Datatilsynet

Personvernnemnda
Postboks 4594 Nydalen
0404 OSLO

Deres ref. | Vår ref. (bes oppgitt ved svar) 06/00047-17 /AFL | 25. august 2006

OVERSENDER KLAGE – TYSVÆR KOMMUNE - BRUK AV FINGERAVTRYKK

Datatilsynet fattet 10. juli 2006 følgende vedtak:

> Tysvær kommune må avslutte enhver bruk av fingeravtrykk i tilknytning til pålogging av datasystem.

Vedtaket ble påklaget i brev datert 2. august 2006. Klagen er rettidig.

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

1. Diverse innledende problemstillinger

Datatilsynet har notert at klager ønsket at saken skulle bli direkte ekspedert til Personvernnemnda fordi klagen ikke inneholder nye opplysninger og at klager også har sendt klagen direkte til Personvernnemnda. Tilsynet vil kort bemerke at det følger av forvaltningslovens (fvl.) § 32, første ledd a, at klager skal fremsettes overfor det forvaltningsorgan som har truffet vedtaket. Det følger videre av fvl. § 33 at underinstansen skal foreta de undersøkelser klagen gir grunn til. Videre at underinstansen kan oppheve eller endre vedtaket dersom den finner klagen begrunnet. Det er Datatilsynets oppfatning at det ville utgjøre en saksbehandlingsfeil dersom saken ikke ble gjort til gjenstand for ny vurdering i tilsynet før oversendelse til Personvernnemnda. Datatilsynet tar sterkt avstand fra klagers påstander om ubegrunnet trenering av saken.

Datatilsynet kan ikke se at det utgjør noen saksbehandlingsfeil at det er sendt et brev til Stortinget i sakens anledning. Datatilsynet finner at det var grunn til å undersøke om Stortinget benyttet fingeravtrykk, da opplysningen synes å være gitt som et argument for at bruk av fingeravtrykksløsningene må være lovlig. Stortingets svar følger vedlagt. Denne informasjonsutvekslingen har ikke medført lenger saksbehandlingstid.

Datatilsynet vil bemerke at, i den grad det skal anses som en saksbehandlingsfeil at Datatilsynet ikke kontaktet Stortinget om den påståtte bruk av fingeravtrykk når slike opplysninger første gang ble fremmet for Datatilsynet i brev av 19. mai 2006, så er denne feilen rettet opp gjennom vår henvendelse til Stortinget av 14. august 2006.

Datatilsynet ser at det i klagen opplyses at det er mulig at det vil bli sendt et brev direkte til Personvernnemnda fra Kommunenes Sentralforbund (KS) og at KS må ha rettslig klageinteresse i saken. Datatilsynet har bedt klager om eventuelt å få kopi av dette brevet. Advokat Kyrre Eggen har i e-post av 18. august 2006 opplyst at KS fortsatt ikke har tatt standpunkt til om de skal gi uttalelse i saken. På denne bakgrunn finner Datatilsynet at det kan overlates til Personvernnemnda å ta stilling til eventuell klageinteresse for KS dersom de klager.

Advokat Kyrre Eggen har tidligere hatt en stilling ved Institutt for rettsinformatikk under Personvernnemndas leder, Jon Bing. Datatilsynet finner ikke grunnlag for å stille spørsmål ved Personvernnemndas habilitet som følge av dette.

2. Utsatt iverksetting av vedtak

Klager har bedt om at vedtaket ikke iverksettes før klagen er ferdig behandlet hos Personvernnemnda. Datatilsynet har vurdert dette jf. fvl. § 42.

Datatilsynets vedtak er knyttet til den aktuelle bruken av fingeravtrykksløsningen. Klager kan fortsatt benytte datautstyret, men må opprette en annen løsning for pålogging.

Datatilsynet kan ikke se at vedtaket som sådan er til hinder for innkjøp av utstyr eller videre planlegging av slike innkjøp. I og med at det foreligger en klage, er det knyttet noe usikkerhet til om man etter at klagen er ferdig behandlet kan benytte fingeravtrykksløsningen eller ikke. Denne usikkerheten er imidlertid like stor selv om man tillates å benytte fingeravtrykk i tiden frem til klagen er ferdig behandlet. Datatilsynet har derfor funnet at det har mindre betydning for klager om klagen gis utsatt iverksetting og at vedtaket er lite byrdefullt å gjennomføre. Datatilsynet finner etter dette at det ikke er grunnlag for å etterkomme klagers ønske om utsatt iverksetting av vedtaket.

3. Sakens gang:

Datatilsynet mottar 20. desember 2005 en e-post fra Tysvær kommune vedlagt kommunenes IT-reglement. I IT-reglementets pkt. 5.10. tredje avsnitt fremgår det at sensitiv informasjon ikke må lagres uten at dette er klarert med IT-kontoret og *"gjort i samsvar med Datatilsynet sine retningslinjer med biometrisk tilgangskontroll, kryptering av harddisk og andre tryggleikstiltak"*. I e-post av 9. januar 2006 spør Datatilsynet om kommunen benytter biometrisk tilgangskontroll, eventuelt til hva, hvordan og om personopplysningslovens § 12 er vurdert.

