Datatilsynet

Justis- og politidepartementet
Postboks 8005 Dep
0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
201101405	11/00222-2	20. mai 2011

Høringsuttalelse - Endringer i utlendingsloven ved innføring av Schengen standardisert oppholdskort med elektronisk lagret biometri

Det vises til departementets høringsbrev av 23. februar 2011 om endringer i utlendingsloven ved innføring av Schengenstandardisert oppholdskort med elektronisk lagret biometri. Datatilsynet har enkelte merknader til forslaget.

1 Generelt om bruk av biometriske kjennetegn

Departementet legger i sine vurderinger vekt på at biometriske kjennetegn ikke er å anse som sensitive personopplysninger i henhold til definisjonen i personopplysningslovens § 2 nr 8.

Datatilsynet er enig i dette, men vil understreke at biometriske kjennetegn allikevel ikke kan vurderes på lik linje med andre ikke-sensitive personopplysninger.

Det vises til at biometriske kjennetegn er *unike* identifikatorer, og at disse er *uløselig* knyttet til det enkelte individet. Det tilsier både at terskelen for å ta i bruk biometriske kjennetegn skal legges høyt, og at behandlingen skal underlegges en særskilt beskyttelse.

Av nevnte grunner et det også etablert en egen bestemmelse i personopplysningsloven, som oppstiller skjerpede krav til bruk av biometri.

Datatilsynet vil også kort nevne at den rettslige statusen til denne type opplysninger kan endres i overskuelig fremtid. I forbindelse med at personverndirektivet skal revideres har det vært tatt sterkt til orde for å innlemme biometriske kjennetegn i listen over sensitive personopplysninger.

2 Nærmere om fingeravtrykket – fullt fingeravtrykk eller markører?

Departementet foreslår at det skal registreres to fulle fingeravtrykk ved behandlingen, i tillegg til et bilde av innehaverens ansikt.

For at et tiltak skal være proporsjonalt i henhold til EMK artikkel 8 er det en forutsetning at andre mindre inngripende tiltak ikke fungerer tilfredsstillende for det aktuelle formålet.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Datatilsynet vil bemerke at den foreslåtte løsningen innebærer en større trussel mot personvernet enn for eksempel bruk av markører (templates).

For det første er behandlingen mer *omfattende*, idet man ved bruk av bilde reelt sett registrerer flere opplysninger om den enkelte enn ved bruk av markører. Videre vil tilsynet peke på at *misbrukspotensialet* for et fullt fingeravtrykk er betraktelig mye større enn for markører.

Datatilsynet savner en begrunnelse for hvorfor det i denne forbindelse er nødvendig å benytte det fulle fingeravtrykket. Tilsynet vil i den forbindlese bemerke at bruk av markører *i seg selv* kan gi svært god identifikasjon. I dette tilfellet skal innehaver av kortet i tillegg identifiseres med et *bilde av ansiktet.* Datatilsynet anser at disse elementene i kombinasjon tilfredsstillende vil kunne ivareta identifikasjonshensynet.

Det å benytte fullt fingeravtrykk fremstår etter tilsynets vurdering å være unødvendig, og derfor uproporsjonalt i henhold til EMK artikkel 8.

3 Nærmere om lagring – lokalt eller sentralt?

Datatilsynet er tilfreds med forslaget om at biometriske data kun skal oppbevares i kortet, og at det ikke skal etableres en sentral lagring. Tilsynet merker seg imidlertid at departementet allikevel utreder *fremtidig sentral lagring* av biometri, for blant annet å forenkle prosessen med fornyelse av kortet.

Tilsynet vil allerede nå bemerke at sentral lagring av biometri vil medføre en langt større trussel mot den enkeltes personvern, enn en løsning hvor opplysningene kun lagres i kortet.

For det første medfører sentral lagring at den enkelte innehaver får mindre *kontroll* med egne personopplysninger. I tillegg kommer at en sentral lagring vil øke muligheten for at opplysningene blir benyttet for *andre formål* enn de egentlig ble hentet inn for (formålsglidning). Endelig vil en sentral base måtte underlegges svært strenge krav til *informasjonssikkerhet.*

Disse hensynene gjør seg selvsagt sterkere gjeldende dersom *hele fingeravtrykket*, og ikke bare markørene, skal lagres i løsningen.

Datatilsynet forutsetter at et eventuelt sentralt register vil måtte hjemles i lov, og avventer en eventuell egen lovprosess knyttet til dette.

4 Nærmere om ansvarsforhold

4.1 Behandlingsansvarlig

Departementet plasserer behandlingsansvaret for "innhenting og lagring av biometrisk personinformasjon" i Utlendingsdirektoratet (UDI), jf utkast til § 18-4a.

Datatilsynet vil bemerke at ordlyden kan virke begrensende for UDIs behandlingsansvar. Tilsynet stiller derfor spørsmål ved om direktoratets ansvar er ment å være begrenset til innhenting og lagring, og ikke til *annen behandling* som finner sted i den konkrete prosessen, for eksempel matching, oppdatering, kvalitetssikring og sletting. Dersom denne avgrensningen er tilsiktet ber tilsynet om at ansvaret for all øvrig behandling plasseres tydelig. Dersom avgrensningen er utilsiktet anbefaler tilsynet at ordlyden endres. Det kan for eksempel skje gjennom at ordene "innhenting og lagring" erstattes med ordet "behandling".

4.2 Databehandlere

Departementet legger til grunn at det kan bli aktuelt å sette ut (outsource) oppgaven med å innhente biometri, til aktører utenfor utlendingsforvaltningen.

Datatilsynet vil i den forbindelse understreke at det å benytte en leverandør ikke medfører endringer i direktoratets behandlingsansvar. Leverandøren blir i denne forbindelse å anse som en databehandler, som behandler opplysninger på vegne av UDI.

Som behandlingsansvarlig påhviler det direktoratet å påse at en aktuell tjenesteyter gjennomfører behandlingen i tråd med direktoratet instruksjoner. Det skjer gjennom inngåelse av en databehandleravtale etter personopplysningslovens § 15, hvor det etableres nødvendig instruksjonsmyndighet for direktoratet overfor den aktuelle leverandøren.

5 Kort om informasjonssikkerhet

Personopplysningslovens bestemmelser om informasjonssikkerhet vil komme til anvendelse ved behandlingen. I den forbindelse vil Datatilsynet peke på at det å benytte en såkalt "kontaktløs databrikke" vil kunne medføre en sikkerhetsutfordring. Slike brikker kan leses av på avstand, hvilket medfører en risiko for at uvedkommende skaffer seg tilgang til opplysninger i kortet ved bruk av fjernavlesningsutstyr for eksempel på flyplasser og andre steder hvor folk ferdes med pass.

Med hilsen

Bjørn Erik Thon
direktør

Cecilie L. B. Rønnevik
seniorrådgiver