



Justis- og beredskapsdepartementet  
Politiavdelingen  
Postboks 8005 Dep.  
0030 Oslo

Deres ref.:  
13/1108 - TKH

Dato: 27.03.2013

## **HØRINGSUTTALELSE: FORSLAG TIL ENDRINGER I PASSLOVEN OG PASSFORSKRIFTEN – UTVIDET ADGANG FOR POLITIET TIL Å BENYTTE OPPLYSNINGER FRA PASSREGISTERET**

Norsk forening for kriminalreform (KROM) viser til departementets høringsbrev av 20.02.13. Med dette ble forslag til endringer i passloven og passforskriften, med sikte på å gi politiet utvidet adgang til å benytte opplysninger fra passregisteret, sendt på høring.

Nedenfor følger KROMs merknader til forslaget.

### **1. Bakgrunn**

Etter gjeldende rett kan opplysninger fra passregisteret benyttes til utstedelse av pass, ved grensekontroll og i saker om innlevering og beslag av pass etter passloven § 7. Det fremgår av høringsnotatet at departementet legger til grunn at opplysningene videre kan anvendes ved etterforskning av forfalskning av pass, i saker om savnede personer, når vilkårene for utlevering og beslag etter straffeprosessloven kap. 16 er oppfylt, og ellers når den registrerte samtykker. Etter passloven § 8 er det passmyndigheten (politiet), Kripos og norsk grensekontrollmyndighet som har tilgang til passregisteret.

Ifølge passloven § 8 inneholder passregisteret opplysninger som ansiktsfoto, navn, signatur, fødselsnummer, høyde, øyenfarge, hårfarge, fødested og (utsendelses)adresse. I tillegg åpner passloven for at det også kan inntas «*opplysninger som er nødvendig for forvaltning av registeret og utstedelse av pass*». Ifølge departementet vil det særlig være aktuelt å innta opplysninger som begrunner hvorfor noen nektes pass (beslutning om passhindring, jf. passloven § 5). Beslutning om passhindring vil kunne ha bakgrunn i sinnslidelse, domfellelse og andre forhold av personlig karakter, altså personopplysninger som må kunne karakteriseres som sensitive i personopplysningslovens forstand (jf. personopplysningsloven § 2, nr. 8).



I foreliggende forslag foreslår departementet å åpne for at politiet skal kunne benytte opplysningene i passregisteret til flere formål enn det som følger av dagens regelverk. I tillegg til det som følger av dagens regelverk, foreslås det at opplysningene skal kunne anvendes

1. for å finne savnede personer og identifisere personer som politiet er lovpålagt å hjelpe,
2. for å identifisere personer som kan innbringes eller skal pågripes eller anbringes i politiarrest,
3. for å forebygge straffbare forhold som kan medføre fengsel i mer enn tre år og for å etterforske forhold som kan medføre fengsel i mer enn seks måneder,
4. for å kontrollere opplysninger som skal føres inn i det sentrale registeret over strafferettslige reaksjoner, og
5. for andre formål når den registrerte samtykker.

Det fremgår av høringsnotatet (s. 1) at bakgrunnen for forslaget er at «[d]et har vært praksis også tidligere at politiet – som i Norge er passmyndighet, jf. passloven § 2 – har benyttet opplysninger fra passregisteret til andre formål enn dem som kan knyttes til passloven. Denne praksis, som har vært basert på en forståelse av at informasjonen i registeret kunne benyttes generelt til politimessige formål, var imidlertid ikke fullt ut avstemt mot de begrensninger som følger av personopplysningsloven». KROM finner det derfor riktig å karakterisere forslaget som et forsøk på å hjemle en formålsutglidning.

## 2. Generelle merknader

Politiets bruk av opplysninger fra passregisteret har også tidligere blitt kritisert. I Datatilsynets årsmelding for 2012<sup>1</sup> går det frem at Politidirektoratet i lang tid har utlevert opplysninger fra passregisteret til politiets etterforskning, typisk fotografier i forbindelse med automatisk trafikk kontroll. Tilsynet skriver at de ved flere anledninger har kritisert etaten for å ha utlevert opplysningene uten å ha forsikret seg om at straffeprosesslovens vilkår for utlevering var oppfylt. Datatilsynet valgte å følge opp praksisen i etaten, noe som endte med varsel om vedtak fra tilsynets side.