I e-post av 9. januar bekrefter kommunen at de benytter biometrisk tilgangskontroll på alle nye bærbare PCer, og også på noen stasjonære maskiner. I e-post av 7. februar ber

Datatilsynet om mer presise svar på 5 konkrete spørsmål knyttet til bruken av fingeravtrykk. Kommunens svar gis i e-post av samme dato. I brev av 7. mars 2006 varsler Datatilsynet vedtak om at bruk av fingeravtrykk må opphøre. Frist for eventuelle bemerkninger til det varslede vedtak settes til 3. mai 2006. Fristen blir på forespørsel fra advokatfirmaet Wiersholm på vegne av kommunen utsatt først til 15. mai 2006 og deretter til 19. mai 2006.

I brev datert 19. mai gir advokatfirmaet Wiersholm bemerkninger til det varslede vedtaket på vegne av Tysvær kommune, samt Levono Technology B.V. Norway Branch, (Levono) som er leverandør av fingeravtrykkssystemet Tysvær kommune benytter.

I brev datert 10. juli 2006 fatter Datatilsynet vedtak om at kommunens bruk av fingeravtrykk må avsluttes innen 1. september 2006. Både Tysvær kommune og Levono har påklaget vedtaket i brev av 2. august 2006. Brevet er også sendt direkte til Personvernnemnda. I e-post av 4. august 2006 ber Datatilsynet om nærmere informasjon knyttet til opplysninger om at Stortinget benytter Levonos løsning med fingeravtrykk. I e-post av 7. august gir advokat Kyrre Eggen tilleggsinformasjon knyttet til dette. I brev av 14. august ber Datatilsynet om Stortingets kommentarer til opplysningene gitt av advokatfirmaet Wiersholm. I e-post av 15. august reagerer advokat Kyrre Eggen i Wiersholm på at Datatilsynet innhenter flere opplysninger og ber om at saken umiddelbart oversendes til Personvernnemnda. I e-post av 15. august 2006 ber Datatilsynet om at eventuell klage fra KS oversendes til Datatilsynet. I e-post av 18. august 2006 opplyser Advokat Kyrre Eggen at KS følger saken, men at det ikke er truffet beslutning om de kommer til å fremsette noen uttalelse i klagesaken. Advokaten ber samtidig om at klagen blir oversendt Personvernnemnda. I e-post av 21. august 2006 opplyser Datatilsynet at klagen vil bli oversendt etter ny vurdering hos Datatilsynet jf. fvl. § 33, andre ledd. I e-post av 21. august 2006 ber advokat Kyrre Eggen igjen om at saken blir oversendt til Personvernnemnda. Advokaten argumenterer for at Datatilsynet ikke skal gjøre noen ny vurdering av saken før oversendelse.

4. Klagers anførsler

I det følgende gis en sammenfatning av kommunen og Levonos anførsler, slik disse er uttrykt gjennom sakens dokumenter.

Biometrisk tilgangskontroll er enkelt i bruk. Brukeren trenger kun å dra fingeren en gang for å gi inn fire-fem passord, samtidig som harddisken er låst og kryptert når maskinen er avslått. Administratornivået er også låst for andre enn de som arbeider på IT-avdelingen. Brukeren kan ikke installere andre programmer enn de som er godkjent og lagt ut på en dertil egnet webside hvor brukerne selv med ett trykk kan installere programvaren. Dette medfører full lisenskontroll og også sikkerhet for at kun arbeidstakeren bruker maskinen og ingen andre. Samtidig gjør dette maskinen veldig brukervennlig.

Ved å bruke spesielle teknikker låses den bærbare maskinen til å bruke kommunens sikkerhetssystemer (brannmur, viruskontroll, SPAM filtrering, filtrering av uønsket innhold osv.) uansett hvor de er tilkoblet. Sikkerhetsregimet er så strengt at man kan oppbevare sensitive data også lokalt på bærbare maskiner, samt at brukeren kan ha tilgang på ressursene på jobb uansett hvor man måtte befinne seg ved hjelp av kryptert tunnellering (VPN). Løsningen sikrer at opplysninger ikke kommer på avveie selv om de ligger lagret på lokal harddisk.

De biometriske dataene oppbevares på en kryptert server på sikret datarom på Rådhuset, og det er etablert rutiner for håndteringen av disse slik at dataene ikke skal brukes noen andre steder og slik at disse dataene heller ikke skal tas ut av systemet. Det lagres ikke fingeravtrykk, bare identifikatorer. Fingeravtrykk kan ikke gjenskapes og informasjonen kan heller ikke overføres til andre.

Det benyttes ikke passord eller annet i tillegg til fingeravtrykket. Fingeravtrykket brukes på flere nivåer i systemet, men brukeren drar fingeren bare en gang. Dette låser opp hovedkortet på maskinen, harddisken og kryptert partisjon på maskinen (dataområde). Fingeravtrykket identifiserer brukeren mot Active Directory og tildeler rettigheter. Brukeren kan selv benytte metoden for å legge inn passord som de bruker andre steder, for eksempel på WEB.

Kommunen har vurdert flere alternative løsninger, men ønsket tidlig å gå inn for et system som er støttet av trusted computing group hvor alle de store leverandørene sitter. Alternative løsninger har ikke like stor grad av sikkerhet.

