovreguleres. En lovregulering vil også føre til en styrking av de registrertes rettigheter. Forslaget innebærer ikke noen endring av gjeldende utgangspunkt i politiet om at testing mv. primært skal skje med bruk av syntetiske data.

PU har bemerkninger til utvalgte punkter i høringsnotatet, og innspillene følger samme struktur som høringsnotatet. Innledningsvis redegjør vi kort for dagens praksis ved testing i UTSYS. Vi har ingen innspill til de deler av høringen som gjelder PSTs behandling av åpent tilgjengelig informasjon.

.

Politidirektoratet har forelagt høringen for [Fyll inn underliggende enheter]. [Dersom POD har sendt en bestilling til underliggende enheter og særlig bedt om innspill, bør det fremgå innledningsvis hva POD har bedt om innspill på].

Dagens praksis ved testing i Politiets utlendingsregister (UTSYS)

PU har i medhold av politiregisterforskriften § 56-3 behandlingsansvar for UTSYS. Testing er i den nasjonale instruksen for UTSYS regulert på samme måte som for de andre sentrale politisystemene. I instruksens punkt 11.4 sies følgende:

Som utgangspunkt skal utvikling, test og opplæring skje ved bruk av anonyme opplysninger. Med anonyme opplysninger menes både anonymiserte, avidentifiserte og fiktive opplysninger. Der det ikke er mulig eller hensiktsmessig å bruke anonyme opplysninger kan det være nødvendig å benytte produksjonsdata for å få gjennomført tilfredsstillende utvikling og testing i et system, samt opplæring. Slik bruk av produksjonsdata skal vurderes konkret for de tilfeller der det anses nødvendig, og i samråd med behandlingsansvarlig.

I praksis er dagens ordning at PU ved testing i UTSYS i utgangspunktet bruker reelle data eller opplysninger hentet fra registeret, men likevel slik at noen av dataene manipuleres. Dette skyldes for det første at UTSYS henter deler av opplysningene fra Utlendingsdatabasen (UDB) til UDI. Det er ikke mulig å teste med anonymiserte data fra UDB. Videre skyldes dette at fiktive opplysninger ikke på samme måte vil oppfylle formålet med testingen, herunder ikke gi et like godt grunnlag for testingen og den videre utviklingen av systemet. Testing med produksjonsdata blir alltid vurdert konkret i samråd med behandlingsansvarlig, og anonymiserte data benyttes der dette er mulig og hensiktsmessig.

Forholdet til utlendingsloven § 83 a, jf. punkt 2.3.2

Høringsnotatet omhandler ikke behandling av personopplysninger etter utlendingsloven. Utlendingsloven § 83 a regulerer utlendingsmyndighetenes adgang til å behandle opplysninger for å utøve myndighet eller andre oppgaver etter utlendingsloven. Utlendingsforskriftens § 17-7 a gir nærmere regler for hvilke formål personopplysninger kan behandles for. Ettersom utlendingslov og forskriftens bestemmelser er nært beslektet med det som reguleres i høringsforslaget, jf. spesielt redegjørelsen for grenselovgivningen i punkt 2.9, er det naturlig med en tilsvarende endring av utlendingsloven § 83 a og utlendingsforskriftens § 17-7a. Særlig siden departementet i punkt 2.3.2 vurderer at testing mv. i en GDPR-kontekst ofte vil være å anse som et uforenelig formål. Vi foreslår at det benyttes samme tilnærming som i forslag til politiregisterlov, politiforskrift og grenselov.

Vi gjør oppmerksom på at det nå foregår en omfattende utvikling av nye datasystemer for utlendingsforvaltningen.

Ad. 2.6.2 - nærmere om behovet

Vi slutter oss til departementets vurdering av behovet for testing og utvikling med reelle opplysninger. Selv om utgangspunktet skal være testing på syntetiske data vil det, som departementet redegjør for, i mange sammenhenger være nødvendig å bruke reelle opplysninger.

Ad. 2.6.3 - forslag til endringer

Vi er enig med departementet bruk av opplysninger av testing mv. bør reguleres eksplisitt fremfor at dette innfortolkes til å være omfattet av politiregisterloven. Sistnevnte kan utledes av EU-kilder. Dette betyr uansett av testing i seg selv er å anse som et politimessig formål. Vi antar at også opplysninger som både har et politimessig formål og et forvaltningsmessig formål, jf. politiregisterforskriften § 1-3 nr. 3, omfattes av det som sies i punkt 2.6.3.1.

PU slutter seg til de foreslåtte bestemmelsene i politiregisterloven § 3 og forskriftens § 1-5, og har ikke noen innspill til vurderingene av disse i punkt 2.6.3.2 og 2.6.3.3.

Ad 2.6.3.5 – hvilke opplysninger som kan brukes

PU er enig i at særlige kategorier personopplysninger må kunne brukes til testing og utvikling. Vi viser særlig til at det som oftest ikke vil være mulig å skille ut disse opplysningskategoriene.

Departementet har i høringsnotatet bedt om høringsinstansenes syn på testing med bruk av reelle opplysninger fra Informantregisteret. Vi er skeptiske til en slik løsning, og er enig med departementet at det vil være betenkelig å åpne for bruk av reelle data. Kripos som behandlingsansvarlig vil kunne redegjøre for de nærmere risikoene ved dette. Det bemerkes likevel at opplysningene i registeret vil være å anse som strengt fortrolig. Det vil kunne få svært uheldige konsekvenser, blant annet for informanternes sikkerhet om reelle opplysninger brukes til testing og utvikling.

