

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Deres referanse
24/7353 - NNO

Vår referanse
24/04795-2

Dato
24.01.2025

Høringssvar - endringer i politiregisterloven og grenseloven mv.

Datatilsynet viser til Justis- og beredskapsdepartementets Høring - endringer i politiregisterloven og grenseloven mv - testing og utvikling og PSTs behandling av åpent tilgjengelig informasjon mv., med forlenget frist til 24.01.2025.

Om forslaget

Forslaget omfatter endringer i politiregisterloven, politiloven, straffeprosessloven, grenseloven og politiregisterforskriften.

Endringsforslagene gjelder i hovedsak regulering av bruk av opplysninger til testing og utvikling av informasjonssystemer innenfor politiregisterlovens og grenselovens virkeområde.

Oppsummering av Datatilsynets innspill

Datatilsynet er positive til forslaget om lovregulering, men har enkelte prinsipielle bemerkninger:

- De registrertes rettigheter må sikres gjennom størst mulig grad av åpenhet
- Det er uklart om behandling av personopplysninger til test- og utviklingsformål innenfor forslaget reguleres av personopplysningsloven eller politiregisterloven
- Det må innføres tilstrekkelige kontrollmekanismer ved bruk av personopplysninger, særlig ved bruk av data fra skjulte metoder
- Datatilsynets tilsynskompetanse må være i tråd med personvernforordningen og LED

Overordnet om bruk av data for utvikling av kunstig intelligens og maskinlæring

Forslagene i høringsnotatet åpner for større bruk og innsamling av data til å utvikle og teste informasjonssystemer. Datatilsynet mener det er viktig å vurdere forslagene opp mot mulighetene som åpnes for utvikling av kunstig intelligens og maskinlæring.

Det er et uttalt politisk mål at offentlige virksomheter skal ta i bruk kunstig intelligens. Denne teknologien medfører en risiko for potensielt store inngrep i den enkeltes personvern.

Borgernes tillit til bruken av den nye teknologien er avhengig av at personvernet ivaretas. Det er særskilte utfordringer ved inngripende og skjult bruk av ny teknologi fra myndighetenes side.

Datatilsynet mener det er viktig å ha en prinsipiell tilnærming til forslagene, da de kan ha store konsekvenser for samfunnet. De generelle personvernprinsippene er formulert i personvernforordningen art. 5 hvor det blant annet fremgår at personopplysninger skal behandles på en lovlig, rettferdig og åpen måte. I tillegg vil prinsippet om dataminering være relevant i tilknytning til forslagene.

I [Nasjonal strategi for kunstig intelligens](#) er det uttalt at et viktig hensyn og etisk prinsipp er at KI-baserte løsninger skal respektere menneskets selvbestemmelse og kontroll. Dette omfatter kontroll over egne personopplysninger.

Ved utvikling av kunstig intelligens vil særlig informasjonsrettferdighet være sentralt. Informasjonsrettferdighet innebærer at den registrerte skal ha tilstrekkelige informasjon til kunne forstå hvilke opplysninger om vedkommende som behandles og hvordan dette skjer.

I fortalepunkt 60 til personvernforordningen er dette omtalt:

«Prinsippene om rettferdig og åpen behandling krever at den registrerte informeres om at behandlingen skjer, samt om formålet med den. Den behandlingsansvarlige bør gi den registrerte eventuell ytterligere informasjon som er nødvendig for å sikre en rettferdig og åpen behandling, idet det tas hensyn til de særlige omstendighetene rundt behandlingen av personopplysningene og sammenhengen den skjer i. Den registrerte bør dessuten informeres om forekomsten av profilering og konsekvensene av dette»

Personvernkommisjonen har i [NOU 2022: 11 Ditt personvern – vårt felles ansvar — Tid for en personvernpolitikk](#) lagt vekt på følgende:

«Personvernkommisjonen mener det er avgjørende med åpenhet og muligheter for kontroll ved anskaffelser i justissektoren. Ved anskaffelse av potensielt inngripende verktøy må personvern vurderinger være en sentral del av beslutningsgrunnlaget.

Personvernkommisjonen mener det bør tas spesielt hensyn til etterprøvnbarhet og ivaretagelse av den enkeltes rettigheter ved bruk av maskinlæringssystemer i justissektoren. For at slike metoder skal kunne tas i bruk i Norge, må de også være forklarbare for den som anvender teknologien, og risikovurderinger og pålagt teknisk dokumentasjon må foreligge i tråd med forslaget om forordning for kunstig intelligens.»