Bruken av fingeravtrykk er obligatorisk for bærbare maskiner, mens den for stasjonære maskiner vil være obligatorisk for lukket sone. Omfanget av bruken vil bli vurdert fortløpende.

Datatilsynet har lagt til grunn feil forståelse av hvordan Levonos fingeravtrykksleser virker. Personopplysningsloven § 12 må tolkes på en annen måte enn det Datatilsynet har lagt til grunn. Bestemmelsen får ikke anvendelse på foreliggende sak da kommunens bruk av fingeravtrykklesere ikke faller inn under begrepet "entydig identifikasjonsmiddel".

Selv om § 12 skulle komme til anvendelse, er de krav bestemmelsen oppstiller oppfylt da bruk av fingeravtrykkleseren ivaretar et saklig behov, samtidig som slik bruk må anses nødvendig ut i fra den proporsjonalitetsvurdering bestemmelsen anviser. Det faktum at bruk av fingeravtrykklesere gir en personverngevinst, står sentralt i denne vurderingen.

Datatilsynets vedtak gir uønskede konsekvenser. Behandlingsansvarlige tvinges blant annet til å velge løsninger som gir en lavere grad av informasjonssikkerhet Et slikt vedtak vil også være problematisk i forhold til Norges EØS-forpliktelser. Norsk rett vil være i utakt med det gjennomgående syn på slik teknologi i Europa for

øvrig; et forhold som i seg selv er i strid med grunnhensynene bak EUs personverndirektiv, og vil medføre at Norge generelt sett vil få en lavere grad av informasjonssikkerhet enn øvrige europeiske land. Det faktum at slik ulik regulering i praksis vil innebære et tilnærmet omsetningsforbud for slik teknologi, underbygger det problematiske i forhold til de EØS-rettslige forpliktelsene.

Den teknologiske løsning kommunen som behandlingsansvarlig har valgt for å sikre autentisering, skaper et bedret personvern for kommunens klienter, samtidig som løsningen ikke innebærer noen økt personverntrussel for kommunens ansatte. Løsningen gir bedre informasjonssikkerhet fordi fingeravtrykklesere er en sikrere autentiseringsmetode enn tradisjonell bruk av brukernavn og passord. Kommunen er kjent med de innvendinger Datatilsynet generelt sett har hatt mot bruk av slik teknologi. Den fingeravtrykkleseteknologi som kommunen benytter er imidlertid spesielt utformet for å ivareta og imøtekomme de personvernrisikoer som generelt sett er knyttet til bruk av fingeravtrykklesere. De hensyn personopplysningsloven skal beskytte taler derfor samlet for at den valgte løsning er lovlig i henhold til personopplysningsloven § 12. Samme type løsning er kjøpt av Stortinget.

De bærbare maskinene til kommunens ansatte er utstyrt med fingeravtrykklesere. Avleserne leser ikke fingeravtrykk som sådan, men matematiske koder.
De matematiske kodene blir innhentet ved første gangs pålogging i forbindelse med at den ansatte får tildelt maskinen. Etter vanlig pålogging med brukernavn og passord vil en applikasjon be den ansatte om å presentere to til tre fingre for avleseren. Biometriske data leses av internt i avleseren. Opptil 75 punkter i avtrykket, såkalte minutia points, behandles ved hjelp av algoritmer. Det er altså ikke tradisjonelle biometriske data som lagres; heller ikke lagres det noen form for fotografisk kopi eller annen kopi av brukernes fingeravtrykk. Det som lagres er utelukkende matematiske verdier og koordinater som definerer disse opptil 75 punktene. Dataene utgjør personens template. Den lagrede templaten linkes opp mot det unike brukernavnet. Det eksisterer ingen direkte kobling mellom template og brukerens identitet. Brukernavnet, derimot, kan være linket opp mot identitet, dersom slike data legges inn i de sentrale databaser. De ulike koblingene mellom dataene er illustrert i brev av 19. mai 2006 s. 4.

"Match" mellom finger og template gjør at passord automatisk fylles inn.
Det vil kun være brukernavn og passord som blir kommunisert til operativsystemet (databaser), ikke templaten som sådan. Her kan det legges inn informasjon om brukerens identitet (under General), slik at identitet knyttes opp mot brukernavn (Account). Det er derimot ingen mulighet til å legge inn data om selve templaten i slike databaser. Slike databaser - og de data som legges inn i slike - vil altså være uavhengig av om det benyttes fingeravtrykklesere eller ikke.
I Tysvær kommune skjer denne automatiske utfyllingen av passord ved tre autentiseringsstadier - BIOS-login, harddisk-login og Windows-login.

Templater kan vanligvis lagres på forskjellige måter - lagring på lokal disk, sentral server eller lagring i den fysiske avleserenheten. De to førstnevnte løsningene

innebærer lagring i programvare; sistnevnte løsning innebærer lagring i den fysiske maskinvaren. De ulike lagringsalternativene medfører enkelte forskjeller med hensyn til krypterings- og beskyttelsesnivå. Tysvær kommune har valgt en kombinasjon av lokal- og serverlagring.