Ad punkt 2.6.3.6 – særlig om opplysninger fra digitale beslag

PU deler departementets syn om at opplysninger fra speilkopier ikke skal brukes til testing. Det vises til at speilkopier fra elektroniske enheter inneholder store mengder data og ofte vet man ikke hva som finnes av opplysninger før en nærmere gjennomgang. Dessuten kan det være tilfelle at en slik bruk vil føre til mer administrasjon enn nytte, dersom en først må gjennomgå materiale og sile ut de viktigste opplysningene for en testing.

Ad punkt 2.6.3.7 – sletting i test og utviklingsmiljøer

PU har forståelse for departementets forslag om at opplysninger som behandles i egne utviklings- og testmiljøer må slettes når de slettes i det systemet de opprinnelig er hentet fra. Vi ser imidlertid at dette kan by på utfordringer i praksis. Dette kan for eksempel gjelde om testing og utvikling av en endret funksjonalitet er i en slutfase når store deler av den kopien som benyttes må slettes på grunn av slettefrist i det underliggende systemet. Det er derfor viktig at slettefrister hensyntas allerede når testdata hentes ut. Alternativt kan det foreslås til departementet at det bør være adgang til å slutføre testingen før kopien slettes i tråd med slettingen av de underliggende opplysningene.

Ad punkt 2.9 – regulering av testing og utvikling i grenselovgivningen

PU støtter forslaget om en særskilt hjemmel i grenseloven § 22a for testing og utvikling av informasjonssystemer for grenseformål. Departementet redegjør etter vår vurdering godt for de ulike sider av dette i punkt 2.9. Det virker også fornuftig at det åpnes for at foto og fingeravtrykk kan lagres utover den underliggende reguleringen.

Med vennlig hilsen

Jon Andreas Johansen
Politiinspektør

Zubia A. Kiani
Politiadvokat

Dokumentet er elektronisk godkjent uten signatur.

Kopi:

Gunnvor Hovde



Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:
24/269754-5

Vår referanse:
24/282564 - 4

Sted, dato:
Oslo, 17.01.2025

Høring - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv Frist 08012025

Innledning

Politiets IT-enhet (PIT) viser til brev fra Justis- og beredskapsdepartementet av 20. november 2024 om høring av endringer i politiregisterloven og grenseloven mv, samt brev fra Politidirektoratet av 6. desember 2024.

PIT har forelagt høringen for, og mottatt innspill fra, de interne team og grupperinger som arbeider med:

- Testdata
- Informasjonsforvaltning
- Etterlevelse
- Utvikling og KI

Foreslåtte regler om bruk av opplysninger til test og utvikling av informasjonssystemer innenfor politiregisterlovens virkeområde vil ha stor betydning for hvordan PIT samhandler med, og agerer på krav knyttet til behandling av personopplysningene stilt av, behandlingsansvarlig.

PIT ønsker forslagene velkomne. Et regelverk vil klargjøre rettstilstanden på et stadig viktigere område både for politiets digitalisering og for digitalt politiarbeid. Bruk av identifiserbare opplysninger i test og utvikling vil bidra til kvaliteten i løsninger av stor betydning for kriminalitetsbekjempelsen og politiets øvrige oppgaveløsning.

For PIT er fart og opprettholdelse av kontinuitet i utviklingsarbeidet viktig. Det er derfor viktig at de nye forslagene ikke legger opp til et omstendelig godkjenningsregime som krever individuell og uforutsigbar behandling i hvert enkelt tilfelle. PIT oppfatter de nye forslagene til å tilrettelegge for en strukturert og forutsigbar godkjenningsprosess, og vil

jobbe tett med behandlingsansvarlige for å få på plass et regime som tilfredsstiller de gitte krav. PIT anerkjenner at forslagene vil innebære en rekke krav til etterlevelse og helhetlig informasjonsforvaltning som må implementeres i politiets IT-løsninger.

PIT stiller seg bak de faktiske beskrivelsene i høringsnotatet av politiets virksomhet, utviklingsarbeid og behov. Som departementet peker på vil bestemmelsene omfatte en rekke forskjellige typetilfeller av test og utvikling, hvor ulike hensyn gjør seg gjeldende med varierende styrke. Departementet avgrenser virkeområdet for bestemmelsene mot innmelding og korrigering av feil i programvaren. PIT støtter dette.

Videre ønsker PIT å påpeke at politiet utvikler og tester en rekke løsninger som samvirker med systemer fra samarbeidende etater. Integrasjoner på tvers av sektorer og organisatoriske skillelinjer blir stadig mer aktuelt. Det er da viktig at hjemlene for test- og utvikling som gjelder for de ulike aktørene er, om ikke like, så kompatible. Vi oppfatter at de foreslåtte hjemlene følger samme mønster som tilsvarende hjemler gitt andre etater, og støtter dette.

Slik PIT ser det, vil de nye forslagene føre til:

- En enhetlig og mer konsistent håndtering av regelverket
- Tydeligere krav til økt produksjon, bruk og styring av testdata
- Økte krav til sporing og analyse knyttet til bruk av personopplysninger i test og utvikling

Tilfredsstillende håndtering av disse økte kravene vil ha en administrativ og økonomisk konsekvens for PIT, da PIT vil være utførende aktør i mange tilfeller. Det er vanskelig å si noe om omfanget av økte administrative og økonomiske konsekvenser, men PIT vil påpeke at endringene uansett ønskes velkommen og at fler av PITs pågående initiativ støtter opp under et mer systematisk etterlevelseregime knyttet til bruk av data.

Med hilsen

Lene Cecilie Høydahl

Avdelingsdirektør

Dokumentet er elektronisk godkjent uten signatur.

Kopi:

Gunnvor Hovde

Hege Lise Glent

Ragnhild Sandberg