

PVN-2006-08 Oxigeno Fitness – fingeravtrykk ved adgangskontroll

Klage på Datatilsynets vedtak om at Oxigeno Fitness må avslutte bruken av fingeravtrykk ved adgangskontroll til treningssenter

Personvernemndas avgjørelse av 26. mars 2007 (Jon Bing, Gro Hillestad Thune, Leikny Øgrim, Siv Bergit Pedersen, Jostein Halgunset, Hanne I Bjurstrøm, Tom Bolstad)

Datatilsynets referanse: 06/00083-6/AFL

1 Innledning

Personvernemnda har ved oversendelse fra Datatilsynet mottatt klage fra Oxigeno Fitness på Datatilsynets vedtak om at Oxigeno Fitness må avslutte bruken av fingeravtrykk ved adgangskontroll.

2 Saksgang

Datatilsynet mottok tidlig i 2006 spørsmål knyttet til bruk av fingeravtrykk ved treningssenteret Oxigeno Fitness i Oslo. Det ble rettet en henvendelse til treningssenteret 23.1.2006 hvor det ble gitt generell informasjon om personopplysningsloven § 12. Treningssenteret ble gitt en svarfrist til 6.2.2006 til å gi en redegjørelse for hvordan selskapet oppfylte vilkårene i denne paragrafen.

Datatilsynet purret opp brevet 8.3.2006. Ny svarfrist ble satt til 24.3.2006. I brev av 23.3.2006 redegjør Oxigeno Fitness for sin bruk av fingeravtrykk.

I brev av 28.4.2006 ga Datatilsynet pålegg om at bruken av fingeravtrykk måtte avsluttes.

Vedtaket ble påklaget av Oxigeno Fitness 19.5.2006. Klager ba om oppsettende virkning til 12.7.2006, da nytt system ville være på plass.

Personvernemnda er klageorgan for vedtak fattet av Datatilsynet

Sekretariat: Tonje Røste Gulliksen
Postboks 4594
Nydalén
0404 OSLO

Sentralbord +47 23 40 05 00
Direkte +47 23 40 05 97
Mobil +47 92 88 14 07
post@pvn.no
www.personvernemnda.no

Personvernemnda mottok saken fra Datatilsynet 1.9.2006. Klager ble orientert om dette i brev fra nemnda 11.9.2006.

Datatilsynet hadde pålagt treningssenteret å stanse bruken av fingeravtrykkspålogging innen 19.5.2006. Oxigeno Fitness ba om oppsettende virkning til 12.7.2006. Tidspunktet var passert og Datatilsynet vurderte dette, jf forvaltningsloven § 42, men fant at det ikke lenger var grunn til å gi vedtaket oppsettende virkning.

Personvernemnda sendte klager et brev den 29.1.2007 og ba om mer utfyllende opplysninger om hvilke opplysninger om kunden som blir lagret under "kunde-ID". Nemnda mottok ikke svar og sendte derfor en puring den 1.3.2007. Purrebrevet er heller ikke blitt besvart. Nemnda må derfor legge til grunn det faktum som foreligger.

3 Faktum

Oxigeno Fitness bruker en løsning kalt IdentX. Fingeravtrykket benyttes som identifikator ved adgangskontroll til senteret.

IdentX er programvare utviklet for å identifisere oppføringer eller personer i en database. Den brukes til adgangskontroll og adgangsregistrering. En template blir utformet på bakgrunn av fingeravtrykket som lagres i en lokal database. Når personen skal identifiseres i databasen gjøres det et todelt søk for å finne en template som stemmer med det som opprettes ved innlesing. Såkalt "kunde-ID" returneres da fra databasen. Selve innskanningen av fingeravtrykket lagres ikke og brukes ikke til identifisering. Sensoren som brukes til fremstillingen av en template inneholder ikke minne. Dersom en sensor kommer på avveie, ligger det derfor ingen templer lagret der. Når en kunde skal slutte, slettes templatene og kunde-ID fra databasen.

Det fremgår av kundeavtalen at fingeravtrykksløsningen brukes i adgangskontroll. Dersom den tekniske løsningen svikter, testes kundene inn manuelt. Registreringen er frivillig for senterets medlemmer.