### 2.1 Proporsjonalitetsprinsippet

Datatilsynet fremhever at proporsjonalitetsprinsippet må stå sterkt ved vurdering av tiltak som potensielt kan krenke personvernet i justissektoren. «*Selv om formålet er godt skal man kunne diskutere om inngrepet som foretas overfor enkeltpersoner virkelig er tilstrekkelig hjemlet i lov, at det er proporsjonalt ut fra formålet, og at det er nødvendig i den konkrete situasjonen*»<sup>2</sup>. I personvernssammenheng består proporsjonalitetsprinsippet av tre kumulative krav: Behandlingen av personopplysninger må være *relevant* for å oppfylle det formål som søkes oppnådd, behandlingen må være *nødvendig* for å oppfylle formålet, og behandlingen må være *forholdsmessig* i forhold til formålet<sup>3</sup>.

<sup>1</sup> Datatilsynet. (2013). *Årsmeldingen for 2012. Manus til stortingsmeldingen om Datatilsynets virksomhet, jf. personopplysningsloven § 42*. Nedlastet fra <http://www.datatilsynet.no>

<sup>2</sup> Datatilsynet. (2012). *Strategi for godt personvern i justissektoren mv. Politi, påtalemyndighet, domstol og kriminalomsorg – offentlige kontrollmyndigheter og utlendingsforvaltningen*. Nedlastet fra <http://www.datatilsynet.no>. Side 8

<sup>3</sup> Schartum, D. W., & Bygrave, L. A. (2004). *Personvern i informasjonssamfunnet* (2. utg.). Bergen: Fagbokforlaget. Side 104





KROM kan ikke se at departementet i tilfredsstillende grad har godtgjort at de foreslåtte endringene er proporsjonale sett i forhold til de personverninngrep forslaget vil medføre. I sin drøfting av økonomiske og administrative konsekvenser av forslaget, fremhever departementet at «[m]uligheten antas å kunne bidra til effektivt arbeid i politiet. Gevinsten vil være mer indirekte enn at den kan konkretiseres i form av prognoser for flere oppklarte saker eller kortere saksbehandlingstid» (høringsnotatet, s. 18).

KROM anerkjenner at det ofte kan oppstå dilemmaer i skjæringspunktet mellom hensynet til personvern og hensynet til effektiv politivirksomhet. Dersom hensynet til effektivt politiarbeid skal veie tyngst, er vi av den klare oppfatning at det i det minste må kunne dokumenteres at personvernkretnende tiltak faktisk vil ha den tilsiktede effektiviserende virkning. I denne saken registrerer vi at departementet ikke engang ser seg i stand til å produsere en prognose for hvorvidt de foreslåtte endringene vil medføre flere oppklarte saker eller kortere saksbehandlingstid. Dermed finner KROM at hensynet til personvernet utvilsomt må veie tyngst i denne saken.

## **2.2 Formålsutglidning**

Et grunnkrav til behandling av personopplysninger er at opplysningene bare nyttes til uttrykkelig angitte formål og ikke senere brukes til formål som er uforenlige med det opprinnelige formålet (personopplysningsloven § 11, bokstav b og c). Dersom en behandlingsansvarlig vil benytte opplysninger til formål som ikke dekkes av den opprinnelige formålsangivelsen, foreligger det et vilkår om at det nye formålet oppfyller kravene til lovlig behandling etter personopplysningsloven § 8 (evt. også § 9 dersom behandlingen omfatter sensitive personopplysninger). At opplysningene allerede er samlet inn og foreligger i et register er intet selvstendig argument for å tillate den nye behandlingen<sup>4</sup>. I tillegg vil det være et vilkår om at det nye formålet ikke er uforenlig med det formål som opprinnelig lå til grunn for innsamlingen (finalitetsprinsippet). Dersom en behandlingsansvarlig samler inn opplysninger for å kunne gi de registrerte fordeler (f.eks. utstedelse av pass), men senere bruker opplysninger på en måte som er til ulempe for de registrerte (f.eks. politietterforskning), vil dette ikke være i samsvar med kravene til endret formål i personopplysningsloven § 11, bokstav c.

At personopplysninger kun skal benyttes til uttrykkelig angitte og legitime formål følger også av EUs personverndirektiv (direktiv 95/46/EF, art. 6) og Europarådets konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger (art. 5).

