Datatilsynet

Personvernnemnda
Postboks 4594 Nydalen

0404 OSLO

Deres ref. Vår ref. (bes oppgitt ved svar)
06/01169-1 /AFL 25. august 2006

OVERSENDELSE AV KLAGESAKER OM BRUK AV FINGERAVTRYKK

Vedlagt følger fem klagesaker knyttet til bruk av fingeravtrykk i forskjellige sammenhenger. Sakene er forskjellige med hensyn til faktum og formål, men har store likheter i det de alle gjelder bruk av fingeravtrykk som bearbeides til en såkalt "template" og spørsmålet er i hvilken grad slik bruk av fingeravtrykk medfører bruk av entydige identifikasjonsmidler som faller inn under personopplysningslovens § 12 og hva som eventuelt skal til for at vilkårene i denne paragrafen er oppfylt. Det er Datatilsynets oppfatning at konklusjonene i hver av sakene vil ha betydning for de øvrige sakene, og at det derfor er viktig at de behandles i sammenheng.

Det er i klagesakene hevdet at bruken av fingeravtrykk oppfattes som enkel og praktisk av brukerne. Bruk av fingeravtrykk oppleves imidlertid av mange som en inngripen i den enkeltes integritet. Datatilsynet mottar jevnlig henvendelser fra enkeltpersoner som opplever det som krenkende at man skal måtte gi fra seg fingeravtrykk, det være seg på jobb eller ved inngangen til et treningssenter og lignende. Flere av klagesakene er oppstått på denne måten. Selv om fingeravtrykket legges igjen en rekke plasser uten at man er seg dette bevisst, oppleves det som svært inngripende når dette avkreves for at man skal få en gitt rettighet eller adgang til et område. Som det fremgår nedenfor samt vedlegg til dette brevet, finner Datatilsynet at det er en reell usikkerhet med hensyn til mulig misbruk, og at det derfor ikke kan utelukkes at bruken av fingeravtrykk utgjør en personverntrussel. Dette er et viktig bakteppe for behandlingen av de foreliggende sakene.

Fingeravtrykk og "template"
En personopplysning er etter Personopplysningslovens § 2 nr. 1 *"opplysninger og vurderinger som kan knyttes til en enkeltperson"*.

I samtlige av klagesakene benyttes fingeravtrykk til å generer en "template". Templaten er en bearbeidet utgave av en biometrisk prøve. Når en person registreres i et biometrisk system, tas en biometrisk prøve av personen, for eksempel ved at det gis et fingeravtrykk. Fra denne biometriske prøven velges det ut bestemte målepunkter som bearbeides og lagres. En template har to særskilte egenskaper; den tar vesentlig

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

mindre plass å lagre enn den opprinnelige biometriske prøven, og den er egnet for sammenligning.

Ingen av klagerne har hevdet at fingeravtrykket eller template av et fingeravtrykk ikke skal anses som en personopplysning. Fire av de fem klagerne har argumentert med at formålet med bruken av fingeravtrykk er å identifisere enkeltpersoner. I disse fire sakene er det også faktum at fingeravtrykket og templaten av dette er tenkt kontrollert opp mot tidligere registrert templater som er lagret i personregistre som ansattregister eller medlemsregister.

Den ene klageren, Tysvær kommune, har argumentert med at templaten ikke benyttes til identifisering og at den heller ikke er entydig. Datatilsynet finner derfor at det er nødvendig å berøre spørsmålet om fingeravtrykket eller templaten av dette skal anses som en personopplysning.

Datatilsynet viser til vurderinger i klagesak 06/0047 og bemerker kort at tilsynet vanskelig kan se at en sikkerhetsløsning kan fungere godt med mindre det finnes en eller annen kobling mellom den presenterte finger som benyttes til å utarbeide templaten og identitet på den som tillates å koble seg på maskinen. Det er usannsynlig at arbeidsgiver ikke har et eller annet register over hvem som har fått tildelt den enkelte maskin og/eller hvem som kan benytte dem. Dette er for øvrig en oversikt som arbeidsgiver er forpliktet til å ha jf. personopplysningslovens §§ 13 og 14 samt personopplysningsforskriftens bestemmelser om datasikkerhet og internkontroll, særlig personopplysningsforskriftens §§ 2-8, 2-10 flg.

Datatilsynet vil bemerke at det ikke kan garanteres at en generert template for all fremtid vil være irreversibel, slik det er beskrevet fra klagernes side. Videre er det uansett slik at man kan finne ut hvem som eier en bestemt lagret template, ved å avkreve nytt fingeravtrykk av den gruppen mennesker som er registrert (for eksempel. ansatte eller medlemmer på et treningssenter), for deretter å se hvor man får treff. Dersom man kjenner til algoritmen som benyttes og templaten, kan man dessuten sammenligne fingeravtrykk samlet inn uten eierens kunnskap og samtykke for å se om fingeravtrykket gir match med den lagrede template.

Datatilsynet støtter seg for øvrig på art. 29 gruppens[1] vurdering i *Working document on biometrics* vedtatt 1. august 2003 av at biometriske kjennetegn, herunder templater laget på bakgrunn av slike kjennetegn, må anses som personopplysninger i personverndirektivets (Direktiv 95/46/EF) forstand. I direktivets art. 2 a) er *"personal data"* definert som *"any information relating to an identified or identifiable natural person (…); an identifiable person is one who can be identified, dierctly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental (…) identity"*. Det uttales videre i fortalens pkt 26: *"to determine wether a person is identifiable, account should be taken of all means likely reasonably to be used either by the controller or by any other*

[1] Jf. Direktiv 95/46/EF art. 29.

person to identify the said person". På denne bakgrunnen har Art. 29 trukket følgende konklusjon på s. 5: *"It appears that biometric data can always be considered as "information relating to a natural person" as it concerns data, wich provides, by its very nature, information about a given person"*.

Art. 29 gruppens arbeidsdokument vedlegges i kopi.

Personopplysningslovens § 12 – entydig identifikasjonsmiddel
Datatilsynet har utformet et forslag til endring av personopplysningslovens § 12. Forslaget er nå oversendt til Justisdepartementet som ansvarlig departement for loven. Forslaget vedlegges i kopi, da det i stor grad redegjør for Datatilsynets tolkning av gjeldende rett. Det vises særlig til forslagets kap. 2.2 og kap. 3.1. Notatet har betydning i forhold til samtlige av klagesakene.

Datatilsynet støtter seg på Ot. Prp. Nr. 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven) s. 114 hvor det i merknad til § 12 uttales: "Bestemmelsen gir en generell regulering av bruk av fødselsnummer og andre entydige identifikasjonsmidler som for eksempel fingeravtrykk og andre biometriske data" (vår understrekning). Det må tillegges stor vekt i vurderingen at fingeravtrykk er nevnt spesielt i forarbeidene som et av de entydige identifikasjonsmidler som paragrafen er ment å skulle omfatte.

Datatilsynet vil understreke at en template genereres ved en elektronisk bearbeidelse av et presentert fingeravtrykk. Selv om systemet kun sammenligner en tidligere lagret template med senere genererte templater, må fingeravtrykket presenteres hver gang løsningen skal benyttes. Fingeravtrykket – som i henhold til Ot.prp. 92 anses å være et entydig identifikasjonsmiddel – behandles elektronisk i det man produserer templaten, både ved første gangs registrering og ved senere bruk av løsningen. Datatilsynet finner derfor at personopplysningslovens § 12 kommer til anvendelse for bruk av de forskjellige løsningene som klagerne ønsker å benytte.