Er template lagret i den fysiske avleserenheten (brikken i selve fingeravtrykkavleseren), vil all behandling av data foregå internt i denne enheten, og det er derfor ikke nødvendig med noen kryptering av kommunikasjon. Enheten er et beskyttet minneområde, og det er teknisk tilnærmet umulig å hente data ut fra dette området. Er template lagret lokalt eller på server, er templaten, og dermed også kommunikasjonen av denne, kryptert ved hjelp av algoritmer, som DES og Blowfish. Dersom template er lagret på server, er all kommunikasjon av template mellom klient og server beskytt et med en SSL-tilkobling.

Kommunens primære lagringsområde er serveren, hvor alle ansattes templater er lagret. Når den ansatte logger seg på en av kommunens maskiner, vil maskinen kommunisere med serveren og lage en lokal replika av templaten i den fysiske avleserenheten. Neste gang denne personen logger seg på samme maskin, er det derfor ikke nødvendig med kommunikasjon av template mellom server og lokal maskin. All kommunikasjon av templater skjer internt i den fysiske avleserenheten, hvor verifisering av finger og template skjer automatisk.

De fleste av Tysvær kommunes bærbare maskiner er personlige, det vil si knyttet til en ansatt. Det vil derfor normalt bare være lagret templater knyttet til en person i den enkelte avleserenheten. Som vist ovenfor, skjer det ingen bekreftelse av vedkommendes sanne identitet; systemet brukes ikke for identifikasjon. Når en ansatt logger inn ved bruk av fingeravtrykkleseren, skjer det – som ved bruk av brukernavn og passord - en verifisering av hvorvidt personen som forsøker å logge seg på er autorisert , og eventuelt hva slags rettigheter vedkommende har i systemet. Vedkommende er altså legitimert . Bruk av fingeravtrykkleseren i denne forbindelse er utelukkende en autentiseringsmetode. Bruk av fingeravtrykkleseren innebærer ingen økt risiko for identifisering i forhold til tradisjonell bruk av brukernavn og passord.

Klager anfører at systemer som utelukkende baserer seg på brukernavn og passord kan være sårbare med hensyn til informasjonssikkerhet. I brev av 19. mai 2006 s. 5 flg. beskrives forskjellige sikkerhetsrisikoer. Klager mener at bruk av fingeravtrykk gir bedre informasjonssikkerhet i det den gir sikkerhet for at man er rett bruker av maskinen. Misbruksfaren er kun hypotetisk. Bruk av fingeravtrykksleseren innebærer heller ingen krenkelse av den personlige integritet. Dette blant annet fordi det er den ansatte selv som foretar innrulleringen av de biometriske dataene. Den ansatte kan selv velge om systemet skal benyttes.

Templater er ikke et entydig identifikasjonsmiddel, og brukes heller ikke som identifikasjonsmiddel av kommunen. Hensikten med personopplysningslovens § 12 er å redusere bruk av identifikasjonsmidler som ikke er egnet til

legitimering/autentisering til slike formål. Templater egner seg utmerket til autentisering.

Biometriske data er en uensart et gruppe av opplysninger som kan anvendes på mange måter. Eksempelvis kan prøver av DNA, bilder, signatur, tatoveringer og lignende langt på vei brukes til å bekrefte en persons sanne identitet. Det samme kan fingeravtrykk brukt i visse sammenhenger, eksempelvis ved bruk i pass, jf passloven § 6. Enkelte biometriske data kan imidlertid også anvendes utelukkende som autentiseringsmetode.

Departementets uttalelse i forarbeidene til personopplysningslovens § 12, og Datatilsynets forståelse, må derfor nyanseres. Kommunen er av den oppfatning at autentisering er noe annet enn, ikke en underkategori av, identifisering. I Artikkel 29-gruppens arbeidsdokument om biometri av 1. august 2003 understrekes viktigheten av skillet mellom autentisering og identifikasjon. Det presiseres her at autentisering er svar på "er jeg den jeg pretenderer å være?", mens identifikasjon er svar på "hvem er jeg ?". Et autentiseringssystem kan etter dette ikke samtidig være et identifiseringssystem.

Uansett om man anser autentisering som en underkategori av et vidt identifiserings-begrep, er det ingen forhold som tilsier at man ved lovtolkningen skal legge denne vide forståelsen av "identifikasjon" til grunn. Tvert om følger det av gjeldende tolkningsprinsipper at man skal legge til grunn en alminnelig ordlydsforståelse dersom man ikke har holdepunkter for annet. En alminnelig forståelse av identifikasjon inkluderer ikke autentisering . Det er denne forståelse av identifisering som Datatilsynet må anvende ved tolkningen av § 12.