Personvernemnda har ikke lyktes i å finne ut av hva som omfattes av "kunde-ID". I kundeavtalen som er fremlagt i saken står det at kunden skal oppgi navn, adresse, bankkontonummer og opplysninger om medlemskap. Nemnda legger til grunn at dette utgjør "kunde-ID". Det er ikke opplyst i kundeavtalen noe om hvorvidt og eventuelt på hvilken måte kunden må legitimere seg ved inngåelse av medlemskap.

Datatilsynet har fattet følgende vedtak:

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

4 Anførelse

Klager opplyser at på tross av ca 1800 medlemmer har man ikke mottatt klager på fingeravtrykksløsningen.

Med en så stor medlemsmasse er det et sterkt behov for 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. Ved innsjekking med fingeravleser i resepsjonen forebygges misbruk av personlig medlemskap.

Alle kunder undertegner en kundeavtale. Her gjøres kunden oppmerksom på den tekniske løsningen rundt innsjekkingen før kunden signerer avtalen. Som vedlegg får kunden informasjon om løsningen IdentX.

5 Datatilsynets vurdering

I følge Datatilsynet er et fingeravtrykk, også når dette benyttes til å utarbeide en template, å anse som et entydig identifikasjonsmiddel. Fingeravtrykk kan derfor bare benyttes når dette er tillatt etter personopplysningsloven § 12.

Bestemmelsen i personopplysningsloven § 12 har to kumulative vilkår;

1. det er saklig behov for sikker identifisering
2. metoden er nødvendig for å oppnå slik identifisering

Datatilsynet viser i den forbindelse til notat om endring av personopplysningsloven § 12 som er oversendt Justisdepartementet.

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.

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

Datatilsynet mener 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.

Datatilsynet finner at fingeravtrykk ikke er nødvendig for sikker identifisering i tilknytning til adgangskontroll på treningssentre. Kontroll av medlemskort opp mot registrert personalia, eventuelt bruk av medlemskort kombinert med en PIN-kode eller et passord gir tilstrekkelig sikker identifisering. Oversikt over antall personer i lokalet kan man oppnå ved innføring av telleport, adgangsprotokoll eller manuell telling.

6 Personvernemndas merknader

Når det gjelder generelle svenske og danske saker vedrørende bruk av fingeravtrykk som adgangs- eller tilgangskontroll, viser nemnda til sak PVN-2006-07 (Tysvær kommune), avsnitt 7.4.

Nemnda skal likevel vise til en dansk sak som er relevant i denne saken. I danske Datatilsyns avgjørelse av 26.11.2004 i sak 2004-219-0208, om adgangskontroll til et mosjonssenter, nektet tilsynet mosjonssenteret å bruke fingeravtrykksskanner. Ved inngangen til senteret skulle medlemmene lese av fingeravtrykket på en skanner, som regnet ut en verdi og som deretter ble holdt opp mot senterets medlemsdatabase. Utrekningen av verdien skjedde i skanneren og skanningen av fingeravtrykket skulle ikke forlate skanneren. Det danske Datatilsynet la vekt på at saken skilte seg fra saken om Bornholmerkortet. Den utregnede verdien ble ikke oppbevart i et smartkort som den registrerte var i besittelse av, slik som i Bornholmerkortet, men i en database som den registrerte ikke har samme mulighet til å føre kontroll med. Det danske Datatilsynet konkluderte med at formålet med behandlingen ikke sto i samsvar med hvor inngripende behandling det var tale om. Tilsynet mente at det ønskede formål kunne oppnås med mindre inngripende midler.

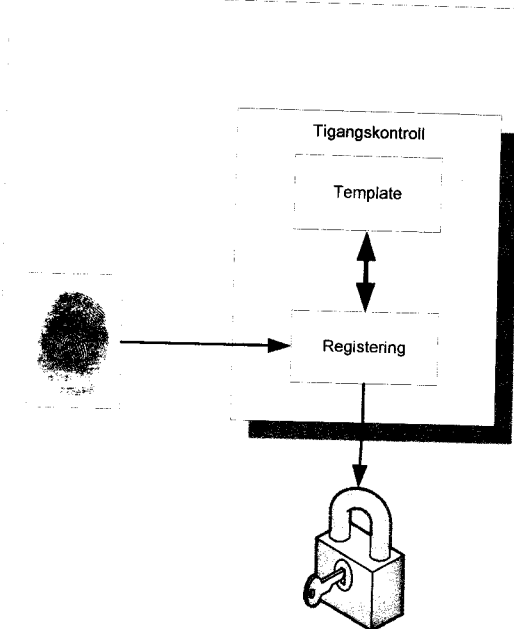
I svensk og dansk rett finnes det ingen bestemmelse tilsvarende den norske personopplysningsloven § 12 – for øvrig finnes det heller ingen bestemmelse som tilsvarende den norske personopplysningsloven § 12 i personverndirektivet. I Sverige og Danmark benytter man derfor de vanlige reglene, tilsvarende den norske personopplysningsloven §§ 11, jf 8.