Under det meste av argumentasjon Datatilsynet har møtt for bruk av fingeravtrykk ligger en formening om at fingeravtrykket er den sikreste løsning fordi bare du og ingen andre kan produsere ditt fingeravtrykk. Dette gjelder også for løsninger hvor fingeravtrykket benyttes for å generere en template. Datatilsynet legger derfor til grunn at også den alminnelige forståelsen er at et fingeravtrykk, om enn omformet til en template, er et entydig identifikasjonsmiddel. Også i markedsføring av løsningene er denne forståelsen lagt til grunn; templaten er ment å skulle være så entydig som hensiktsmessig gjennomførbart, for derigjennom å gi best mulig sikkerhet for at man står overfor rett person. Det er imidlertid stor spredning i kvaliteten på de forskjellige løsninger, og Datatilsynet ser ikke bort i fra at det kan finnes løsninger som er såpass dårlige, dvs. har såpass høy akseptert feilrate, at den template som utarbeides i realiteten ikke blir entydig. Datatilsynet finner ikke dette avgjørende, fordi man ved utarbeidelsen av templaten uansett behandler den biometriske prøve (her fingeravtrykket) som anses å være entydig.

Det er etter dette tilsynets oppfatning at bruk av fingeravtrykk må oppfylle kravene i personopplysningslovens § 12.

Fingeravtrykk kan etter dette bare benyttes når:
1. Det er saklig behov for sikker identifisering og
2. Metoden er nødvendig for å oppnå slik identifisering.

Vilkårene er kumulative.

Saklig behov for sikker identifisering

I NOU 1997: 19 Et bedre personvern s. 85 er det i tilknytning til det som i dag er personopplysningslovens § 12 uttalt om identifikasjon: *"Med identifikasjon menes at fødselsnummeret på en relativt entydig måte peker ut en bestemt person. Dette er den funksjonen fødselsnummer primært bør ha. I visse sammenhenger har imidlertid fødselsnummer blitt sett på som legitimasjon, dvs. sannsynliggjøring av at en enkeltperson er den han utgir seg for å være. Fødselsnummer er imidlertid ikke egnet til å tillegges slike legitimasjonsvirkninger, noe som blant annet har ført til en rekke brudd på taushetsplikt fordi taushetsbelagte opplysninger er blitt gitt ut når et fødselsnummer er blitt oppgitt. Dersom det innskjerpes at fødselsnummer skal tjene som identifikasjon og ikke legitimasjon, kan personvernet være tjent med at fødselsnummer brukes i større utstrekning og i tilfeller der andre teknikker gir for usikker identifikasjon. Dette er bakgrunnen for utvalgets forslag om bruk av fødselsnummer."* Det er ingen realitetsforskjell mellom utvalgets forslag til bestemmelse og dagens § 12.

Datatilsynet er klar over at utvalgets uttalelser er gitt i forhold til fødselsnummer, og at andre entydige kjennetegn, som for eksempel fingeravtrykk, har egenskaper ved seg som gjør dem bedre egnet for legitimasjonsformål enn det fødselsnummer er. Datatilsynet finner imidlertid at man ved lovens utforming klart har ment at bestemmelsen kun skulle tillate bruk av entydige identifikasjonsmidler for ren identifisering i motsetning til legitimering/bekreftelse av identitet. Det kan vanskelig forsvares å innføre en ny tolkning av ordet i tilknytning til fingeravtrykk, selv om dette kan gi et bedre resultat i enkelttilfeller. Det må i denne sammenheng nevnes at en slik "utvidet" tokning av bestemmelsen på dette feltet nødvendigvis vil ha betydning for tolkningen også hva gjelder fødselsnummer. Det vil ha svært alvorlige konsekvenser for personvernet dersom § 12 skulle tolkes på en slik måte at konsekvensen blir at man for eksempel tillater at fødselsnummer blir benyttet som passord ved pålogging til datamaskin.

Datatilsynet viser også til at man i sikkerhetsteori normalt skiller mellom identifisering og autentisering eller bekreftelse av identitet jf. det vedlagte notats pkt. 3. 1 og 1.3. I informasjonssikkerhetsteorien er begrepet autentisering klart forstått som prosessen i å bekrefte en påstått eller antatt identitet. Definisjonene av identifisering varierer generelt innenfor det som er drøftet i Datatilsynets notat. Det vises her til

definisjonene lagt ut av standardiseringsorganet ETSI[2] som et eksempel. Her er identifisering (user identification) definert som prosessen med å kjenne igjen en bruker, mens autentisering (authentication) er definert som metoden for å bevise den påståtte identiteten til en part.

På denne bakgrunn har Datatilsynet funnet at ordet "identifisering" skal tolkes strengt, slik at bruk av entydige identifikasjonsmidler som legitimasjon eller i tilknytning til verifisering av identitet/autentisering, ikke er tillatt. Denne forståelsen er lagt til grunn i alle klagesakene.

Sikker identifisering og sikkerhet

Det følger av personopplysningslovens § 12 at entydige kjennetegn bare kan benyttes der det er saklig behov for sikker identifisering. Dette blir av enkelte klagere forvekslet med behov for fysisk sikring. Sikker identifisering av enkeltpersoner kan ha betydning for fysisk sikring, men det vil være i strid med personopplysningslovens § 12 å benytte entydige identifikasjonsmidler ved behov for fysisk sikring hvis det ikke samtidig foreligger et behov for sikker identifisering eller hvis den samme eller bedre fysisk sikring kan oppnås uten bruk av entydige identifikasjonsmidler. Bedre inngjerding av fysiske områder, er et eksempel. Bruk av autentisering ved hjelp av passord eller kontroll av smartkort ved pålogging til datasystemer er et annet.

Vurdering etter personopplysningslovens § 8 og 11

Datatilsynet har ikke funnet grunn til å vurdere om personopplysningslovens §§ 8 og 11 er oppfylt i tilknytning til klagesakene, da behandlingen uansett ikke anses lovlig etter personopplysningslovens § 12. Dette innebærer at Datatilsynet ikke har foretatt noen helhetlig proporsjonalitetsvurdering av andre elementer enn det som er ansett riktig i forhold til denne paragrafen. Dersom Personvernnemnda skulle komme til en annen forståelse av personopplysningslovens § 12 enn Datatilsynet, slik at vilkårene i denne paragrafen ikke blir avgjørende, ber tilsynet om at sakene sendes tilbake for ny behandling jf. forvaltningslovens § 34, siste ledd. Det vises i denne anledning til at det foreligger vedtak mot bruk av fingeravtrykk som ikke er påklaget i andre saker, og at Datatilsynet ønsker å se sakene i sammenheng og å innhente ytterligere informasjon om momenter andre europeiske tilsynsmyndigheter har vektlagt i vurderingen.

[2] The European Telecommunications Standards Institute (ETSI), Telecom Terms and Definitions, http://webapp.etsi.org/Teddi/

Det er Datatilsynets oppfatning at de problemstillinger som behandles i klagesakene er kompliserte, og at resultatet av Personvernnemndas vurdering vil få vidtrekkende konsekvenser. Datatilsynet ber derfor om anledning til å gi innspill i forhold til eventuelle utredninger og andre opplysninger som Personvernnemnda eventuelt måtte beslutte å innhente i tilknytning til sakene.