Et "identifikasjonsmiddel " må da være et middel for å angi et entydig individ. Som det fremgår av Artikkel 29-gruppens arbeidsdokument, vil et identifikasjonsmiddel anerkjenne et individ ved å skjelne biometriske data knyttet til vedkommende fra biometriske data knyttet til andre. I motsetning vil en autentiseringsmetode anerkjenne et individ ved å verifisere om to faktiske forhold har en tilstrekkelig sammenheng. Videre uttaler Art. 29-gruppen: *"In principle, it is not necessary for the purposes of authentication/verification to store the reference data in a database; it is sufficient to store the personal data in a decentralised way. Conversely, identification can only be achieved by storing the refrence data in a centralised database, because the system, in order to ascertain the identity of the data subject, must compare his/her templates or raw data (image) with the templates or raw data of all persons whose data are already centrally stored".* (Klagers utheving). Klager mener etter dette at Artikkel 29-gruppen utelukker muligheten for at templater kan være et identifikasjonsmiddel dersom den er lagret lokalt. Klager anfører videre at heller ikke templater lagret sentralt nødvendigvis et identifikasjonsmiddel.

I Tysvær kommune er templatene lagret sentralt. Likevel er det bare ved den ansattes første gangs bruk av en maskin at det skjer en kommunikasjon mellom den presenterte fingeren og den sentralt lagrede template. Deretter skjer dette lokalt i den fysiske

avleserenheten. Her er det normalt kun lagret templater knytt et til en person. Den ansattes forsøk på innlogging blir "besvart" ved 'ja" eller "nei"; det skjer en verifikasjon av at to faktiske omstendigheter korresponderer med hverandre. Det skjer altså ingen skjelning av ett individ fra et annet hvor "svaret" er at vedkommende ansatt er X. Tysvær kommunes fingeravtrykkleser er derfor ikke et identifikasjonsmiddel. Denne forståelsen underbygges av bestemmelsens formål . Personopplysningsloven § 12 regulerer primært fødselsnummer. Hensikten er særlig å unngå at fødselsnummer brukes til andre formål enn identifikasjon. Klager anfører at uttaleser i NOU 1997:19 pkt. 12.5.7.3.3. støtter forståelsen av at template er noe annet enn de opplysninger personopplysningslovens § 12 er ment å skulle omfatte og at template faller utenfor lovens anvendelsesområde. Det vises til brev av 19. mai 2006 s. 10.

Det anføres videre at template er et substitutt for passord og ikke et middel for identifikasjon. Det anføres videre at templater ikke er "entydige". Sannsynligheten for uautorisert match er 1:2500.

Subsidiært anføres at dersom personopplysningslovens § 12 får anvendelse er vilkårene for bruk oppfylt. Det anføres at det foreligger saklig behov for sikker identifisering og at Datatilsynet synes å være enig i denne vurderingen. Det anføres videre at metoden er nødvendig. Bestemmelsens ordlyd "nødvendig" gir anvisning på en helhetsvurdering av de personvernrisikoer og gevinster metoden medfører. Det er en rimelig og fornuftig tolkning av regelen å anse bruken som lovlig. Datatilsynets tolkning gir en uhensiktsmessig tolkning av bestemmelsen som "fryser" utviklingen av informasjonssikkerhet. Klagers lovforståelse støttes også av lovgivers intensjon om at samfunnshensyn bør inngå som et moment i vurderingen av nødvendighet.

Det anføres at Stortingets datasystem bruker fingeravtrykk som påloggingsmetode og at det fremstår som underlig dersom lovgiver anvender et system de selv har vedtatt er forbudt.

Det anføres at det følger av personverndirektivet jf. uttaleser fra art. 29-gruppen at proporsjonalitet er et viktig tolkningsprinsipp med hensyn til regler om bruk av biometriske data. Det vises til argumentasjon i brev av 19. mai 2006 s. 14. Det er anført at direktivets bestemmelser er tolket annerledes i Sverige, hvor bruk av biometriske data følger de vanlige behandlingsregler. Dette bekreftes av to saker behandlet av Datainspektionen om bruk av fingeravtrykk som autentisering til skolers datasystem og Kammarrättens avgjørelse i 2005 knyttet til bruk av fingeravtrykk på tallerkenautomater i skolekantine. Det er videre anført at direktivets bestemmelser også er tolket annerledes i Danmark, hvor bruk av biometri er tillatt i tilknytning til rabattkort for pendlere hos Bornholm Trafikken. Også andre land i Europa tolker direktivet på denne måten.

Det anføres at personopplysningslovens § 12 omfatter enhver form for personopplysninger. Resultatet av Datatilsynets tolkning vil bli at et forbud mot alle

former for identifikasjons- og autentiseringsmidler, som for eksempel elektronisk signatur.

Det anføres videre at Datatilsynet kan avstå fra å fatte vedtak jf. personopplysningslovens § 46 fordi vedtaket får større konsekvenser utenfor den foreliggende sak. Videre fordi Datatilsynet prinsippielt synes å være enige med klager og at verken Datatilsynet eller kommunen ønsker et tilnærmet forbud mot bruk av biometriske løsninger.

Det anføres at det er en saksbehandlingsfeil dersom Datatilsynet ikke tar stilling til om bruk av Levonos fingeravtrykksleser innebærer sikkerhetsmessige gevinster i forhold til bruk av brukernavn og passord.

5. Datatilsynets vurdering

Klager synes å være enig med Datatilsynet i at identifisering er noe annet enn autentisering, eller bekreftelse av identitet. Uenigheten ligger i spørsmålet om et fingeravtrykk, og templater av dette, skal anses som entydige identifikasjonsmidler, og om bruken av fingeravtrykk eller template for autentiseringsformål skal falle inn under bestemmelsen i personopplysningslovens § 12. Datatilsynet viser til vurderinger gjort i samlet oversendelsesbrev til Personvernnemnda med hensyn at fingeravtrykket og templater skal anses som entydige identifikasjonsmidler. Datatilsynet viser også til notat om endring av personopplysningslovens §12 som er oversendt Justisdepartementet.

Datatilsynet vil understreke at generering av templaten i seg selv innebærer en elektronisk behandling av personopplysninger. Hver gang en template skal utformes, må det først avgis et fullstendig fingeravtrykk. Fingeravtrykket må avgis hver gang løsningen benyttes. Deretter blir dette elektronisk bearbeidet. Oppramsingen i personopplysningslovens § 2 nr. 2 av forskjellige typer behandlinger er ikke uttømmende, og det kan derfor ikke tillegges vekt at elektronisk bearbeiding ikke er nevnt eksplisitt.

Bearbeidelsen av et fingeravtrykk til en "template" har som hovedformål å gjøre sammenligning av fingeravtrykk enklere. All argumentasjon med hensyn til sikkerhet ved bruk av fingeravtrykksløsninger (med template) bygger på en forståelse av at fingeravtrykket og templatene er entydige, og derfor er egnet til å bekrefte at man er den man utgir seg for å være.

Personopplysningslovens § 12.

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 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.

Denne saken skiller seg fra andre saker Datatilsynet har behandlet ved at kommunen, etter det opplyste, benytter fingeravtrykk alene. På Datatilsynets direkte spørsmål er det opplyst at det ikke skal tastes brukerID eller lignende i tillegg til at fingeravtrykket avleses. Datatilsynet oppfatter det likevel slik at det mest sannsynelig skjer en eller annen form for identifisering ved pålogging. BrukerID kan for eksempel være forhåndsutfylt. En annen mulighet er at fingeravtrykket i løsningen benyttes både til identifisering av individ og autentisering. Datatilsynet har ikke funnet det nødvendig til å ta stilling til dette, da det avgjørende for saken er at Datatilsynet mener at fingeravtrykk (template) kun er tillatt i tilknytning til identifisering og ikke brukt til autentisering slik kommunen benytter det, mens klagers hovedargument er at identifisering er noe annet enn autentisering, og at fingeravtrykket kun benyttes til autentisering. Datatilsynet og klager er dermed enige om at kommunen ihvertfall benytter fingeravtrykket (template) i tilknytning til autentisering. Slik bruk er som nevnt over etter Datatilsynets oppfatning ikke tillatt.

Datatilsynet er uenig med klager i at den folkelige forståelsen av ordet "identifisering" er at ordet ikke omfatter autentisering. Klager Datatilsynet har mottatt i andre saker om bruk av fingeravtrykk gir inneholder en rekke argumenter for at autentisering nettopp er ledd i identifiseringsprosessen.[1]. Datatilsynet er imidlertid enig med klager i at ordet, slik det er benyttet i personopplysningslovens § 12, ikke er ment å skulle omfatte også autentisering. Det er Datatilsynets oppfatning at man har valgt ordet identifisering for å avgrense mot legitimering/autentisering. Lovgivers formål har vært å forby bruk av entydige identifikasjonsmidler til annet enn den rene identifisering. Bruk av entydige identifikasjonsmidler til autentisering er etter dette ikke tillatt. Det vises til felles oversendelsesbrev til Personvernnemnda for utdyping av disse vurderingene.

Saklig behov for sikker identifisering

Datatilsynet finner det problematisk at klager på den ene siden anfører at det ikke skjer noen form for identifisering, mens det på den andre siden subsidiært anføres at det foreligger saklig behov for sikker identifisering. Som nevnt over antar Datatilsynet at det skjer en eller annen form for identifisering, men at det er usikkert om fingeravtrykket (templaten) benyttes til dette.

Datatilsynet er ikke uenig med klager i at det foreligger et behov for sikring mot at sensitive personopplysninger i datasystemet kommer på avveie. Det er Datatilsynets oppfatning at dette igjen medfører et behov for sikker identifisering av brukere ved pålogging til datamaskin og datasystemer. Sikker identifisering er en forutsetning for overholdelse av en rekke bestemmelser i personopplysningsloven og

[1] Datatilsynets saker nr. 06/83, 06/180 og 06/1556 som er oversendt Personvernnemnda for behandling.

personopplysningsforskriften, blant annet personopplysningsforskriftens §§ 2-8, 2-11 og 2-14. Identifiseringen kan for eksempel skje gjennom angivelse av brukernavn.

Metoden er nødvendig for sikker identifisering
Selv om det etter Datatilsynets vurdering foreligger saklig behov for sikker identifisering, er det Datatilsynets oppfatning at bruk av fingeravtrykksløsning (template) ikke er nødvendig for å oppnå slik sikker identifisering.

Spørsmålet i forhold til personopplysningslovens § 12 er ikke om innføring av fingeravtrykkskontroll gir bedre datasikkerhet som sådan, 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."*

Datatilsynet forstår at bruk av fingeravtrykk kan fremstå som enkelt og praktisk for den enkelte i hverdagen. Dette kan imidlertid ikke være avgjørende for vurderingen av om bruken er nødvendig.

Det fremstår som uklart om bruken av fingeravtrykk er ment å skulle være frivillig. I kommunens e-post av 7. februar 2006 opplyses at bruken vil være obligatorisk for bærbare datamaskiner og for lukket sone på de stasjonære maskinene. I brev av 19. mai 2006 antydes det imidlertid at det skal finnes alternativer for de som ikke ønsker å benytte løsningen(jf. pkt. 4.4 s. 8). Datatilsynet legger til grunn at det teknisk sett er mulig for den ansatte å velge å benytte en annen løsning, men at kommunen vil pålegge bruk av fingeravtrykk for sine ansatte, fordi de anser at dette gir best datasikkerhet. Datatilsynet er enig i at god autentisering av brukere kan gi god datasikkerhet. Man kan imidlertid oppnå like sikker identifisering av brukerne uten å benytte fingeravtrykk. Identifiseringen kan for eksempel skje gjennom bruk av brukeridentitet eller ansattnummer. For å gi bedre datasikkerhet kan deretter andre lovlige autentiseringsmidler benyttes, som for eksempel smartkort kombinert med passord.

Det er anført at bruk av fingeravtrykk (template) må anses som nødvendig fordi løsningen er personvernfremmende. Det er blant annet anført at den ansatte selv har kontroll over registreringen og bruken av fingeravtrykket. Datatilsynet vil bemerke at den ansattes kontroll er illusorisk dersom bruken gjøres obligatorisk. Da blir alternativet eventuelt å ikke benytte dataløsningen. For øvrig har den ansatte ingen kontroll med hva som faktisk skjer med fingeravtrykket når dette er avgitt. Det er arbeidsgiver som velger hvordan det skal behandles, herunder hvordan templaten skal lagres og hvem som skal ha tilgang til denne.

Betydningen av at andre land tillater bruk av biometriske kjennetegn etter en proporsjonalitetsvurdering

Personverndirektivet utgjør en minstestandard for lovgivning. De enkelte EU/EØS-land kan velge å ha strengere bestemmelser i nasjonal lovgivning, så fremt ikke dette er til hinder for gjennomføringen av EU/EØS-forpliktelser for øvrig. Det følger av direktivets art. 8 nr. 7 at *"Member States shall determine the conditions under wich a national identification number or any other identifier of general application may be processed"*. Norske myndigheter har valgt å utforme en spesiell bestemmelse for bruk av fødselsnummer og andre entydige identifikasjonsmidler. I odelstingsproposisjonen (Ot.prp. nr. 92 (1998-99) som ligger til grunn for bestemmelsen er nettopp fingeravtrykk og andre biometriske data spesielt nevnt som eksempel på slike entydige identifikasjonsmidler. De andre landene som klager har vist til har ikke gitt noen slik særlig bestemmelse for bruk av entydige identifikasjonsmidler. Når Datatilsynet har trukket frem tolkningen av direktivet i andre land i notatet til Justisdepartementet, er dette nettopp som et argument for at den norske bestemmelsen fremstår som noe streng og bør endres. Datatilsynet ser at det kan være hensiktsmessig om norsk rett bringes nærmere andre europeiske lands rett. Datatilsynet finner imidlertid ikke at andre lands tolkning av direktivet kan gis avgjørende betydning for tokningen av personopplysningslovens § 12, når Stortinget bevisst har vedtatt en regel med strenge vilkår for bruk av fødselsnummer og andre entydige identifikasjonsmidler.

Datatilsynet er ikke kjent med avgjørelser i andre EU/EØS-land knyttet til fingeravtrykk brukt i pålogging til datasystemer hvor sensitive personopplysninger behandles. Det er ikke grunnlag for å si at den bruk klager ønsker av fingeravtrykk ville blitt akseptert av andre europeiske datatilsynsmyndigheter, på tross av at de har mindre strenge bestemmelser for bruken av fingeravtrykk.

Stortingets bruk av fingeravtrykk

Det medfører ikke brudd på personopplysningsloven å kjøpe datamaskiner hvor bruk av fingeravtrykk i pålogging er en opsjon. Datatilsynet anser imidlertid at det utgjør et brudd på personopplysningsloven hvis Stortinget gjennom sin dokumenterte datasikkerhet og internkontroll pålegger de ansatte å benytte fingeravtrykk i tilknytning til pålogging. Det er ingen selvfølge at Stortinget, som følge av sin posisjon som lovgiver, aldri bryter loven.

Det fremgår av e-posten fra Stortinget v/ Frode Rein, at Stortinget ikke benytter nøyaktig samme fremgangsmåte som Tysvær kommune. Etter det opplyste benytter Stortinget fingeravtrykket kun til to stk. bærbare maskiner, og da kun i pålogging til selve maskinen. Templaten er kun lagret lokalt i en sikkerhetsbrikke i maskinen. Ved pålogging til Stortingets datasystemer kreves i tillegg brukernavn og passord. Da Datatilsynet var i kontakt med leder for sikkerhetsavdelingen, Gerrit Løberg, per telefon fikk vi opplyst at man ikke benyttet fingeravtrykk i datasikkerhetsløsninger nettopp fordi dette ikke var lovlig. Datatilsynet antar derfor at det i dette tilfellet kan dreie seg om en feil oppstått som følge av manglende kommunikasjon mellom ansatte

i sikkerhetsavdelingen og IT-avdelingen. For ordens skyld opplyses at Datatilsynet vil skille ut den videre behandlingen av Stortingets bruk av fingeravtrykk til en egen sak.