Bestemmelsen i personopplysningsloven § 11, bokstav b, innebærer at det er lovstridig å behandle personopplysninger uten at et formål er uttrykkelig fastlagt, og at det er forbudt å behandle personopplysningene utenfor et eller flere angitte formål<sup>5</sup>. Nytt formål vil også alltid kreve ny melding til Datatilsynet (personopplysningsloven § 31, tredje ledd), og unnlattelse av å sende melding er straffbart med bøter og/eller fengsel i inntil ett år (personopplysningsloven § 48).

Departementet medgir eksplisitt i høringsnotatet (s. 1) at «[d]et har vært praksis også tidligere at politiet (...) har benyttet opplysninger fra passregisteret til andre formål enn dem som kan knyttes til

<sup>4</sup> Ot.prp. nr. 92 (1998-99). Om lov om behandling av personopplysninger (personopplysningsloven)

<sup>5</sup> Schartum & Bygrave (2004, s. 167)



passloven», og at «denne praksis (...) var imidlertid ikke fullt ut avstemt mot de begrensninger som følger av personopplysningsloven». KROM kan ikke annet enn å konkludere med at det i denne saken foreligger en eksplisitt erkjennelse av lovstridig bruk av opplysningene i passregisteret, og at departementet nå foreslår å hjemle den lovstridige praksisen ved å endre passloven og passforskriften.

### 3. Spesielle merknader

#### 3.1 Tilgang til opplysningene i passregisteret

Det fremgår av høringsnotatet at politiet vil ha direkte søketilgang i passregisteret, men at det ikke er avklart hvem i politiet som skal ha slik direkte søketilgang. Det fremheves i notatet at spørsmålet om hvem som eventuelt skal ha direkte tilgang må bero på administrative vurderinger: «Etter § 8 a annet ledd vil det bero på interne instruksjoner om adgangen til å benytte opplysninger fra passregisteret skal realiseres gjennom direkte søketilgang til registeret eller anmodning om utlevering gjennom andre som har søketilgang» (høringsnotatet, s. 19).

KROM er kritiske til en situasjon der samtlige politiansatte får direkte søketilgang til opplysningene i passregisteret. Dersom forslagene blir vedtatt, er vi av den oppfatning at tilgang må begrenses til særskilt autorisert personell.

#### 3.2 Automatiserte søkeprosesser og biometrisk gjenkjenning

Ansiktsfotografiene i passregisteret har digitale egenskaper som gjør dem egnet til biometrisk ansiktsgjenkjenning. Biometriske teknikker gjør det, ved hjelp av digital teknologi for mønster- og ansiktsgjenkjenning, mulig å identifisere personer blant tusenvis av ansikter skannet fra et foto- eller videokamera. De mest avanserte systemene kan gjenkjenne 500-1000 ansikter pr. sekund i en menneskemengde, og systemene kan samtidig logge tid og sted for hvert individ<sup>6</sup>. Biometriske systemer kan samtidig kryssjekke og kombinere mange ulike databaser og registre, herunder passregisteret. Tilsvarende teknikker kan også benyttes opp mot fotografier fra f.eks. Facebook.

Departementet problematiserer muligheten til å gjennomføre automatiserte søkeprosesser i passregisteret og fremhever at dette i realiteten innebærer at hele befolkningen stilles til disposisjon for politiet uten at de registrerte har foretatt seg noe som tilsier at de bør inngå i mer enn nettopp passregisteret.

KROM finner det riktig å understreke at biometrisk identifikasjon synes å være særlig egnet for formålsutglidninger. Eksempelvis ble utlendingsregisteret (som inneholder biometrisk informasjon som fingeravtrykk) åpnet for politiet i etterforskningsøyemed, selv om det opprinnelige formålet med databasen var å bidra til å fastslå identiteten til asylsøkere (da registeret ble opprettet ble det eksplisitt poengtert at opplysningene ikke kunne anvendes i etterforskningsøyemed)<sup>7</sup>.

<sup>6</sup> NOU 2009: 1. Individ og integritet. Personvern i det digitale samfunnet.