6.1 Grunnkrav til behandling av personopplysninger

Etter personopplysningsloven § 11, 1. ledd *litra* a, jf § 8, må det foreligge et behandlingsgrunnlag før personopplysninger kan behandles. Et av behandlingsgrunnlagene som § 8 gir anvisning på er samtykke. Det kan hevdes at samtykke er innhentet ved at bruk av teknologien er frivillig. Medlemmene avgir fingeravtrykket frivillig, de gjør dette selv ved første gangs besøk på treningssenteret, og det er mulig å velge teknologien vekk. Vilåret i personopplysningsloven § 8, 1. ledd, er dermed oppfylt.

Spørsmålet er videre om de øvrige kravene i personopplysningsloven § 11 er oppfylt. Det gjelder særlig personopplysningsloven § 11 *litra* b og c, om at opplysningene bare brukes til formål som er saklig begrunnet i den behandlingsansvarliges virksomhet og at de ikke brukes senere til formål som er uforenelig med det opprinnelige formålet. Personvernemnda legger til grunn at disse vilkårene også er oppfylt.

6.2 Generelt om fingeravtrykk som adgangskontroll



Ved bruk av fingeravtrykk for å gi adgang til treningssenter har brukeren på forhånd registrert avtrykk av en eller flere fingrer ved å trekke fingeren over en smal skanner (optisk leser). Ved første gangs registrering trekkes som regel fingeren flere ganger inntil maskinen finner at avtrykket avleses på samme måte hver gang og godkjenner registrering.

Avtrykket behandles av registreringsenheten. Først velges det ut visse punkter fra mønsteret i fingeravtrykket etter en regel som kan variere fra enhet til enhet. Disse punktene vil ha ulike verdier alt etter utseendet til de deler av mønsteret som faller sammen med punktene.

Disse verdiene behandles så etter en regneregul (en algoritme) som danner en "template".¹ Denne template lagres så i enheten for tilgangskontroll. Det er gjerne et lite antall punkter som velges ut, i saken er det opplyst at det benyttes 50 punkter. Dette er for få punkter til at det er mulig å regenerere fingeravtrykket ved hjelp av templatene. Om det skal være mulig, må det registreres nok punkter til at det kan regenereres et bilde – en vanlig telefaks har en oppløsning på 90 000 punkter per kvadrattomme, som gir et inntrykk av hva som kreves for å lagre avtrykket som et "bilde". Men punktene er tilstrekkelig til at sannsynligheten for at to ulike fingrer skal generere samme template er svært små, også sammenlignet med sannsynligheten for at en uvedkommende skal finne frem til et passord valgt av bruker.

Når brukeren skal trene, trekkes fingeren over leseren på ny. Punkter registreres etter regelen, og det beregnes en verdi. Denne sammenlignes med den registrerte verdi, dvs templatene. For å godkjennes, må den beregnede verdien ligge innenfor en definert grense for avvik, ellers avvises forsøket på å få adgang.

Dette er en forenklet og prinsipiell fremstilling av bruken. I saken benyttes en teknikk som svarer til dette. I praksis er det både raskt og enkelt for brukeren å få adgang på denne måten.

¹ På norsk brukes gjerne uttrykket "mal" for det engelske "template", men i vedtaket er det brukt samme terminologi som i sakens dokumenter.

6.3 Personopplysningsloven § 12

Personopplysningsloven § 12, 1. ledd lyder:

Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.

Det følger av forarbeidene (Ot prp nr 92 (1998-99) side 114, 1. spalte):

Bestemmelsen gir en generell regulering av bruk av fødselsnummer og andre entydige identifikasjonsmidler som for eksempel fingeravtrykk og andre biometriske data. Slike identifikasjonsmidler bør ikke benyttes i utrengsmål. 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 sikker identifisering er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt.