Alle de foreslåtte endringene utfordrer de generelle personvernprinsippene ved at opplysningene ikke er frivillig avgitt og ved at de registrerte ikke nødvendigvis vil få informasjon om innhenting og bruk av opplysningene.

Det er også problematisk at det åpnes for å utvikle verktøy uten at det nødvendigvis finnes lovhjemmel for å bruke verktøyene. Bruk av verktøy basert på kunstig intelligens i justissektoren kan potensielt innebære svært inngripende behandling og legalitetsprinsippet må derfor anvendes strengt på dette området.

Det er utfordrende at politiregisterloven, slik loven er utformet i dag, er lite egnet til å regulere bruk av kunstig intelligens i justissektoren. Deler av politidirektivet som kunne avhjulpet situasjonen er ikke gjennomført i norsk rett.

Regulering av test og utvikling av kunstig intelligens

Personvernforordningen er inkorporert i norsk rett gjennom personopplysningsloven, hvilket betyr at forordningen skal gjelde som norsk rett. Hovedregelen er at all behandling av personopplysninger er regulert av personopplysningsloven, med mindre personvernforordningen selv gjør unntak fra dens virkeområde. Personopplysningsloven § 2 regulerer lovens saklige virkeområde og angir at personvernforordningen i tilfelle konflikt går foran bestemmelser i annen lov som regulerer samme forhold, jf. EØS-loven § 2.

Politiets behandling av personopplysninger er i hovedsak regulert av politiregisterloven, som implementerer politidirektivet (LED), supplert av politiregisterforskriften. Personvernforordningens regler gjelder ikke på området som dekkes av politidirektivet jf. personvernforordningens artikkel 2 nr. 2 bokstav d og politidirektivet artikkel 1 nr. 1.

I vurderingen av hvilket av regelverkene som kommer til anvendelse, er det naturlig å ta utgangspunkt i unntaket fra personvernforordningens virkeområde i dens artikkel 2 nr. 2 bokstav d. Unntaket angir at forordningen ikke får anvendelse på politiets behandling av personopplysninger som utføres:

«(...) med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, herunder vern mot og forebygging av trusler mot den offentlige sikkerhet».

Dersom politiet behandler personopplysninger til andre formål enn disse, reguleres behandlingen av personvernforordningen. Det er *formålet* med behandlingen som bestemmer hvilket regelverk som kommer til anvendelse.

Utvikling av verktøy basert på kunstig intelligens vil kunne hjelpe politiet med å utføre sitt samfunnsoppdrag, og dermed bedre kunne utnytte sine ressurser til blant annet kriminalitetsbekjempelse. Samtidig er unntakene som opplistet i personvernforordningen artikkel 2 nr. 2 bokstav d, etter sin ordlyd, rettet mot mer tradisjonelle og utpregede «politioppgaver». EU-domstolen har også uttalt at unntaket i artikkel 2 nr. 2 bokstav d i personvernforordningen skal tolkes «strengt».

Slik Datatilsynet vurderer det, retter unntakene i forordningen artikkel 2 nr. 2 bokstav d seg mot politiets kriminalitetsbekjempende virksomhet. I og med at unntakene skal tolkes strengt, er det vanskelig å innfortolke *utvikling* av verktøy basert på kunstig intelligens i disse

unntakene. Denne forståelsen har også støtte i politiregisterlovens definisjon av «politimessige formål» jf. § 2 nr. 13, som omfatter politiets kriminalitetsbekjempende virksomhet, herunder etterforskning, forebyggende arbeid og ordenstjeneste, og politiets service- og bistandsfunksjon samt føring av vaktjournaler. Heller ikke denne definisjonen omfatter teknologiutvikling som sådan, selv om formålet er å utvikle verktøy som skal benyttes i kriminalitetsbekjempelsen.

Etter Datatilsynets syn vil derfor bruk av personopplysninger til utvikling av kunstig intelligens i politisektoren i alminnelighet kunne reguleres av personvernforordningen.

Dette synspunktet kan imidlertid nyanseres noe. Det er få kilder på området, men i artikkelen [Between GDPR and Law Enforcement Directive in Security Research: The Use of Personal Data by Law Enforcement Authorities](#), publisert i European Journal of Law and Technology, Vol. 15No. 3(2024) argumenteres det at forskning og utvikling i noen tilfeller kan falle inn under begrepet «forebygging».