Med hilsen

Knut B. Kaspersen
avdelingsdirektør

Astrid Flesland
seniorrådgiver

Kopi: Justis- og politidepartementet, Lovavdelingen, Postboks 8005 Dep, 0030 OSLO
Gymmet AS v/Rune S. Henriksen, Fredriksborgveien 38, 0286 Oslo
Oxigeno Fitness v/Rune S. Henriksen, Maridalsveien 17, 0175 Oslo
Esso Norge AS, v/Finn Arne Hobæk, Pb. 2001 Postterminalen, 3103 Tønsberg
Advokatfirmaet Wiersholm v/Kyrre Eggen, Pb. 1400 Vika, 0115 Oslo
Kluge advokatfirma, v/Ingvild Mestad, Pb. 1548 Vika, 0117 Oslo

Vedlegg: Klagesaker 06/83, 05/1556, 06/47, 05/1226, 06/180
Brev til Justisdepartementet av 31. mars 2006
Notat fra Datatilsynet – forslag til revisjon av personopplysningslovens § 12
Working document on biometrics 12168/02/EN

Datatilsynet

Personvernnemnda
Postboks 4594 Nydalen
0404 OSLO

Deres ref. Vår ref. (bes oppgitt ved svar)
05/01226-12 /AFL 25. august 2006

OVERSENDER KLAGE - ESSO NORGE AS - BRUK AV FINGERAVTRYKK

Datatilsynet fattet 16. februar 2006 vedtak om at Esso Norge AS ikke kunne benytte fingeravtrykk i tilknytning til adgangskontroll til tankanlegg. Vedtaket ble påklaget i brev datert 23. februar 2006. Klagen er rettidig. Tilsynet beklager svært lang saksbehandlingstid som skyldes behov for grundig utredning av saken, herunder gjennomføring av befaring, og ferieavvikling.

Datatilsynet har vurdert klagen. Datatilsynet finner ikke grunn til å endre vedtaket. Saken oversendes derfor til Personvernnemnda, jf personopplysningsloven § 42 fjerde ledd.

1. Sakens gang:
Esso Norge AS søkte 15. september 2005 om konsesjon for behandling av fingeravtrykk i tilknytning til adgangskontroll ved fire forskjellige tankanlegg, henholdsvis i Fredrikstad, Tønsberg, Trondheim og Bergen. Som vedlegg til konsesjonssøknaden fulgte et eksempel på samtykkeerklæring samt en utskrift av selskapets "Safety Policy".

I brev av 5. oktober 2005 opplyste Datatilsynet at konsesjonssøknaden ikke ga tilstrekkelige opplysninger for at Datatilsynet kunne vurdere lovligheten av tiltaket. Det ble blant annet vist til vilkårene for bruk av entydige identifikasjonsmidler i personopplysningslovens § 12. Det ble understreket at konsesjonssøknaden ikke ville bli behandlet før mer utfyllende opplysninger var mottatt hos tilsynet. Brevet gir uttrykk for at det er aktuelt å utforme konsesjon for den planlagte bruken av fingeravtrykk. Datatilsynet vil derfor understreke at fingeravtrykk ikke er ansett som en sensitiv personopplysning jf. personopplysningslovens § 2 nr. 8, og at bruk av fingeravtrykk ikke er underlagt konsesjonsplikt med mindre Datatilsynet gjør særskilt vedtak om dette etter bestemmelsen i personopplysningslovens § 33, andre ledd. Noe slikt vedtak er ikke fattet, verken i denne saken eller i andre saker vedrørende bruk av fingeravtrykk.

I brev av 14. oktober 2005 redegjør Esso Norge nærmere for den planlagte bruken av fingeravtrykk. I brev av 23. november opplyser Datatilsynet om at tilsynet ville se

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

samlet på en rekke saker om bruk av fingeravtrykk og andre biometriske opplysninger i forhold til personopplysningslovens § 12 , bl.a. for å vurdere å innføre konsesjonsplikt jf. personopplysningslovens § 33, andre ledd. Det blir videre antydet at tilsynet uansett finner det tvilsomt om lovens vilkår er oppfylt hva gjelder den bruken Esso Norge AS hadde søkt om.

Som nevnt over har tilsynet ikke fattet vedtak om konsesjonsplikt. Det ble imidlertid i brev av 16. februar 2006 fattet vedtak om at Esso Norge ikke oppfylte vilkårene i personopplysningslovens § 12 for bruk av fingeravtrykk i adgangskontroll.

Vedtaket ble påklaget i brev av 23. februar 2006. 23. mars 2006 var Datatilsynet på befaring på Esso Norges tankanlegg på Slagentangen ved Tønsberg. Et kortfattet referat fra befaringen vedlegges til orientering.

2. Klagers anførsler

I det følgende gis en sammenfatning av klagers anførsler, slik de er uttrykt gjennom sakens dokumenter, samt muntlig under befaring.

Klager er enig i at personopplysningslovens § 12 kommer til anvendelse, men er ikke enig i at den planlagte bruken av fingeravtrykk strider mot denne paragrafen. Det opplyses at formålet med fingeravtrykksløsningen er identifisering. Etter klagers oppfatning endres ikke dette formålet av at man også benytter adgangskort, da begge deler er elementer i identifiseringen, og at kun adgangskort ikke er tilstrekkelig av sikkerhetshensyn.

Det trekkes frem at leverandør og løsning er besluttet sentralt av ExxonMobil som eier Esso Norge. Det er meningen at den samme løsningen skal benyttes i flere land i Europa. Det blir beskrevet at ID-kort kombinert med fingeravtrykk er valgt i adgangskontrollen av flere årsaker. Det vises til viktigheten av at kun autoriserte personer får adgang til anlegget fordi det er store mengder brennbart materiale samlet der, og at det vil ha sikkerhetsmessige aspekter dersom de brannfarlige varene kommer i uautoriserte hender. Det vises videre til krav til adgangskontroll i ISPS code. Det vises også til de økonomiske verdier produktene innehar, samt at anlegget benyttes på alle tider av døgnet. Selskapet tillater at personer som ikke samtykker til bruk av fingeravtrykk benytter en PIN kode i stedet.

Det er presisert at man kun benytter en template beregnet ut i fra syv punkter i fingeren som lagres separat fra personelldata, i egen database. Kortnummer (fra adgangskort) er link mellom databasene. Løsningen er nærmere beskrevet i informasjonsskrivet fra TopTech som Datatilsynet har mottatt.

Klager hevder at bruk av fingeravtrykk er nødvendig fordi det gis direkte adgang til områder hvor det lagres og håndteres brannfarlig vare (bensiner), og at sikker identifisering er nødvendig for å få adgang. Det opplyses at klager må være helt sikker på at vedkommende som gis adgang er godkjent og innehar nødvendig kunnskaper til å ferdes alene på området.

Klager anfører videre at den overordnede begrunnelse for bruk av fingeravtrykk er relatert til sikkerhetsmessige aspekter, herunder forhindre at store volum kommer på avveie. Videre at virksomheten er underlagt krav til sikkerhet, og har en godkjenning fra Kystdirektoratet som forutsetter at tankanlegget har et godt og tilfredsstillende system for adgangskontroll slik at uautorisert adgang ikke skal forekomme. Det er klagers oppfatning at fingeravtrykk er en bedre metode for å redusere mulig terrortrussel.

Klager anfører også at adgangskort og kode kan benyttes av uvedkommende. Bruk av fingeravtrykk hindrer misbruk. Klager anfører videre at godkjent adgang gir tilgang på uttak av produkter som kan være farlige i uautoriserte hender og som også har stor økonomisk verdi. Videre at adgang til anlegget gis hele døgnet og at vedkommende kan være helt alene innenfor anlegget.

Klager har opplyst at bruken av fingeravtrykk er godkjent i Belgia og Nederland.

3. Datatilsynets vurdering

Det foreligger ingen uenighet mellom klager og Datatilsynet med hensyn til at fingeravtrykk/template er et entydig identifikasjonsmiddel og at bruken skal følge reglene i personopplysningslovens § 12. Datatilsynet vil likevel vise til de vurderinger som er gjort i samlet oversendelsesbrev til Personvernnemnda, samt notat om endring av personopplysningslovens § 12 som er oversendt til Justisdepartementet.

<u>Personopplysningslovens § 12.</u>

Fingeravtrykk kan etter personopplysningslovens § 12 bare benyttes når:

1. Det er saklig behov for sikker identifisering og
2. Metoden er nødvendig for å oppnå slik identifisering.

Vilkårene er kumulative.

Datatilsynet finner at ordet ”identifisering” skal tolkes strengt, slik at bruken av entydige identifikasjonsmidler som legitimasjon eller i tilknytning til verifisering av identitet/autentisering, ikke er tillatt.

<u>Saklig behov for sikker identifisering</u>

Det er Datatilsynets oppfatning at klager har misforstått det første vilkåret i § 12 dit hen at et stort behov for fysisk sikring også gir stort behov for sikker identifisering. Datatilsynet er ikke uenig med klager i at det foreligger et behov for fysisk sikring av tankanlegget mot terrorangrep og tyveri, og at god adgangskontroll kan være et ledd i slik fysisk sikring. Et ønske om på en bedre måte å stenge uvedkommende ute fra dette tankanlegget, kan imidlertid oppfylles gjennom andre grep enn fingeravtrykkskontroll. For eksempel vil høye murer, øket vakthold, døgnbemanning m.m. kunne ha en effekt på dette. Behovet for sikker identifisering er knyttet til spørsmålet om hvem man faktisk skal slippe inn gjennom den ordinære porten til anlegget.

Datatilsynet finner at det kan sies å foreligge et saklig behov for adgangskontrollen til tankanleggene. Adgangskontroll forutsetter at de personer som har rettmessig adgang

gjenkjennes. Det kan på denne bakgrunn anføres at det foreligger et visst saklig behov for sikker identifisering. Tilsynet finner imidlertid at fingeravtrykket ikke benyttes til identifisering, men til autentisering etter at identifiseringen har funnet sted. Datatilsynet understreker at leverandøren av fingeravtrykksløsningen, ToptechSystems Inc, synes å dele Datatilsynets oppfatning av at verifisering av identitet ved hjelp av fingeravtrykk er noe annet enn identifisering. Det vises i denne anledning til informasjonsskrivet om Toptech VeriFID hvor det i første avsnitt opplyses at en persons fingeravtrykk benyttes "to confirm their identity", mens det i fjerde avsnitt opplyses at "During the verification process, a User is identified using their proximity card or pin number". Altså identifiserer man seg ved hjelp av ID-kort eller PIN. Mens fingeravtrykket benyttes til autentisering. Datatilsynets konklusjon er på denne bakgrunn at selv om det foreligger et saklig behov for sikker identifisering, benyttes fingeravtrykket ikke til identifisering slik § 12 krever.

Metoden er nødvendig for sikker identifisering

Datatilsynet vil bemerke at heller ikke det andre vilkåret i § 12 anses å være oppfylt.

Spørsmålet i forhold til personopplysningslovens § 12 er ikke om innføring av fingeravtrykkskontroll gir bedre sikkerhet mot terror eller tyveri, men om bruken av fingeravtrykk er nødvendig for å oppnå sikker identifisering. Det er klart uttalt i forarbeidene at entydige identifikasjonsmidler ikke skal brukes i utrengsmål. Det følger av dette at nødvendighetsvurderingen bør være streng. I Ot. Prp. Nr. 92 Om behandling av personopplysninger s. 114 uttales følgende: *"Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f eks navn, adresse og kundenummer ikke er tilstrekkelig. Det vil også ha betydning hvor viktig identifiseringen er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt."*

Det at enkeltpersoner ofte mister kort eller glemmer PIN-kode er etter dette ikke tilstrekkelig for at bruk av fingeravtrykk skal anses som nødvendig for sikker identifisering. Det er heller ikke et argument i denne tiknytning at de det gjelder ønsker løsningen, og finner denne praktisk i bruk.

Det er Datatilsynets oppfatning at klager kan oppnå like sikker identifisering ved å innfører døgnbemannet adgangskontroll, slik selskapet har for raffineriet som ligger i tilknytning til tankanlegget. Manuelle visuell kontroll opp mot adgangsbevis er et godt alternativ til bruk av fingeravtrykk. Dersom klager mener det er behov for autentisering av identiteten, kan løsningen suppleres med bruk av PIN-kode. Den visuelle kontrollen vil forhindre at kort og kode blir benyttet av andre enn den rettmessige innehaveren av kortet.

Bruken av fingeravtrykk er ment å skulle være frivillig. De som ikke kan eller vil benytte fingeravtrykk, skal benytte adgangskort kombinert med PIN-kode. Etter Datatilsynets oppfatning taler dette for at klager faktisk har vurdert det slik denne løsningen gir tilstrekkelig sikkerhet.

Godkjenning i andre land

Datatilsynet vil bemerke at de nasjonale tilsynsorganene i Belgia og Nederland på forespørsel har opplyst at de har mottatt melding om Exxon Mobiles planlagte løsning med fingeravtrykk i adgangskontrollen. Det er imidlertid ikke gitt tillatelse til denne bruken, slik som det fremgår i brev fra klager av 14. oktober 2005. Svar fra tilsynsorganene vedlegges saken.

4. Konklusjon

På bakgrunn av de ovennevnte vurderinger, kan ikke Datatilsynet se at det foreligger grunnlag for å endre vedtaket av 16. februar 2006. Klagen oversendes derfor Personvernnemnda for behandling.

Med hilsen

Knut B. Kaspersen
avdelingsdirektør

Astrid Flesland
seniorrådgiver

Kopi: Esso Norge as

Vedlegg: Kopi av sakens dokumenter
E-post fra Belgia
E-post fra Nederland
Internt notat/referat fra befaring

Datatilsynet

Personvernnemnda
Postboks 4594 Nydalen

0404 OSLO

Deres ref. Vår ref. (bes oppgitt ved svar)
05/01556-9 /AFL 25. august 2006

OVERSENDER SAK - FINGERAVTRYKK - OSLO TRIMSENTER

Datatilsynet fattet 7. mars 2006 vedtak med følgende ordlyd:

> Oslo Trimsenter AS må avslutte enhver bruk av fingeravtrykk eller andre biometriske kjennetegn i forbindelse med adgangskontroll.

Klager fikk utsatt klagefristen grunnet ferie. Klagen av 7. april 2006 stemplet inn hos Datatilsynet 18. april 2006 anses å være rettidig. Datatilsynet beklager svært lang saksbehandlingstid som skyldes behov for grundig utredning av saken samt ferieavvikling.

Datatilsynet har vurdert klagen, men finner ikke grunn til å omgjøre vedtaket. Saken oversendes derfor til Personvernnemnda jf. personopplysningslovens § 42, fjerde ledd.

1. Sakens gang

Datatilsynet mottok i høsten 2005 informasjon om at Oslo Trimsenter benyttet fingeravtrykk i tilknytning til adgangskontroll. I brev datert 24. november 2005 ber Datatilsynet om en redegjørelse fra Oslo Trimsenter. I brev datert 5. desember 2005 gir Oslo Trimsenter en kort redegjørelse for den valgte løsning for fingeravtrykkskontroll, herunder formål og behandlingsgrunnlag. I brev av 12. desember 2005 ber Datatilsynet om utfyllende opplysninger, bl.a. med hensyn til mulige alternative løsninger. Oslo Trimsenter fikk frist til 1. januar 2006 med sitt svar. 3. februar 2006 ble det sendt purring og varsel om vedtak med ny frist til 20. februar 2006. 7. mars fattet Datatilsynet vedtak om pålegg. Pålegget er påklaget i brev av 7. april 2006.

2. Faktum om løsningen

Klager benytter fingeravtrykk i tilknytning til adgangskontrollen ved treningssenteret. Løsningen heter IdentX. Ved første gangs registrering blir personalia, bilde og fingeravtrykk registrert i treningssenterets database. Databasen krever passord og personalet er pålagt taushetsplikt med hensyn til personopplysninger.

Om IdentX er det opplyst at løsningen er utviklet for identifisering av oppføringer/personer i en database. Det benyttes en template som er utviklet på grunnlag av fingeravtrykket. Når personene skal identifiseres i databasen gjøres det et todelt søk. Kunde-id returneres fra databasen. Det er videre opplyst at selve bildet (innskanningen) av fingeravtrykket ikke lagres og heller ikke benyttes til identifisering.

Det er opplyst at det ikke er mulig å reversere prosessen for å fremstille et bilde av fingeravtrykket, og at det vil kreve full tilgang til databaseløsningen og direkte adgang til kildekodene dersom en lagret template skal kunne benyttes til noe annet enn løsningen med IdentX.

Klager opplyser videre at IdentX kan benytte og kommunisere med mange ulike sensorer for fremstilling av template. Vanligvis benyttes U.are.U 4000B, som er en optisk sensor. Felles for sensorene er at de ikke inneholder minne og at det derfor ikke er noen personvernrisiko knyttet til om en sensor skulle komme på avveie.

Det er frivillig å benytte løsningen. De som ikke ønsker å avgi fingeravtrykk blir logget inn manuelt ved hvert besøk. Av ca. 500 medlemmer opplyses det at kun to personer ikke har samtykket til bruk av fingeravtrykk.

Det er opplyst at fingeravtrykk slettes fortløpende når medlemskap utgår.

3. Klagers anførsler

Klager anfører at tidligere ordninger med medlemskort har medført for dårlig kontroll på gyldig betalt medlemskap fordi medlemskortene blir manipulert ved at kortet overdras til andre, bildet byttes ut eller utløpsdato blir endret. Det er også anført at ordningen er meget effektiv fordi innsjekkingen ved besøk tar liten tid.

Klager anfører at man også har et ønske om å registrere hvor mange som er i lokalene til enhver tid for bedre utnyttelse av aktiviteter.

Klager anfører at personopplysningene er godt nok sikret med den valgte løsningen. Det vises til at faren for at en template kommer på avveie er ekstremt liten.

4. Datatilsynets vurdering

Datatilsynet anser at fingeravtrykk, også når dette benyttes til å utarbeide en ”template” er å anse som et entydig identifikasjonsmiddel. Fingeravtrykk kan etter dette bare benyttes når dette er tillatt etter personopplysningslovens § 12. Paragrafen stiller som vilkår for bruken at:

1. Det er saklig behov for sikker identifisering og
2. Metoden er nødvendig for å oppnå slik identifisering.

Vilkårene er kumulative.

Datatilsynet viser i denne anledning til notat om endring av personopplysningslovens § 12 som er oversendt Justisdepartementet og som følger som vedlegg til denne saken.

Datatilsynet viser også til den nærmere redegjørelsen for tilsynets tolkning av personopplysningslovens § 12 som er gitt i samlet oversendelsesbrev til personvernnemnda.

Datatilsynet finner at ordet ”identifisering” skal tolkes strengt, slik at bruk av entydige identifikasjonsmidler som legitimasjon eller i tilknytning til verifisering av identitet/autentisering, ikke er tillatt.

Saklig behov for sikker identifisering
Datatilsynet finner at det kan sies å foreligge et saklig behov for sikker identifisering i tilknytning til adgangskontrollen, slik at betalende medlemmer blir identifisert.

Det er ikke gitt noen beskrivelse av om fingeravtrykke benyttes alene i adgangskontrollen eller om man i tillegg fortsatt benytter et medlemskort. Det kan ikke utelukkes at fingeravtrykket blir benyttet i tilknytning til identifisering dersom dette alene gir adgang til treningssentrert. Dersom det derimot benyttes sammen med medlemskort, er det Datatilsynets vurdering av fingeravtrykket benyttes for å verifisere identiteten og ikke til identifisering slik § 12 krever. Datatilsynet har ikke funnet grunn til å innhente ytterligere informasjon i forhold til dette, da det neste vilkåret uansett ikke anses oppfylt.

Metoden er nødvendig for å oppnå slik identifisering.
Det er Datatilsynets oppfatning at lovens krav til nødvendighet ikke er oppfylt.

Det er klart uttalt i forarbeidene at entydige identifikasjonsmidler ikke skal brukes i utrengsmål. Det følger av dette at nødvendighetsvurderingen bør være streng. I Ot. Prp. Nr. 92 Om behandling av personopplysninger s. 114 uttales følgende: *”Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f eks navn, adresse og kundenummer ikke er tilstrekkelig. Det vil også ha betydning hvor viktig identifiseringen er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt.”*

Datatilsynet finner at fingeravtrykk ikke er nødvendig for sikker identifisering i tilknytning til adgangskontroll på treningssentre. Datatilsynet finner at kontroll av meldemskort opp mot registrert personalia, eventuelt bruk av medlemskort kombinert med en PIN eller et passord gir tilstrekkelig sikker identifisering.

Klagers anførsler om at medlemskort blir manipulert er ikke nok til at bruk av fingeravtrykk kan anses som nødvendig. Det vil være et langt mindre personvernkrenkende inngrep dersom man sørger for at medlemskortene ble vanskeligere å manipulere. Datatilsynet legger til grunn at det finnes virksomheter som kan bistå i denne anledning. Datatilsynet finner for øvrig at manipulasjon av bilde bør kunne avdekkes gjennom visuell kontroll og kontroll mot fotografi i database.

Datatilsynet vil bemerke at de økonomiske verdier som står på spill ved at enkelte medlemmer forfalsker sitt medlemskort må anses som begrenset, og at innføring av fingeravtrykkskontroll fremstår som et uproporsjonalt inngrep.

Oversikt av antall personer som er i lokalet kan man oppnå ved innføring av "telleport", adgangsprotokoll eller manuell telling.

5. Konklusjon

På bakgrunn av de ovennevnte vurderinger, kan ikke Datatilsynet se at det foreligger grunnlag for å endre vedtaket av 10. april 2006. Klagen oversendes derfor til Personvernnemnda for behandling.

Datatilsynet gjør oppmerksom på at virksomheten benytter samme løsning som Oxigeno Fitness som også har påklaget et vedtak til Personvernnemnda. Det kan være fordelaktig om Personvernnemnda ser det to sakene i sammenheng.

Med hilsen

Knut B. Kaspersen
avdelingsdirektør

Astrid Flesland
seniorrådgiver

Kopi: Oslo Trimsenter, Munchsgt 7, 0165 OSLO
Vedlegg: Sakens dokumenter

Datatilsynet

Personvernnemnda
Postboks 4594 Nydalen

0404 OSLO

Deres ref. Vår ref. (bes oppgitt ved svar)
06/00083-6 /AFL 24. aug. 2006

OVERSENDER SAK – FINGERAVTRYKK – OXIGENO FITNESS

Datatilsynet fattet 28. april 2006 vedtak med følgende ordlyd:

> Oxigeno Fitness må straks avslutte enhver bruk av fingeravtrykk i forbindelse med adgangskontroll.

Klagen datert 19 mai 2006 er registrert inn hos Datatilsynet 1. juni 2006. Datatilsynet legger til grunn at klagen er rettidig jf. forvaltningslovens § 30, 1. pkt. Det vises i denne anledning til at fristen gikk over en periode med en rekke offisielle fridager, og at også registreringen hos Datatilsynet av denne grunn kan ha vært noe sen.

Datatilsynet beklager svært lang saksbehandlingstid som skyldes behov for grundig utredning av saken samt ferieavvikling.

Datatilsynet har vurdert klagen, men finner ikke grunn til å omgjøre vedtaket. Saken oversendes derfor til Personvernnemnda jf. personopplysningslovens § 42, fjerde ledd.

1. Sakens gang

Datatilsynet mottok tidlig i 2006 en del spørsmål knyttet til bruk av fingeravtrykk ved treningssenteret Oxigeno Fitness i Oslo. På bakgrunn av disse spørsmålene ble det rettet en henvendelse til Oxigeno Fitness 23. januar 2006. Det ble gitt generell informasjon om tolkningen av personopplysningsloven § 12. I tillegg ba Datatilsynet om en redegjørelse for hvordan Oxigeno Fitness oppfylte vilkårene i denne paragrafen. Selskapet ble gitt frist for svar til 6. februar 2006. Det kom ikke noen tilbakemelding, og saken ble purret i brev av 8. mars 2006. I samme brev ble det varslet om vedtak om at bruken av fingeravtrykk måtte avsluttes. Ny frist ble satt til 24. mars 2006. I brev datert 23. mars redegjør Oxigeno Fitness for bruken av fingeravtrykk. Som vedlegg til redegjørelsen fulgte en beskrivelse av den valgte løsningen, samt et eksemplar av virksomhetens kundeavtale. I brev av 18. april 2006 fattet Datatilsynet vedtak om at bruken av fingeravtrykk måtte opphøre. Vedtaket er påklaget i brev av 19. mai 2006. Klager ber om oppsettende virkning til 12. juli 2006 når nytt system vil være på plass.

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

2. Behandlingsansvarlig – vedtakets gyldighet

Behandlingsansvarlig defineres i pol § 2 nr 4 som: *"den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes"*

Det følger av forarbeidene til personopplysningsloven (Ot prp nr 92 1998-99) s 102-103, at den behandlingsansvarlige er den som alene eller sammen med andre har bestemmelsesrett over personopplysningene og den elektroniske behandlingen av disse. Der den behandlingsansvarlige er en juridisk person, vil den juridiske personen representert ved dens ledelse være behandlingsansvarlig. Ledelsen må sørge for at loven etterleves og som ledd i dette foreta en intern arbeidsfordeling slik at det er klart hvilken stilling det ligger til å sørge for at loven etterleves i praksis. Funksjonen bør knyttes til en lederstilling slik at stillingsinnehaveren har reell daglig innflytelse på behandlingene som foretas. Behandlingsansvarlig kan bare den være som har sivilprosessuell partsevne, dvs. den som kan opptre som saksøkt i en tvist for domstolene.

Datatilsynets brev av 23. januar 2006 samt varsel om vedtak datert 8. mars 2006 er rettet mot Oxigeno Fitness v/daglig leder. Ved en inkurie er vedtaket kun rettet mot Oxigeno Fitness. Imidlertid har vedtaket åpenbart kommet frem til Rune S. Henrichsen på linje med de andre brevene, i det han har påklaget saken innen utløpet av fristen.

På Oxigenos brevark fremgår det at Oxigeno er et merkenavn under Gymmet AS. I Foretaksregisteret står Rune S. Henrichsen oppført som kontaktperson for Gymmet AS. I brev av 23. mars 2006 opplyser Rune S. Henrichsen at han er eier og daglig leder av senteret. Oxigeno Fitness er ikke registrert i Enhetsregisteret. Virksomheten har ikke på noe tidspunkt hevdet at vedtaket eller de øvrige brevene er rettet mot feil virksomhet eller person.

Datatilsynet finner etter dette at vedtaket er stilt til feil virksomhet, da behandlingsansvarlige er Gymmet AS, men at det likevel har kommet frem til rett virksomhet og person. Feilen har ikke vært bestemmende for vedtakets innhold, og den behandlingsansvarlige har hatt like god anledning til å ivareta sine rettigheter som om vedtaket hadde vært stilt til Gymmet AS v/Rune S. Henrichsen. Datatilsynet finner dermed at feilen er ubetydelig og at den ikke medfører at vedtaket som sådan må anses som ugyldig jf. forvaltningsloven (fvl.) § 41.

3. Utsatt iverksetting av vedtak

Klager opplyser at ny løsning skal være på plass 12. juli 2006, og ber om oppsettende virkning på vedtaket til den datoen. Tidspunktet er passert.
Datatilsynet har vurdert spørsmålet jf. fvl. § 42 og finner at det ikke lenger er grunn til å gi vedtaket oppsettende virkning.

4. Faktum om løsningen

Klager benytter IdentX. Løsningen er beskrevet i vedlegg til dokument 3 i saken. Det fremheves i denne beskrivelsen at fingeravtrykket benyttes som identifikator.

Man utformer en template på bakgrunn av fingeravtrykket som lagres i lokal database. Når personene skal identifiseres i databasen gjøres det et todelt søk. Kunde-id returneres fra databasen. Det er videre opplyst at selve bildet (innskanningen) av fingeravtrykket ikke lagres og heller ikke benyttes til identifisering.

Det er opplyst at det ikke er mulig å reversere prosessen for å fremstille et bilde av fingeravtrykket, og at det vil kreve full tilgang til databaseløsningen og direkte adgang til kildekodene dersom en lagret template skal kunne benyttes til noe annet enn løsningen med IdentX.

Klager opplyser videre at IdentX kan benytte og kommunisere med mange ulike sensorer for fremstilling av template. Vanligvis benyttes U.are.U 4000B, som er en optisk sensor. Felles for sensorene er at de ikke inneholder minne og at det derfor ikke er noen personvernrisiko knyttet til om en sensor skulle komme på avveie.

Det fremgår av kundeavtalen at fingeravtrykksløsningen benyttes i adgangskontroll. Klager opplyser at alle kunder foretrekker denne løsningen. Dersom den tekniske løsningen svikter, tastes kunden inn manuelt. I klagen er det opplyst at registreringen er frivillig.

5. Klagers anførsler

I det følgende gis en sammenfatning av klagers anførsler slik disse er fremkommet i brev av 23. mars 2006 samt klage av 19. mai 2006.

Klager opplyser at på tross av ca. 1800 medlemmer har man ikke mottatt klager på fingeravtrykksløsningen. Det opplyses at kundene er fornøyd og at løsningen fungerer bra.

Med en så stor medlemsmasse er det et sterkt behov å kunne vite til enhver tid hvem som er i bygget i forhold til personlig sikkerhet, brann sykdom etc. I tillegg er det viktig å sikre at de personer som er medlem har gyldig medlemskap. Dette gjøres ved innsjekking i resepsjonen. På denne måten forebygges misbruk av personlig medlemskap.

Det er videre anført at Datatilsynets vedtak er totalt umoderne og at en vanskelig kan se logikken og grunnlaget for vedtaket i den sammenhengen virksomheten benytter fingeravtrykk.

6. Datatilsynets vurdering

Datatilsynet vil innledningsvis bemerke at første kontakt mellom Oxigeno Fitness og Datatilsynet ble opprettet på bakgrunn av informasjon Datatilsynet mottok om bruken av fingeravtrykk og spørsmål rundt lovligheten av dette. Det kan dermed ikke avvises at det kan være medlemmer som oppfatter bruken av fingeravtrykk som uheldig og ubehagelig, selv om dette ikke har kommet til uttrykk direkte overfor de ansatte ved treningssenteret som en klage.

Datatilsynet anser at fingeravtrykk, også når dette benyttes til å utarbeide en ”template” er å anse som et entydig identifikasjonsmiddel. Fingeravtrykk kan etter dette bare benyttes nå dette er tillatt etter personopplysningslovens § 12. Paragrafen stiller som vilkår for bruken at:

1. Det er saklig behov for sikker identifisering og
2. Metoden er nødvendig for å oppnå slik identifisering.

Vilkårene er kumulative.

Datatilsynet viser i denne anledning til notat om endring av personopplysningslovens § 12 som er oversendt til Justisdepartementet og som følger i kopi til denne saken. Datatilsynet viser også til den nærmere redegjørelsen for tilsynets tolkning av personopplysningslovens § 12 som er gitt i samlet oversendelsesbrev til Personvernnemnda.

Datatilsynet finner at ordet ”identifisering” skal tolkes strengt, slik at bruk av entydige identifikasjonsmidler som legitimasjon eller i tilknytning til verifisering av identitet/autentisering, ikke er tillatt

Saklig behov for sikker identifisering

Datatilsynet finner at det kan sies å foreligge et saklig behov for sikker identifisering i tilknytning til adgangskontrollen, slik at betalende medlemmer blir identifisert.

I det fingeravtrykket benyttes alene og en av funksjonene i systemet er å kontrollere om medlemskapet er gyldig, legger Datatilsynet til grunn at fingeravtrykket benyttes i identifiseringsøyemed.

Metoden er nødvendig for å oppnå slik identifisering.

Det er Data tilsynets oppfatning om at lovens krav til nødvendighet ikke er oppfylt.

Det er klart uttalt i forarbeidene at entydige identifikasjonsmidler ikke skal brukes i utrengsmål. Det følger av dette at nødvendighetsvurderingen bør være streng. I Ot. Prp. Nr. 92 Om behandling av personopplysninger s. 114 uttales følgende: *”Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f eks navn, adresse og kundenummer ikke er tilstrekkelig. Det vil også ha betydning hvor viktig identifiseringen er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt.”*

Datatilsynet finner at fingeravtrykk ikke er nødvendig for sikker identifisering i tilknytning til adgangskontroll på treningssentre. Datatilsynet finner at kontroll av meldemskort opp mot registrert personalia, eventuelt bruk av medlemskort kombinert med en PIN eller et passord gir tilstrekkelig sikker identifisering.

Datatilsynet ser at det kan fremstå som praktisk både for kundene og virksomheten å benytte fingeravtrykk benyttes i stedet for kort. Dette er imidlertid ikke tilstrekkelig til å fastslå at metoden er nødvendig for sikker identifisering.

Datatilsynet vil bemerke at de økonomiske verdier som står på spill ved at enkelte medlemmer mister sitt medlemskort eller misbruker sitt medlemskap må anses som begrenset, og at innføring av fingeravtrykkskontroll fremstår som et uproporsjonalt inngrep.

Oversikt av antall personer som er i lokalet kan man oppnå ved innføring av "telleport", adgangsprotokoll eller manuell telling.

7. Konklusjon

På bakgrunn av de ovennevnte vurderinger, kan ikke Datatilsynet se at det foreligger grunnlag for å endre vedtaket av 10. april 2006. Klagen oversendes derfor til Personvernnemnda for behandling.

Datatilsynet gjør oppmerksom på at klager benytter samme løsning som Oslo Trimsenter AS som også har påklaget et vedtak til Personvernnemnda. Det kan være en fordel om Personvernnemnda ser de to sakene i sammenheng

Med hilsen

Knut B. Kaspersen
avdelingsdirektør

Astrid Flesland
seniorrådgiver

Vedlegg: Sakens dokumenter
Utskrift fra Enhetsregisteret

Kopi: Gymmet AS, v/Rune S. Henrichsen, Fredriksborgveien 38, 0286 OSLO
Oxigeno Fitness v/Rune S. Henrichsen, Maridalsveien 17, 0175 Oslo

Datatilsynet

Personvernnemnda
Postboks 4594 Nydalen

0404 OSLO

Deres ref. Vår ref. (bes oppgitt ved svar)
06/00180-7 /AFL 25. august 2006

OVERSENDELSE AV SAK - REMA 1000 – FINGERAVTRYKK

Datatilsynet fattet 10. april 2006 vedtak med følgende ordlyd:

> REMA 1000 må straks avslutte enhver bruk av fingeravtrykk i forbindelse med timeregistrering for de ansatte.

Klager fikk utsatt klagefristen til 18 mai 2006. Datatilsynet mottok 19 mai 2006 klagen som er datert 18. mai 2006. Datatilsynet legger til grunn at klagen er rettidig jf. forvaltningslovens § 30, 1. pkt. Datatilsynet beklager svært lang saksbehandlingstid som skyldes behov for grundig utredning av saken samt ferieavvikling.

Datatilsynet har vurdert klagen, men finner ikke grunn til å omgjøre vedtaket. Saken oversendes derfor til Personvernnemnda jf. personopplysningslovens § 42, fjerde ledd.

1. Sakens gang

Datatilsynet mottok tidlig i 2006 en del spørsmål fra ansatte i REMA 1000 knyttet til selskapets bruk/planlagte bruk av fingeravtrykk. På bakgrunn av disse spørsmålene blir det 16. februar 2006 sendt et brev til REMA 1000. Brevet redegjør kort for personopplysningslovens § 12. Samtidig ber Datatilsynet om å få selskapets redegjørelse for eventuell planlagt bruk av fingeravtrykk.

I brev av 6. mars 2006 redegjør kjeden for en igangsatt innføring av en timeregistreringsterminal som innebærer bruk av fingeravtrykk til verifikasjon av den ansattes identitet. Datatilsynet fatter 10. april 2006 pålegg om at bruken av fingeravtrykk må opphøre. I brev av 9. mai 2006 bekrefter REMA 1000 at bruken av fingeravtrykk er opphørt. I brev av 18. mai 2006 påklages Datatilsynets vedtak i saken.

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

2. Faktum om løsningen

Klager benytter systemet KRONOS 4500 som leveres av Time Nordic AS. Det genereres en template fra fingeravtrykket som lagres lokalt i terminalen. Registrering i terminalen skjer ved at den ansatte taster sitt ansattnummer/ID-nummer. Deretter blir vedkommende bedt om å legge en finger på leseplaten/sensoren for å verifisere at det er tastet riktig nummer.

Det er opplyst at tidsterminalen og fingeravtrykket ikke kan benyttes til noen form for adgangskontroll. Datatilsynet tolker dette slik at løsningen ikke samtidig benyttes som døråpner inn til adgangsregulerte områder.

3. Klagers anførsler

I det følgende gis en sammenfatning av klagers anførsler slik disse er fremkommet i brev av 6. mars 2006 samt klage av 18. mai 2006.

Formålet med løsningen opplyses å være "å forenkle det administrative arbeidet for kjøpmennene knyttet til butikkens bemanningsplaner og utbetaling av lønn, herunder sikre at det utbetales korrekt lønn."

Klager anfører at grunnlaget for behandlingen er å finne i personopplysningslovens § 8 a eller alternativt i § 8 f. Videre anføres at det er behov for sikker identifikasjon jf. § 12 av når den ansatte er på jobb for å foreta korrekt lønnsutbetaling. Alternativt må den enkelte kjøpmann selv registrere dette, noe som er vanskelig fordi kjøpmannen ikke er tilstede i hele åpningstiden. I tillegg er det anført at fingeravtrykk er nødvendig fordi det er mange ansatte, opptil 50 i hver butikk, og at det er et omfattende arbeid å holde oversikt over hvem som faktisk er på jobb til enhver tid i forhold til de oppsatte planene, og dermed også hvor mye lønn den enkelte medarbeider har opparbeidet. Klager anser at slik manuell registrering ikke er i samsvar med moderne butikkdrift.