Betydning av Datatilsynets tolkning for bruk av andre autentiseringsmidler
Datatilsynet har foreløpig ikke hatt saker hvor spørsmålet om personopplysningslovens § 12 i forhold til elektronisk signatur er satt på spissen. Datatilsynet vil imidlertid minne om at dersom bruk av elektronisk signatur eller entydige identifikasjonsmidler i autentisering har hjemmel i annen lov, vil ikke personopplysningslovens § 12 være til hinder for bruk, jf. personopplysningslovens § 5.

Fingeravtrykk og eventuelle sikkerhetsgevinster
Datatilsynet vil understreke at det ikke finnes noen garanti mot at templater, på tross av det som er hevdet til nå, med fremtidige løsninger kan reverseres. For øvrig er det vanskelig å overskue virkningen av at man benytter fingeravtrykk, som er tillagt stor vekt blant annet i oppklaring av kriminalsaker, til trivielle formål. Datatilsynet finner derfor at man bør være forsiktig med å benytte fingeravtrykk der dette ikke er strengt nødvendig. Datatilsynet finner at det må veie tungt at lovgiver i forarbeidene nettopp har fremholdt at entydige identifikasjonsmidler skal benyttes med varsomhet jf. Ot. Prp. Nr. 92 (1988-89) s. 114.

Datatilsynet vil for øvrig bemerke at bruk av fingeravtrykk alene i påloggingen ikke medfører noen datasikkerhetsgevinst i forhold til andre løsninger som benyttes i dag. Av sikkerhetsårsaker bør alltid flere parametre, for eksempel brukernavn og passord, benyttes.

Klager har anført at bruk av løsningen med fingeravtrykk gir en sikkerhet for uautorisert "match" på 1:2500. Datatilsynet finner det tvilsomt om dette er en sikkerhet som er tilstrekkelig i forhold til krav i personopplysningsforskriften til at personopplysninger skal sikrets mot uautorisert innsyn og uautorisert endring jf. §§ 2-11 og 2-13 og at informasjonssystemet skal sikres mot uautorisert bruk jf. § 2-14. Det må understrekes at fingeravtrykket (templaten) er tenkt å gi adgang til sensitive personopplysninger. Kravet til sikkerhet er da forholdsmessig høyere enn dersom det kun hadde gitt tilgang til ordinære personopplysninger.

Datatilsynets mulighet til å avstå fra å fatte vedtak i saken
Datatilsynet er enig i klagers anførsel om at personopplysningslovens § 46 er en "kan" regel, og at Tilsynet kan velge å ikke fatte vedtak i saker hvor det er strid med bestemmelser i eller i medhold av personopplysningsloven. Datatilsynet har imidlertid ikke for praksis å avstå fra å fatte vedtak, med mindre den lovstridige behandlingen av personopplysninger allerede er opphørt. Datatilsynet har allerede fattet vedtak i en rekke saker knyttet til bruk av fingeravtrykk. Ikke alle av disse er påklaget til Personvernnemnda. Det vil fremstå som vilkårlig dersom man skulle avstå fra å fatte vedtak i nettopp denne sak.

Datatilsynet er enige i at vedtaket i denne saken får stor virkning for andre saker om bruk av biometriske kjennetegn. Nettopp derfor er det viktig at Datatilsynet foretar en konsekvent tolkning av personopplysningslovens § 12. Noe annet ville fremstå som svært vilkårlig. Det er videre slik at Datatilsynets eventuelle beslutning om ikke å fatte vedtak ville få vel så store konsekvenser utenfor denne konkrete saken. Dersom Datatilsynet på denne måten signaliserte at det er mulig å benytte biometriske kjennetegn, er det stor sannsynlighet for at en rekke virksomheter og kommuner ville gå til innkjøp av slikt utstyr, med de økonomiske konsekvenser dette ville ha dersom det på et senere tidspunkt ble fastslått at bruken faktisk er ulovlig.

Datatilsynet er satt til å håndheve og tolke personopplysningsloven jf. personopplysningslovens § 42. Datatilsynet forstår imidlertid ikke dette mandatet dit hen at det åpner for å tolke reglene i strid med det klar ordlyd og intensjonen da bestemmelsene ble vedtatt. Dersom en bestemmelsen fungerer dårlig i praksis, eller gir uheldige resultater, er det imidlertid Datatilsynets oppgave å gjøre lovgiver oppmerksom på dette. Derfor har Datatilsynet fremmet forslag til endring av personopplysningslovens § 12 overfor Justisdepartementets lovavdeling, som i disse dager arbeider med revisjon av personopplysningsloven.

6. 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 m/vedlegg: Advokatfirmaet Wiersholm v/advokat Kyrre Eggen, Pb. 1400 Vika, 0115 Oslo

Vedlegg: Kopi av sakens dokumenter