Spørsmålet for Personvernemnda er om personopplysningsloven § 12 kommer til anvendelse i denne saken.

Betegnelsen "identifikasjonsmiddel" kan ha ulike tolkninger. For det første kan et identifikasjonsmiddel være "noe" som brukes for å gjenfinne opplysninger om én enkelt, på forhånd kjent person i en stor mengde med data, typisk en database. I en database vil det være en "nøkkel", denne nøkkelen vil måtte være entydig, ellers vil opplysninger om flere personer kunne forveksles. Fødselsnummer er en slik entydig identifikasjonsnøkkel. For det annet kan et identifikasjonsmiddel benyttes til autentisering etter at identifiseringen har funnet sted. Identifisering kan skje på en måte, for eksempel ved fødselsnummer. Når kandidaten for autentisering er funnet, skal man sikre at sannsynligheten for identitet er høy, i alle fall høyere enn den man får ved bruk av navn og fødselsdato. Nemnda har i sak PVN-2006-10 (Esso Norge) kommet til at personopplysningsloven § 12 dekker begge former for bruk av "identifikasjonsmiddel" når bruk av fingeravtrykk til autentisering er en del av et system for sikker identifisering.

Nemnda er i utgangspunktet av den oppfatning at fødselsnummer og fingeravtrykk ikke nødvendigvis kan sammenlignes. Loven forutsetter at fødselsnummer kan brukes som "entydig identifikasjonsmiddel". Med "entydig" sikter loven åpenbart til noe mer enn at identifikasjonen er entydig i forhold til det enkelte system. En identifikasjon må selvsagt være entydig innen systemets rammer, ellers vil den ikke kunne benyttes til oppslag. I denne forstand vil for eksempel en kundeidentifikasjon (KID) også være entydig i forhold til systemet for de aktuelle kunder. Når loven krever at identifikasjonsmiddelet må være entydig, kreves det altså noe *mer*. Nemnda legger til grunn at loven må tolkes slik at identifikasjonsmiddelet må være egnet til bruk som identifikasjon i *flere* systemer. Fødselsnummeret vil i denne forstand være et entydig identifikasjonsmiddel, fordi det er en nøkkel til å gjenfinne informasjon i flere ulike systemer. Fingeravtrykk vil også være et entydig identifikasjonsmiddel i denne forstand fordi samme avtrykk kan brukes for å få tilgang til flere system. Fødselsnummeret vil være velegnet til identifikasjon, men uegnet til autentisering (legitimasjon). Fingeravtrykket kan derimot brukes til begge deler.

Som den innledende presentasjonen (ovenfor i pkt 6.2) illustrerer, vil det internt i systemet ikke nødvendigvis brukes en nøkkel som er identisk med fingeravtrykket eller fødselsnummeret. Fingeravtrykket konverteres til en template, og denne templatene er i seg selv ikke et entydig identifikasjonsmiddel. Også et fødselsnummer kan behandles av et system slik at systemet selv bruker (og viser) et kryptert eller pseudonymisert nummer.

Personvernemnda forstår loven slik at den med "identifikasjonsmiddel" sikter til hva brukeren presenterer til systemet – et fingeravtrykk (som så behandles av systemets adgangskontroll) eller et fødselsnummer (som også kan f eks krypteres). Fingeravtrykket vil kunne brukes til å få tilgang til flere systemer, mens de ulike systemene i praksis vil konvertere det avleste avtrykket til ulike templer. Dette forhindrer ikke at fingeravtrykket anses som et "entydig identifikasjonsmiddel" i lovens forstand.

I det aktuelle systemet i denne saken vil fingeravtrykket avleses av en enhet i adgangskontrollen. Denne avlesningen behandles med sikte på å komme frem til en representasjon. Denne representasjonen bygger på avlesning av visse punkter i fingeravtrykket bestemt av den innebygde logikken i enheten. Representasjonen kan så sammenlignes med de templer som er lagret for fingeravtrykket til autoriserte brukere. Hvis sammenligningen ligger innenfor den forhåndsdefinerte margin for avvik, vil (1) brukeren være identifisert, og (2) brukeren være autentisert. Brukeren får dermed adgang til treningssenteret.

To av nemndas medlemmer (Leikny Øgrim og Jostein Halgunset) ønsker å opprettholde sin særmerknad. Det vises til PVN-2006-11 (Rema 1000).

6.4 Foreligger det "saklig behov", og er metoden "nødvendig for å oppnå slik identifisering"

Personopplysningsloven § 12 åpner for at man kan bruke entydige identifikasjonsmidler hvis særlige forhold foreligger.

I denne saken begrunnes bruken av fingeravtrykk med at medlemmene skal slippe å ta med medlemskort. Videre sikrer man at de personer som er medlem, har gyldig medlemskap, og metoden forebygger misbruk av personlige medlemskap.

Slik Personvernemnda ser det, er fordelene med slik bruk av fingeravleser at det er enkelt, praktisk og brukervennlig. Man behøver ikke å huske medlemskortet.

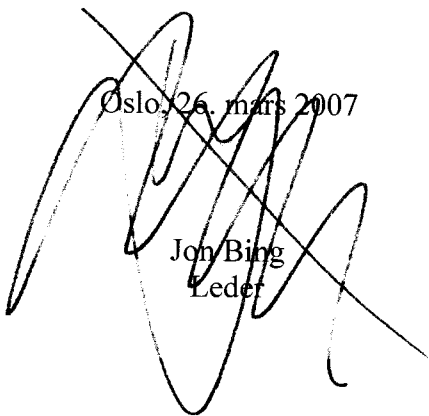
Imidlertid opplever enkelte personer bruk av fingeravtrykk som et inngrep i sin integritet. Dette kan ha sammenheng med at fingeravtrykk tradisjonelt sett er blitt brukt av politiet i forbindelse oppklaring av straffbare forhold. Det at politiet benytter fingeravtrykk i alvorlige kriminalsaker kan gi en opplevelse av mistenkeliggjøring når man må avgi fingeravtrykk i ulike dagligdagse situasjoner. Andre ulemper ved fingeravtrykksleser er at fingeravtrykkene legges igjen som spor i det daglige liv og det er fare for at dataene kan brukes til andre formål enn de formål de opprinnelig ble samlet inn for.

Personvernemnda er kommet til at treningssenteret kan sies å ha et saklig behov for sikker identifisering ved adgangskontrollen. Spørsmålet er imidlertid om kravet til nødvendighet er oppfylt. Det følger av forarbeidene at bruk av entydige identifikasjonsmidler ikke skal tillates dersom "andre og mindre sikre identifikasjonsmidler, som for eksempel navn, adresse og kundenummer" er tilstrekkelig. Etter nemndas syn kan treningssenteret benytte seg av "andre og mindre sikre identifikasjonsmidler" som likevel tilfredsstillende treningssenterets behov. Nemnda aksepterer argumentet om at bruk av fingeravtrykksleser gir medlemmene en enkel inngang og treningssenteret en god adgangskontroll. Dette er imidlertid ikke nok. I følge forarbeidene kreves det noe mer. Det må i tillegg være slik at det ikke kan tas i bruk en løsning som *ikke* forutsetter bruk av et entydig identifikasjonsmiddel, og som gir samme sikkerhet. Nemnda legger til grunn at det finnes tilfredsstillende alternativer som er sikkert nok for treningssenterets formål og behov. Nemnda viser til eksemplene i Datatilsynets vedtak.

Etter en konkret vurdering er Personvernemnda kommet til at i denne situasjonen er ikke bruk av fingeravtrykksleser nødvendig for å oppnå sikker identifisering. Den planlagte bruken er derfor ikke tillatt, jf personopplysningsloven § 12.

7 Vedtak

Klagen tas ikke til følge.



Oslo, 26. mars 2007

Jon Bing
Leder

Sammendrag til bruk ved publisering:

PVN-2006-08 Oxigeno Fitness – fingeravtrykkspålogging. Klage over at Datatilsynet stanset bruk av fingeravtrykksleser i adgangskontrollen ved treningssenteret Oxigeno Fitness i Oslo. Datatilsynet mente at det kunne sies å foreligge et saklig behov for sikker identifisering i tilknytning til adgangskontrollen, men at lovens krav til nødvendighet ikke var oppfylt. Personvernemnda var enig i Datatilsynets vurdering og tok ikke klagen til følge. Nemnda mener at treningssenteret kan benytte seg av ”andre og mindre sikre identifikasjonsmidler”, som likevel er sikkert nok til å tilfredsstille treningssenterets behov.