Det tar utgangspunkt i fortalepunkt 27:

«For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected»

Vi støtter departementets syn om at det må vurderes konkret hvilket regelverk som får anvendelse for hver behandling. Vi ser at dette kan by på vanskelige gresdragninger, men det vil være et sentralt moment å vurdere formålet med behandlingen av de aktuelle opplysningene og om det er nødvendig gjøre behandlingen under virkeområdet til politiregisterloven.

Hvilket regelverk som gjelder for utviklingen av kunstig intelligens har betydning for den registrertes stilling og rettigheter.

Forordningen gir et sterkere vern for den registrertes rettigheter enn politiregisterloven. I henhold til alminnelige personvernprinsipper er informasjon og innsyn sentrale rettigheter for den registrerte, nedfelt i forordningen artikkel 13, 14 og 15. De nevnte rettighetene står ikke like sterkt når personopplysninger behandles i kriminalitetsbekjempelsen, på grunn av de spesielle hensynene som gjør seg gjeldende på området. Det er derfor av stor betydning å fastslå hvilket regelverk som kommer til anvendelse på disse behandlingsformålene.

Problemstillingen er belyst i vår Sandkasserapport i PrevBOT-prosjektet, som ble gjennomført i samarbeid med Politihøgskolen. I dette prosjektet bestod datagrunnlaget av chatlogger hvor det foregikk såkalt grooming. Datagrunnlaget inneholdt opplysninger om både den straffedømte og offer. Datatilsynets synspunkt var at ofre spesielt bør ivaretas når det gjelder kontroll over egne personopplysninger og hva de brukes til.

Det sentrale for Datatilsynet er at de registrertes rettigheter ivaretas. Det bør ikke gjøres større unntak fra rett til informasjon og innsyn enn nødvendig, ettersom den registrerte ikke blir satt i stand til å kunne ivareta sine rettigheter.

Datatilsynet mener derfor at det bør vurderes konkret i hvert enkelt prosjekt eller behandling om det er nødvendig å unnta behandlingen fra de registrertes rettigheter og i hvilken grad åpenhet skal praktiseres. Det vil i mange tilfeller være uproblematisk å gi de registrerte underretning og innsyn i bruken av egne personopplysninger.

Selv om det i mange tilfeller er andre hensyn som må vektlegges, for eksempel ved bruk av opplysninger fra skjulte metoder, bør det som et utgangspunkt tilstrebes størst mulig åpenhet om utvikling og bruk av KI i politiet.

Datatilsynet ber derfor spesielt om at det tas stilling til hvilket regelverk som regulerer test og utvikling i det videre lovarbeidet.

Bruk av informasjon fra skjulte tvangsmidler til test og utvikling

Datatilsynet har enkelte prinsipielle innvendinger mot bruk av informasjon fra skjulte tvangsmidler til test og utvikling.

Forslagene i høringsnotatet begrunnes i behovet for å ha verktøy som kan bidra til enklere oversikt, sammenstilling og oversettelse, samt å finne relevante bevis. Slike verktøy kan bidra til å redusere den manuelle gjennomgangen av opplysninger, noe som kan være positivt i et personvernsperspektiv.

Det er pekt på behov for verktøy som kan transkribere, oversette og lage sammendrag av materiale fra kommunikasjonsskontroll. Dette er verktøy som kan betraktes som ganske grunnleggende bruk av KI. Det vil også være mulig å lage systemer som kan gjenkjenne biometriske kjennetegn, som utseende, stemme eller talemåte.

Det er viktig for Datatilsynet å understreke dette hele tiden må vurderes opp mot profilering som tiltak, som politiregisterloven ikke omfatter, på grunn av manglende implementering av LED art. 11.

Datatilsynet ser at det i mange tilfeller åpenbart er nødvendig å unnta behandling av personopplysninger fra denne typen kilder fra retten til innsyn og informasjon.

Hvorvidt denne bruken av personopplysninger er akseptabel, vil avhenge av hvilke kontrollmekanismer som innføres. Selve innhenting av informasjon vil være regulert av domstolene, og kontrollen underlagt Datatilsynet og KK-utvalget. KK-utvalget vil føre kontroll med bruk.