Klager anfører at det foreligger saklig behov for å benytte fingeravtrykk og at metoden er nødvendig for å oppnå sikker identifisering. Klager viser til at det ikke foreligger noe skille mellom identifisering og verifisering, da poenget med bruken av fingeravtrykk utelukkende er å sikre at identifikasjonen er korrekt, med andre ord å sørge for sikker identifisering. Klager anser at bruk av fingeravtrykk gir sikker identifisering. Det anføres at det ikke kan telle negativt i forhold til denne vurderingen at det valgte system også har andre administrative funksjoner, og at man alternativt kan løse disse funksjonene ved hjelp av andre systemer som ikke bruker fingeravtrykk som identifikasjonsmiddel.

Klager anfører at bruk av kode eller kort medfører at registreringene ikke nødvendigvis er korrekt, fordi et slikt system åpner for så vel utilsiktede som tilsiktede feilregistreringer. Det fremheves at feiltasting kan medføre at ansatte får utbetalt feil lønn, fordi det blir registrert for kort eller for lang arbeidstid. Klager viser også til erfaring med at ansatte benytter hverandres koder og stemplingskort, og at man derfor ikke får korrekte data om hvem som har vært på jobb. Klager trekker også frem at kort

har den ulempe at de ansatte relativt ofte mister eller glemmer kortet, og at det kan bli ødelagt.

Klager anfører at Datatilsynet tar feil når det hevdes at lovens krav til nødvendighet medfører et krev om at andre metoder ikke gir tilstrekkelig grad av identifisering. Det anføres at REMA 1000 kun kan akseptere helt sporadiske feilregistreringer. Det anføres videre at loven ikke kvalifiserer i hvor stor utstrekning det skal være nødvendig med bruk av "andre entydige identifikasjonsmidler". Hvis bruk av fingeravtrykk er nødvendig for sikker identifisering og dermed korrekt data, i et ikke ubetydelig antall tilfeller, anser REMA 1000 at lovens vilkår bør være oppfylt. Det vises i denne anledning til de økonomiske konsekvenser av feilregistreringer.

Klager anfører at det er i alle parters interesse at det blir betalt ut korrekt lønn. Klager kan for øvrig ikke se at det er problematisk i forhold til de ansattes personvern at det benyttes fingeravtrykk, og at det med den valgte metode ikke er noen fare for at opplysningen kommer på avveie. Det vises til at alle krav i personopplysningslovens § 11 ivaretas gjennom systemet. Det vises til at man kun benytter en binærkode av fingeravtrykket, som kun lagres i den lokale terminalen og at det ikke skal være mulig å gjenskape fingeravtrykk på basis av denne. Det opplyses at koden ikke skal overføres i nettverk og at sannsynligheten for at den kommer på avveie er liten.

4. Datatilsynets vurdering

Datatilsynet anser at fingeravtrykk, også når dette benyttes til å utarbeide en "template" er å anse som et entydig identifikasjonsmiddel. Fingeravtrykk/template kan etter dette bar benyttes når dette er tillatt etter personopplysningslovens § 12. Paragrafen stiller som vilkår for bruken at:

1. Det er saklig behov for sikker identifisering og
2. Metoden er nødvendig for å oppnå slik identifisering.

Vilkårene er kumulative.

Datatilsynet viser i denne anledning til notat om endring av personopplysningslovens § 12 som er oversendt Justisdepartementet og som følger som vedlegg til denne saken. Datatilsynet viser også til den nærmere redegjørelsen for tilsynets tolkning av personopplysningslovens § 12 som er gitt i samlet oversendelsesbrev til Personvernnemnda.

Datatilsynet finner at ordet "identifisering skal tolkes strengt, slik at bruken av entydige identifikasjonsmidler som legitimasjon eller i tilknytning til verifisering av identitet/autentisering, ikke er tillatt.

<u>Saklig behov for sikker identifisering</u>

Datatilsynet er ikke uenig i at REMA 1000 har et saklig behov for å sikre at lønn føres korrekt. Tilsynet er imidlertid av den oppfatning at fingeravtrykket ikke benyttes for sikker identifisering slik dette er formulert i personopplysningslovens § 12. Det er opplyst at den ansatte skal benytte en ansattkode /ID-nummer i tillegg til

fingeravtrykk. Datatilsynet oppfatter det slik at identifiseringen skjer ved hjelp av denne ansatskoden/ID-nummeret, mens fingeravtrykket fungerer som legitimasjon eller verifisering av påstått identitet i systemet. Datatilsynets oppfatning er at formålet med personopplysningslovens § 12 nettopp er å forhindre slik bruk av entydige identifikasjonsmidler.

Metoden er nødvendig for å oppnå slik identifisering.
Det er Datatilsynets oppfatning at heller ikke lovens krav til nødvendighet er oppfylt.

Det er klart uttalt i forarbeidene at entydige identifikasjonsmidler ikke skal brukes i utrengsmål. Det følger av dette at nødvendighetsvurderingen bør være streng. I Ot. Prp. Nr. 92 Om behandling av personopplysninger s. 114 uttales følgende: *"Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f eks navn, adresse og kundenummer ikke er tilstrekkelig. Det vil også ha betydning hvor viktig identifiseringen er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt."*

Datatilsynet finner at man kan oppnå tilstrekkelig sikker identifisering sett hen til formålet, ved å benytte ansattnummer/ID-nummer i kombinasjon med en personlig kode eller passord. Tilsynet erkjenner at det vil kunne skje at PIN eller passord kommer på avveie med eller uten den ansattes vilje. Datatilsynet finner imidlertid ikke at det er grunnlag for å si at et større antall med hensikt ansatte vil svindle til seg lønn gjennom misbruk av PIN eller passord, og antar at dette skjer kun sporadisk. Selv om samfunnet er tjent med at svindel bekjempes, fremstår bruk av fingeravtrykk verken som nødvendig eller forholdsmessig i denne anledning.

Hva gjelder feiltastinger legger Datatilsynet til grunn at dette antagelig skjer noe oftere, men at hver enkelt ansatt er forpliktet til å kontrollere sin lønnsutbetaling og gi tilbakemelding dersom det er oppstått feil. På denne bakgrunn finner Datatilsynet at konsekvensen av feiltasting ikke får stor eller langvarig konsekvens for den registrerte. Slike feiltastinger anses heller ikke å ha stor konsekvens verken for arbeidsgiver (de vil som oftest bli korrigert i løpet av noen tid) eller samfunnet for øvrig.

Det er anført at fingeravtrykkskontroll er nødvendig fordi manuell kontroll er for ressurskrevende og umoderne og at arbeidsgiver ikke er tilstede i hele åpningstiden, slik at manuell kontroll er umulig. Datatilsynet vil bemerke at det faktum at arbeidsgiver ikke er tilstede i hele arbeidstiden ikke anses tilstrekkelig for å oppfylle nødvendighetskriteriet. En enkel måte å løse dette på er å delegere ansvaret til andre, slik at det alltid er en ansvarlig tilstede i åpningstiden. Hva gjelder ressursforbruket vil Datatilsynet bemerke at tilsynet ikke anser at 50 ansatte utgjør en slik stor arbeidsplass at manuelt oppsyn med hvem som er tilstede er uforholdsmessig vanskelig å gjennomføre.

5. Konklusjon

På bakgrunn av de ovennevnte vurderinger, kan ikke Datatilsynet se at det foreligger grunnlag for å endre vedtaket av 10. april 2006. Klagen oversendes derfor til Personvernnemnda for behandling.

Med hilsen

Knut B. Kaspersen
avdelingsdirektør

Astrid Flesland
seniorrådgiver

Vedlegg: Sakens dokumenter

Kopi: KLUGE Advokatfirma DA, v/I. Mestad, Pb. 1548 Vika, 0117 Oslo
REMA 1000 AS, Postboks 6428 Etterstad, 0605 OSLO