PVN-2006-09 Oslo trimsenter – fingeravtrykk ved adgangskontroll

Klage på Datatilsynets vedtak om at Oslo trimsenter må avslutte bruken av fingeravtrykk ved adgangskontroll til treningssenter

Personvernemndas avgjørelse av 26. mars 2007 (Jon Bing, Gro Hillestad Thune, Leikny Øgrim, Siv Bergit Pedersen, Jostein Halgunset, Hanne I Bjurstrøm, Tom Bolstad)

Datatilsynets referanse: 05/01556-9/AFL

1 Innledning

Personvernemnda har ved oversendelse fra Datatilsynet mottatt klage fra Oslo trimsenter på Datatilsynets vedtak om at Oslo trimsenter må avslutte bruken av fingeravtrykk ved adgangskontroll.

2 Saksgang

Datatilsynet mottok høsten 2005 informasjon om at Oslo trimsenter benyttet fingeravtrykk i tilknytning til adgangskontroll. Det ble rettet en henvendelse til treningssenteret 24.11.2005 hvor Datatilsynet ber om en redegjørelse.

I brev av 5.12.2005 redegjør Oslo trimsenter for sin bruk av fingeravtrykk, herunder formål og behandlingsgrunnlag.

I brev av 12.12.2005 ber Datatilsynet om utfyllende opplysninger med svarfrist 1.1.2006. Datatilsynet sendte ut en purring 3.2.2006 med ny frist 20.2.2006. I brev av 7.3.2006 fattet Datatilsynet vedtak om at bruken av fingeravtrykk måtte avsluttes. Vedtaket ble påklaget av Oslo trimsenter 7.4.2006.

Personvernemnda mottok saken fra Datatilsynet 1.9.2006. Klager ble orientert om dette i brev fra nemnda 11.9.2006.

Personvernemnda er klageorgan for vedtak fattet av Datatilsynet

Sekretariat: Tonje Røste Gulliksen
Postboks 4594
Ny dalen
0404 OSLO

Sentralbord +47 23 40 05 00
Direkte +47 23 40 05 97
Mobil +47 92 88 14 07
post@pvn.no
www.personvernemnda.no

Personvernemnda sendte klager et brev den 29.1.2007 og ba om mer utfyllende opplysninger om hvilke opplysninger om kunden som blir lagret under "kunde-ID". Nemnda mottok ikke svar og sendte derfor en purring den 1.3.2007. Purrebrevet er heller ikke blitt besvart, men sekretariatet mottok en telefon fra Tom Tangen 6.3.2007. Tangen opplyste da at de har avsluttet treningsdelen av senteret og driver nå kun med fysioterapi. Nemnda legger derfor til grunn det faktum som foreligger.

3 Faktum

Oslo trimsenter bruker en løsning kalt IdentX. Fingeravtrykket benyttes som identifikator ved adgangskontroll til senteret. 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.

IdentX er programvare utviklet for å identifisere oppføringer eller personer i en database. Den brukes til adgangskontroll og adgangsregistrering. En template blir utformet på bakgrunn av fingeravtrykket som lagres i en lokal database. Når personen skal identifiseres i databasen gjøres det et todelt søk for å finne en template som stemmer med det som opprettes ved innlesing. Såkalt "kunde-id" returneres da fra databasen. Selve innskanningen av fingeravtrykket lagres ikke og brukes ikke til identifisering. Sensoren som brukes til fremstillingen av en template inneholder ikke minne. Dersom en sensor kommer på avveie, ligger det derfor ingen templatelagret der. Når en kunde skal slutte, slettes templatens og kunde-id fra databasen.

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

Personvernemnda har ikke lyktes i å finne ut av hva som omfattes av "kunde-ID". I brev fra senteret står det at kunden skal oppgi personalia, ta bilde og registrere fingeravtrykk i databasen. Nemnda legger til grunn at dette utgjør "kunde-ID". Det er ikke opplyst noe om hvorvidt og eventuelt på hvilken måte kunden må legitimere seg ved inngåelse av medlemskap.

Datatilsynet har fattet følgende vedtak:

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

4 Anførelse

Klager opplyser 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 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 til slutt at personopplysningene er godt beskyttet og faren for at en template kommer på avveie er ekstremt liten.

5 Datatilsynets vurdering

I følge Datatilsynet er et fingeravtrykk, også når dette benyttes til å utarbeide en template, å anse som et entydig identifikasjonsmiddel. Fingeravtrykk kan derfor bare benyttes når dette er tillatt etter personopplysningsloven § 12.