Datatilsynet støtter endringen i politiregisterforskriften § 41-2 annet ledd hvor kravet om forhåndsdrøftelser ved testing og utvikling av informasjonssystemer også skal gjelde dersom det skal behandles opplysninger som er innhentet ved kommunikasjonsskontroll,

dataavlesning og romavlytting, med unntak av opplysninger som behandles av Politiets sikkerhetstjeneste.

Datatilsynet mener klart at kravet i § 41-1 om vurdering av personvernkonsekvenser alltid vil gjelde ved bruk av opplysninger fra skjulte tvangsmidler til test og utvikling.

For ordens skyld, nevner vi at denne plikten også følger av art. 35 i personvernforordningen, hvor det pekes på at det er særlig nødvendig gjennomføre en vurdering av personvernkonsekvenser ved behandling i stor skala av personopplysninger om straffedømmer og lovovertrедelser som nevnt i artikkel 10.

Datatilsynet anbefaler at departementet vurderer om det skal gjøres endringer i personopplysningsloven § 16, som regulerer unntak fra de registrertes rettigheter av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger til å også omfatte slike behandlinger som er omfattet av forslaget.

Forhåndsdrøftelser og meldeplikt til Datatilsynet

I høringsnotatet drøftes det om det skal innføres en meldeplikt til Datatilsynet ved testing og utvikling som ikke medfører så høy risiko at det vil være nødvendig å gjennomføre forhåndsdrøftinger.

Datatilsynet har tidligere i møte med departementet ytret ønske om å i større grad kunne ha oversikt over den samlede bruken av kunstig intelligens i politiet, særlig med tanke på at behandlingen som regel ikke vil være kjent for offentligheten. Tilsynet skisserte som en mulighet å etablere en meldeplikt til Datatilsynet om testing og utvikling, særlig av systemer som bruker kunstig intelligens.

Departementet peker i høringsnotatet at det kan være vanskelig å avgrense hva som er meldepliktig, og ber særlig om høringsinstansenes syn på om en slik ordning bør etableres og hvordan den i tilfelle kan innrettes.

Datatilsynet ser at det kan være utfordrende å etablere en meldeplikt gjennom forskrift, særlig med tanke på fremtidig teknologiutvikling. I stor grad vil behovet for en meldeplikt utover kravet til forhåndsdrøftelser være unødvendig, dersom LED art. 28 nr. 3 gjennomføres lojalt i norsk rett.

Denne bestemmelsen gir tilsynsmyndigheten kompetanse til å utforme en liste over behandlingsaktiviteter som skal være gjenstand for forhåndsdrøftinger. Dette vil være et godt og fleksibelt virkemiddel i tilsynsarbeidet.

Vi anbefaler at denne muligheten vurderes og eventuelt gjenspeiles i forslaget til ny politiregisterforskrift § 41-2.

I høringsnotatet er det lagt til grunn at innføring av KI for politioppgaver gir økt behov for forhåndsdrøftinger, jf. personvernforordningen artikkel 36. Dette vil føre til flere oppgaver for Datatilsynet. Det er derfor viktig at forslaget medfører tilføring av ressurser til tilsynet.

Datatilsynets tilsynskompetanse,

Datatilsynet har som oppgave å føre kontroll med behandling av personopplysninger etter både personvernforordningen og politiregisterloven.

Tilsyn og kontrollmekanismer vil være viktige virkemidler for å sikre de registrertes rettigheter, spesielt i tilfeller det er brukt opplysninger innhentet ved skjulte tvangsmidler. Forslaget inneholder begrensninger av Datatilsynets kompetanse som svekker muligheten for kontroll.

I forslag til § 41-3 første ledd siste punktum er Datatilsynets kompetanse begrenset til kun å kunne gi anmerkning og ikke andre virkemidler ved behandling som nevnt i § 41-2 annet ledd annet punktum, det vil si dersom vi finner at behandlingen ikke er i tråd med regelverket ved behandling av opplysninger som er innhentet ved kommunikasjonskontroll, dataavlesing og romavlytting.

Denne begrensningen er i strid med Datatilsynets kompetanse etter personvernforordningen og ivaretar heller ikke den kompetanse tilsynsorganet skal ha etter LED art. 28 nr. 5 jf. art. 47.

Vi legger til grunn at det i det videre arbeidet tas stilling til våre innspill knyttet til forslagens begrensning av Datatilsynets kompetanse.

Med vennlig hilsen

Jan Henrik Mjønes Nielsen
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer