

Politidirektoratet
Postboks 8051 Dep
0031 OSLO

Deres ref.

Vår ref. (bes oppgitt ved svar)
05/01363-3 /AÅr

5. januar 2006

OPPSUMMERING AV KONTROLL - VARSEL OM PÅLEGG

1. Bakgrunn

Datatilsynet gjennomførte 15. november 2005 tilsyn med Politidirektoratets behandling av personopplysninger i forbindelse med utstedelse og bruk av nye biometriske pass med RFID avlesningsmulighet og lagringsenhet. Tilsynet ble gjennomført i medhold av personopplysningsloven § 42 tredje ledd nr 3.

2. Foreløpig rapport

Datatilsynet har utarbeidet en foreløpig rapport fra tilsynet. Rapporten er vedlagt dette brev.

3. Varsel om vedtak

På bakgrunn av foreløpig rapport gir Datatilsynet med dette varsel om at det med hjemmel i personopplysningslovens § 46 vil fattes vedtak om følgende pålegg:

- a) Politidirektoratet må utarbeide en databehandleravtale med de databehandlerne Politidirektoratet benytter i forbindelse med pass, jf. personopplysningsloven § 15. Se foreløpig rapport punkt 5.4.
- b) Politidirektoratet må gjennomføre nødvendige risikovurderinger i henhold til personopplysningsloven § 13 og personopplysningsforskriften § 2-4. Se foreløpig rapport punkt 5.5 med underpunkter.
- c) Politidirektoratet må gi både passøkeren og passinnehaveren tilstrekkelig informasjon om den registrertes rettigheter når det gjelder innsyn, retting og sletting av personopplysninger, jf. personopplysningsloven § 19. Se foreløpig rapport punkt 5.6.
- d) Politidirektoratet må gi passøkeren og passinnehaveren tilstrekkelig informasjon om hvordan personopplysninger behandles på grensekontroller i Norge, samt hvordan passene kan forventes benyttet på grensekontroller i utlandet, jf. personopplysningsloven § 19. Se foreløpig rapport punkt 5.6.

e) Politidirektoratet må utarbeide og implementere system for internkontroll i samsvar med personopplysningslovens § 14, jf. personopplysningsforskriften kap. 3. Systemet må implementeres i virksomheten. Se foreløpig rapport punkt 5.7.

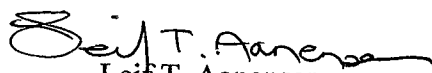
Frist for lukking av vedtakene a til e, settes til 1. mai 2006.

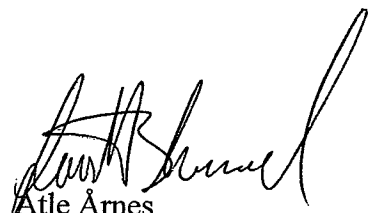
4. Eventuell uttalelse fra virksomheten

Dersom virksomheten har innvendinger mot de varslede pålegg, rapport fra tilsyn, eller kan dokumentere at avvik er brakt til opphør, ber vi om skriftlig tilbakemelding om dette innen 31. januar 2006.

Det gjøres oppmerksom på at dette brevet kun er et varsel om et eventuelt vedtak. Deres tilbakemelding vil være med på å danne grunnlag for et eventuelt vedtak. I Deres svar bes De også å komme med synspunkter på tidspunkt for lukking av vedtak.

Med hilsen


Leif T. Aanensen
Avd. direktør


Atle Årnes
senioringeniør

for

Vedlegg: Foreløpig rapport fra tilsyn

Kopi m/

Vedlegg: Det Kongelige Justis- og Politidepartement

FORELØPIG RAPPORT FRA TILSYN

Saksnummer: 2005/1363 Tilsynsdato: 15.11.2005 Rapportdato: 05.01.2006	Tilsynsobjekt: Politidirektoratet Sted: Oslo	Utarbeidet av: Georg Apenes Hanne P. Gulbrandsen Atle Årnes
--	--	---

1 Innledning

Datatilsynet gjennomførte den 15. november 2005 tilsyn hos Politidirektoratet. Tilsynet ble gjennomført i medhold av personopplysningslovens § 42, 3. ledd jf. § 44. Formålet med tilsynet var å kartlegge om Politidirektoratet har fulgt personopplysningsloven i forbindelse med innføringen av nye biometriske pass med RFID-teknologi og lagringsenhet, fra og med den 3. oktober 2005.

2 Tilstede ved tilsynet

Følgende personer var tilstede ved tilsynet:

Fra Politidirektoratet:

Odd Berner Malme – Assisterende politidirektør

Steinar Talgø – Seksjonssjef, Juridisk seksjon

Unni Norum – Seniorrådgiver, Juridisk seksjon

Eamonn John Casey – Politiets data- og materielltjeneste

Fra Datatilsynet:

Georg Apenes – Direktør

Hanne P. Gulbrandsen – seniorrådgiver

Atle Årnes – senioringeniør

3 Generelt

Anvendelse av elektroniske verktøy etableres på stadig nye felt. For å øke sikkerheten for pass har passmyndighetene i Norge, fra 3. oktober 2005, innført en ny sikkerhetsløsning inkorporert i passene. Norge har i noen år benyttet maskinlesbare pass. Nytt av 3. oktober 2005 er at det også er inkorporert en lagringsenhet med elektronisk lagret ansiktsbilde i passet som kan avleses på avstand via radiobølger (RFID). Norge er et av de første landene i verden som innfører denne nye teknologien i pass.

Under tilsynet ble det opplyst at lagringsenheten pr. i dag inneholder de samme opplysninger som i det papirbaserte pass.

Datatilsynet er opptatt av hvordan den enkelte borger skal kunne føre kontroll med sine personopplysninger. Det er viktig at ikke informasjonssikkerheten for den enkelte blir svekket ved innføring av kontaktløs avlesing av pass.

Passmyndigheten kan langt på vei beslutte hvordan pass skal sikres. Dette setter imidlertid ikke tilside borgernes lovfestede rettigheter. Personvern er en grunnleggende rettighet som er nedfelt i personopplysningsloven. Passmyndigheten må legge dette regelverket til grunn for utarbeidelse av internt regelverk og rutiner.

4 Bakgrunn

Etter hendelsene 11. september 2001 har USA vedtatt som ett av flere tiltak at det fra 26. oktober 2005 skal kreves ansiktsbiometri (digitalt foto) i pass for fortsatt visumfri innreise til USA for reisende med pass utstedt etter denne dato. Denne fristen ble 15. juni 2005 utsatt ett år til 26. oktober 2006 av USA's department of Homeland Security.

Den 13. desember 2004 ble Rådsforordning (EF) nr.2252/2004 om biometri i pass og reisedokumenter, utstedt av medlemslandene, vedtatt. Forordningen ble etter Schengenavtalen også bindende for Norge.

11. mars 2005 sendte Det Konglige Justis- og Politidepartement ut en høring "Elektronisk lagring av biometrisk personinformasjon – forslag til endring i passloven – høring". Høringsfristen var satt til 25. april 2005. Justisdepartementet tok sikte på å fremme en proposisjon for Odelstinget slik at de nødvendige hjemler for bruk av biometrisk personinformasjon lagret i passet kom på plass innen 1. oktober 2005.

8. april 2005 fremskyndet departement høringsfristen for deler av forslaget til 15. april 2005. Dette gjaldt passloven § 6 annet ledd vedrørende ansiktsbiometri. De øvrige forslagene til lovhjemler (fingeravtrykk og lagring av biometri i ekstern database) fikk forlenget frist til 25. juni 2005. Disse øvrige forslagene til lovhjemler er pr. dags dato ikke ferdig behandlet i departementet.

22. mai 2003 ble det vedtatt en anbefaling av ICAO's 188 medlemsland om bruk av biometri i pass.

Når det gjelder sikkerhet for RFID-del og lagringsdel (chip) er det både i Rådsforordning (EF) nr. 2252/2004 og fra norsk side, vist til ICAO (International Civil Aviation Organization) og da spesielt Doc 9303 Machine Readable Travel Documents, Part 1 Machine Readable Passports. Siste utgave er "Fifth Edition" fra 2003. Denne omhandler i hovedsak maskinlesbare pass. Detaljer om biometri, RFID og lagringsenhet fremkommer i "Technical reports". Technical reports publiseres på forhånd før publisering av formelle spesifikasjoner. Technical reports er derfor uformelle spesifikasjoner.

Personopplysningslovens § 13 stiller krav til forholdsmessig sikring av personopplysninger. Bestemmelsen utdypes nærmere i personopplysningsforskriftens kapittel 2. Bestemmelsen innebærer at behandlingsansvarlig må sette rammer for akseptabel risiko og gjennom risikovurdering vise at akseptabel risiko er oppnådd. I arbeide med å oppnå forholdsmessig sikkerhet kan behandlingsansvarlig gjerne støtte seg på internasjonale standarder og tekniske rapporter, men dette setter imidlertid ikke kravet om risikovurdering til side. Behandlingsansvarlig må følgelig uavhengig av slike støttedokumenter kunne dokumentere ovenfor tilsynsmyndigheten at forsvarlig valg er foretatt.

Det understrekes videre at standarder sjeldent har noen formell rettslig stilling i forhold til regelverkets krav, men kan likevel være en måte å oppfylle regelverkets krav på.

5 Vurdering i forhold til personopplysningsloven

I det følgende vil det bli foretatt en gjennomgang av funn vurdert i forhold til personopplysningslovens bestemmelser.

5.1 Lovens virkeområde

Personopplysningslovens § 3 oppstiller saklig virkeområde for loven. All behandling av de nye elektronisk pass innebærer en elektronisk behandling av personopplysninger som faller inn under lovens virkeområde.

5.2 Formål

I henhold til Det Konglige Justis- og Politidepartements høringsbrev skal opplysningene i pass kun brukes til å kontrollere den reisende innehaverens identitet, og at dokumentet er ekte ved passkontroll (grensekontroll).

5.3 Behandlingsansvar

Datatilsynet har, ved tilsynsvarselet, lagt til grunn at behandlingsansvaret ligger sentralt hos Politidirektoratet. Dette er lagt til grunn spesielt med tanke på at det foretas en sentral prosessering/produksjon av pass. Politidirektoratet hadde under tilsynet ingen innvendinger mot at Politidirektoratet entydig er behandlingsansvarlig for utstedelse av pass i Norge.

Politiets data og materielltjeneste (PDMT) er involvert i Politiets arbeid med utstedelse av pass, men sees ikke på som en databehandler, siden etaten er underlagt Politidirektoratet som er behandlingsansvarlig.

Setec OY ansees som en databehandler, da selskapet foretar konkrete oppgaver på vegne av Politidirektoratet i forbindelse med produksjon av pass i Norge.

5.4 Databehandleravtale

En databehandler er en som behandler personopplysninger på vegne av den behandlingsansvarlige jf. personopplysningslovens § 2 nr. 5. Den behandlingsansvarlige kan ikke gjennom en databehandleravtale fri seg fra de plikter og ansvar som påhviler denne etter loven.

Det følger av personopplysningslovens § 15 at en databehandler ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. En databehandleravtale kan ikke gi databehandleren rett til å behandle personopplysninger på en måte som er i strid med personopplysningsloven.

Datatilsynet ba under tilsynet om databehandleravtalen med Setec. Datatilsynet fikk under tilsynet overlevert en kopi av et skriftlig tilbud til Politidirektoratet fra Setec OY. Tilbudet var datert 11. februar 2005. Tilbudet kan bare delvis anses å oppfylle lovens krav til databehandleravtale da det fremgår av loven at databehandler plikter å gjennomføre slike sikringstiltak som tilsvarende de som følger av personopplysningsloven § 13. Tilbudet av 11. februar 2005 er ikke en tilstrekkelig/tilfredsstillende databehandleravtale. Det er nødvendig at det utarbeides en tilstrekkelig databehandleravtale i henhold til personopplysningsloven § 15.

Datatilsynet anser det som en mangel at det ikke er etablert en tilstrekkelig databehandleravtale i henhold til personopplysningsloven § 15.

5.5 Informasjonssikkerhet

Personopplysningslovens § 13 stiller krav om systematiske tiltak for å oppnå forholdsmessig sikring av personopplysninger. Bestemmelsen utdypes nærmere i personopplysningsforskriftens kapittel 2.

Datatilsynet ba under tilsynet om risikovurderinger innen aktuelle områder for de nye passene. Politidirektoratet kunne ikke fremvise dokumentasjon på disse under tilsynet. Manglende fremleggelse av risikovurderinger for informasjonssikkerhet må anses som brudd på personopplysningsloven § 13, jf. personopplysningsforskriftens kap. 2.

Nedenfor opplistes forhold hvor Datatilsynet anser risikovurdering som spesielt nødvendig, men hvor det under tilsynet fremkom at risikovurderinger ikke var foretatt.

Datatilsynet ser det som en mangel at det ikke er etablert risikovurderinger i henhold til personopplysningsloven § 13 og personopplysningsforskriften § 2-4.

5.5.1 Informasjonssikkerhet overordnet

Bruk av elektroniske pass med fjernavlesing via RFID-teknologi vil medføre et sett nye utfordringer med tanke på informasjonssikkerhet.

I Setecs vedlegg 2 i tilbudet til Politidirektoratet, er det satt opp hvilket sikkerhetsnivå som skal benyttes, men det vises kun til uformelle tekniske rapporter fra ICAO. Det vises riktignok til ICAO9303 som er en ferdig standard, men som i femte utgave ikke inneholder detaljer om verken biometri, lagringsmedie eller RFID.

Datatilsynet mener det gir usikkerhet når det i tilbudet med vedlegg er en uklar henvisning til henholdsvis krav fra ICAO og anbefalinger fra ICAO, samt tekniske rapporter fra ICAO. Det er uklart hvilke løsninger som er valgt. All informasjon Datatilsynet har mottatt vedrørende sikkerheten for bruk av pass i Norge henviser til ICAO's dokumenter vedrørende informasjonssikkerhet. Imidlertid er dokumentene kun uformelle tekniske rapporter fra ICAO og ikke formelle dokumenter. Dette har også departementet bekreftet i sitt brev av 12. oktober 2005 til Datatilsynet.

5.5.2 Utsendelse

Utsendelsen av passene til brukere skal gjøres via A-post. Det er ikke fremlagt en risikovurdering av denne avgjørelsen, kun en vurdering rundt kostnader i forhold til rekommandert utsendelse.

Datatilsynet anser at det er nødvendig med en risikovurdering i henhold til personopplysningsloven § 13 og personopplysningsforskriften § 2-4, når det gjelder utsendelse av pass, spesielt med tanke på RFID-enhetens mulighet med fjernavlesning.

5.5.3 Passenes gyldighetstid

Norge har beholdt samme gyldighetstid for de nye passene, som for de maskinlesbare passene. Datatilsynet ble under tilsynet orientert om at det var foretatt en vurdering av om gyldighetstiden kunne beholdes og at grunnlaget for gyldighetstiden lå i den nye elektronikkens levetid på 10 år. Dokumentet er garantert av leverandøren Setec i 10 år. Datatilsynet ble ikke forelagt en konkret

risikovurdering vedrørende passets gyldighetstid. Med tanke på at det er integrert ny teknologi i passet anser Datatilsynet at passets gyldighetstid må risikovurderes. Det ble under tilsynet nevnt at gyldighetstiden ble bestemt av justisdepartementet.

Datatilsynet anser det derfor nødvendig at passenes gyldighetstid risikovurderes i henhold til personopplysningsloven § 13 og personopplysningsforskriften § 2-4.

5.5.4 Passenes sikkerhet for uvedkommendes avlesing

RFID-enheten avgir en UID (unik ID) for å kunne starte kommunikasjon, slik at ikke kommunikasjonen kolliderer med kommunikasjon fra andre pass. Etter at UID er utvekslet benyttes BAC (Basic Access Control) for å forhindre ukontrollert avlesing av pass. Den maskinlesbare koden benyttes som kode (nøkkel) for å åpne for leveranse av personopplysninger fra passet. Datatilsynet stilte under tilsynet spørsmål om BAC er tilstrekkelig for å unngå uønsket avlesing. Datatilsynet nevnte at det i noen tilfeller vil deler av den maskinlesbare koden i passet være opplysninger som kan hentes fra annet hold, for eksempel fødselsdato. Datatilsynet oppfattet svaret fra direktoratet dit hen at BAC er en tilstrekkelig sikker metode, men at metoden ikke er risikovurdert.

Datatilsynet anser det derfor nødvendig at avlesningsmekanismen risikovurderes i henhold til personopplysningsloven § 13 og personopplysningsforskriften § 2-4.

5.5.5 Avlesningsavstand

Ved bruk av BAC forutsettes avlesningsavstanden å være under 10 cm. Uten BAC er det antydning at avstanden vil kunne være 30 cm. Under allerede igangsatt kommunikasjon er det blitt antydning en avlesningsavstander på opp til 10 meter. Avlesningsavstandene er under kontinuerlig utvikling/press med tanke på den teknologiske utvikling. Datatilsynet mener det er en mangel at det ikke foreligger risikoanalyser for avlesningsavstanden. Med tanke på en gyldighetstid på passet på 10 år, bør risikovurderingen også ta høyde for mulig fremtidig utvikling.

Datatilsynet anser det derfor nødvendig at avlesningsavstanden risikovurderes i henhold til personopplysningsloven § 13 og personopplysningsforskriften § 2-4.

5.5.6 Integritet

Det ble under tilsynet opplyst at det elektroniske innholdet i passet ble sikret med en "root key". POD besitter denne "root key". Dette skal sikre at det ikke kan foretas ulovlig endring av innholdet.

Direktoratet opplyste at det ikke er mulig å endre eller legge til opplysninger i den elektroniske lagringsenheten i passet.

Av lovverket fremkommer det ikke hvilke personopplysninger som har fortrinn dersom en av de 3 lagringsmåtene av personopplysninger på passet, skulle inneha uriktige opplysninger (papirutgaven, maskinlesbar del, elektronisk lagret del). Datatilsynet mener at dette er en mangel i henhold til personopplysningsloven § 13 om integritet.

Videre ba Datatilsynet, under tilsynet, om opplysninger om hvor publikum kunne kontrollere at det elektroniske innholdet i eget pass var korrekt, jf. passloven § 6a. Det ble da under tilsynet opplyst at det kun var databehandleren Setec, samt PDMT som var i besittelse av avlesere pr i

dag. Disse var ikke tilgjengelige for publikum. Datatilsynet kunne dermed fastslå at det ikke på en enkel måte var mulig for publikum å verifisere at informasjonen som er lagret i passet er korrekt. Dette anser Datatilsynet som en mangel da dette vanskeliggjør borgerens lovhjemlede innsynsrett.

Datatilsynet spurte under tilsynet om hvilken vurdering som var lagt til grunn for å godta at passøkerne selv leverte inn eget bilde til bruk i passet. I Sverige er det etablert egne stasjoner og fotoapparater for å ta passbilder hos politiet og dermed sikres korrekt bilde. Man hadde fra norsk side vurdert tilsvarende fotostasjoner, men ikke implementert slike. Fotostasjoner ble av Politidirektoratet avvist av økonomiske grunner. Datatilsynet etterspurte en risikovurdering for dersom en person leverte feil bilde og at dermed selve dataleveransen for å kunne produsere passet ble feil. En sammenlikning av de biometriske dataene i passbildet med biometriske data i et annet bilde gjøres sikrest maskinelt. En visuell sammenlikning av bildene kan medføre feil. Politidirektoratet kunne ikke vise til at det var foretatt en risikovurdering på dette. Det ble kun foretatt en visuell kontroll på passutstedelsesstedet.

Datatilsynet anser det derfor nødvendig at datainnhentingens risikovurderes i henhold til personopplysningsloven § 13 og personopplysningsforskriften § 2-4.

5.6 Informasjon

Personopplysningslovens §§ 19 og 20 oppstiller krav til informasjonsplikt når personopplysninger henholdsvis samles inn fra den registrerte og fra andre. Personopplysningslovens § 23 har bestemmelser om unntak fra informasjonsplikten.

Datatilsynet informerte under tilsynet om at tilsynet samme dag som tilsynet fant sted, hadde vært på Politiets nettsted for å finne informasjon om hvordan personopplysninger ble håndtert med tanke på søknad om og utstedelse av pass. Det var lite informasjon vedrørende pass, for de nye biometriske passene var det etter Datatilsynets mening, ikke tilstrekkelig informasjon. Politidirektoratet opplyste under tilsynet at det heller ikke var laget annen informasjon om pass til passøkere.

Under tilsynet påpekte Datatilsynet at informasjonen som var blitt gitt til publikum ga motstridende opplysninger. Det er oppgitt at passbildet ikke skulle være over 3 måneder gammelt, en annen nettside angir at bildet ikke skal være over 6 måneder gammelt.

I henhold til passloven § 6, 4. ledd er det satt krav om sletting av personopplysninger etter at vedkommendes identitet er verifisert ved grensekontroll. Informasjon om hvordan dette vil kunne forventes håndtert i utlandet, mangler.

Datatilsynet anser at Politidirektoratet ikke har gitt tilstrekkelig informasjon slik personopplysningsloven §§ 19 og 20 krever.

5.7 Internkontroll

Personopplysningsloven § 14 oppstiller krav om at den behandlingsansvarlige etablerer internkontroll gjennom dokumenterte, planlagte og systematiske tiltak.

Det stilles ikke krav om et eget system for etterlevelse av personopplysningslovens bestemmelser. Tvert imot er det hensiktsmessig at dette integreres med den behandlingsansvarliges øvrige behov for å føre internkontroll.

Internkontroll var ett blant flere andre temaer under tilsynet, og ble berørt i tilknytning til de forskjellige felt. Det ble generelt konstatert at virksomheten hadde mangelfullt etablert internkontroll for håndtering av de nye pass. Virksomheten kunne fremvise noen fragmenterte rutiner, men viste i all hovedsak til en pågående prosess hvor et tilfredsstillende nivå skulle etableres.

Manglende fremleggelse av etablerte og implementerte rutiner for internkontroll må anses som brudd på personopplysningsloven § 14 jf. personopplysningsforskriftens kap. 3.

6 Avslutning

Varsel om vedtak om pålegg fattet som følge av konklusjoner fra tilsynet, følger i eget brev.