<sup>7</sup> Hafskjold, C. (2011). *Personvern – teknologiske utfordringer*. Nedlastet fra <http://www.teknologiradet.no>





KROM mener at overvåkningspotensialet som ligger i biometrisk ansiktsgjenkjenning i ytterste konsekvens kan representere en trussel mot sentrale demokratiske prinsipper. Det er eksempelvis ikke vanskelig å tenke seg demokratiske komplikasjoner knyttet til at politiet i nær sanntid kan fastslå identiteten til samtlige som deltar i en lovlig politisk demonstrasjon. Stortingets menneskerettighetsutvalg fremhevet, i sin drøfting av hvorvidt Grunnloven bør utstyres med en egen bestemmelse om personvern, at «[e]nkeltindivider som lever i samfunn der de til stadighet opplever overvåkning og kontroll, kan bli mer tilbakeholdne med å fremsette ytringer eller på annen måte delta i det politiske liv. Tilsvarende vil lekkasje av personlige opplysninger fra forvaltning eller fra private kunne oppleves som vilkårlig saksbehandling, eller i verste fall som 'straff' for manglende lydighet. Slike ytterliggående brudd på privatlivets fred vil i realiteten utgjøre en trussel mot det norske demokratiet»<sup>8</sup>.

KROM finner det riktig å vise til at den svenske passloven (1978:302) § 6, bokstav b, inneholder et forbud mot automatiserte søkeprosesser begrunnet utfra personvern hensyn.

KROM er av den oppfatning at et forbud mot automatiske søkeprosesser må gjelde i forhold til passregisteret.

### **3.3 Merknader til enkelte av de foreslåtte utvidelsene**

Som det fremgår av ovennevnte, er KROM prinsipalt av den oppfatning at departementets forslag bør avvises, bl.a. som følge av at forslaget kan karakteriseres som forsøk på å hjemle en lovstridig formålsutglidning og som følge av at de foreslåtte endringene, etter vårt syn, ikke oppfyller proporsjonalitetskriteriene i et personvern perspektiv. Likevel finner vi det nødvendig å kommentere enkelte av de foreslåtte utvidelsene særskilt.

I forslaget til passloven ny § 8 a, første ledd, bokstav a, foreslås det at politiet kan anvende opplysninger fra passregisteret «i arbeid med å finne savnet person, og med å identifisere person som det hører under politiets oppgaver å hjelpe». Departementet fremhever i denne sammenheng at man i slike tilfeller må kunne legge til grunn en presumsjon om samtykke. KROM vil kort bemerke at personopplysningsloven § 2, nr. 7, presiserer at et samtykke må være frivillig, uttrykkelig og informert. At erklæringen om samtykke må være 'uttrykkelig' vil trolig innebære at det ikke er tilstrekkelig med et passivt eller stilltiende samtykke, og heller ikke samtykke gjennom konkludent adferd<sup>9</sup>. Dette vil også være av betydning med hensyn til bokstav e som angir at opplysninger fra passregisteret kan anvendes «når den som opplysningene gjelder, samtykker».

Bokstav c legger opp til at opplysninger fra passregisteret kan brukes «ved forebygging av forhold som etter loven kan medføre fengsel i tre år, og ved etterforskning av forhold som etter loven kan medføre høyere straff enn fengsel i seks måneder». Hva gjelder etterforskning, finner KROM det riktig å understreke at en nedre terskel på seks måneder i praksis vil åpne for bruk av opplysninger fra passregisteret i et betydelig antall saker, herunder mindre alvorlige forhold, eksempelvis brudd på vegtrafikkloven avdekket gjennom automatisk trafikk kontroll. Dette taler, etter KROMs syn, for at grensen bør heves betraktelig dersom forslaget vedtas. Tilsvarende er vi svært kritiske til at

<sup>8</sup> Dokument nr. 16 (2011-2012), pkt. 30.6.5

<sup>9</sup> NOU 1997: 19. Et bedre personvern. – forslag til lov om behandling av personopplysninger. Side 186



opplysninger fra passregisteret skal kunne benyttes i forebyggende øyemed med en nedre grense på tre års fengsel. Vi finner generelt ikke å kunne slutte oss til departementets påstand om at hensynet til å forebygge kriminalitet bør veie tyngre enn den enkeltes interesse i at passregisteret bare benyttes i samsvar med formålet med avgivelsen av opplysningene. KROM mener at politiet allerede, gjennom straffeprosessloven, er gitt svært omfattende virkemidler med hensyn til etterforskning og forebygging av kriminalitet

Med hilsen

Mikkel Haugerud

For styret i Norsk forening for kriminalreform (KROM)