Bestemmelsen i personopplysningsloven § 12 har to kumulative vilkår;

1. det er saklig behov for sikker identifisering
2. metoden er nødvendig for å oppnå slik identifisering

Datatilsynet viser i den forbindelse til notat om endring av personopplysningsloven § 12 som er oversendt Justisdepartementet.

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.

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 fingeravtrykket benyttes alene eller om man i tillegg fortsatt benytter medlemskort. Det kan ikke utelukkes at fingeravtrykket blir benyttet i tilknytning til identifisering dersom dette alene gir adgang til treningssenteret. Dersom det derimot brukes sammen med medlemskort, er det Datatilsynets vurdering at fingeravtrykket brukes for å verifisere identiteten og ikke til identifisering slik § 12 krever.

Datatilsynet mener at uansett er lovens krav til nødvendighet ikke oppfylt. Det er klart uttalt i forarbeidene at entydige identifikasjonsmidler ikke skal brukes i utrengsmål. Det følger av dette at nødvendighetsvurderingen bør være streng.

Datatilsynet finner at fingeravtrykk ikke er nødvendig for sikker identifisering i tilknytning til adgangskontroll på treningssentre. Kontroll av medlemskort opp mot registrert personalia, eventuelt bruk av medlemskort kombinert med en PIN-kode eller et passord gir tilstrekkelig sikker identifisering. Det er mulig å sørge for at medlemskortene blir vanskeligere å manipulere.

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

6 Personvernnemndas merknader

Når det gjelder svenske og danske saker vedrørende bruk av fingeravtrykk som adgangs- eller tilgangskontroll, viser nemnda til sak PVN-2006-07 (Tysvær kommune), avsnitt 7.4.

Nemnda skal likevel vise til en dansk sak som er relevant i denne saken. I danske Datatilsyns avgjørelse av 26.11.2004 i sak 2004-219-0208, om adgangskontroll til et mosjonssenter, nektet tilsynet mosjonssenteret å bruke fingeravtrykksskanner. Ved inngangen til senteret skulle medlemmene lese av fingeravtrykket på en skanner, som regnet ut en verdi og som deretter ble holdt opp mot senterets medlemsdatabase. Utrekningen av verdien skjedde i skanneren og skanningen av fingeravtrykket skulle ikke forlate skanneren. Det danske Datatilsynet la vekt på at saken skilte seg fra saken om Bornholmerkortet. Den utregnede verdien ble ikke oppbevart i et smartkort som den registrerte var i besittelse av, slik som i Bornholmerkortet, men i en database som den registrerte ikke har samme mulighet til å føre kontroll med. Det danske Datatilsynet konkluderte med at formålet med behandlingen ikke sto i samsvar med hvor inngripende behandling det var tale om. Tilsynet mente at det ønskede formål kunne oppnås med mindre inngripende midler.

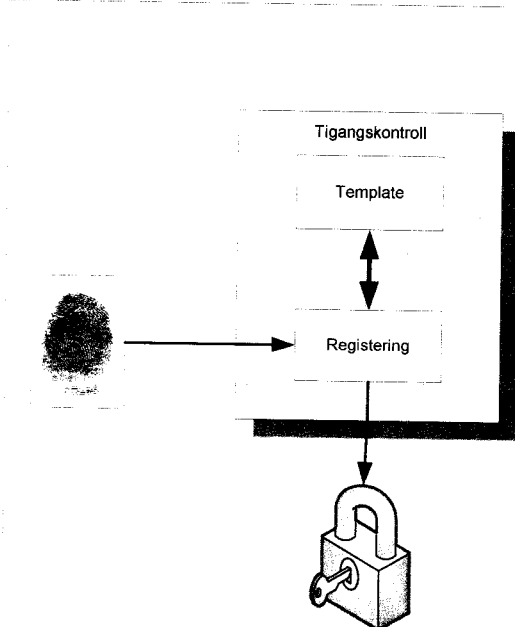
I svensk og dansk rett finnes det ingen bestemmelse tilsvarende den norske personopplysningsloven § 12 – for øvrig finnes det heller ingen bestemmelse som tilsvarende den norske personopplysningsloven § 12 i personverndirektivet. I Sverige og Danmark benytter man derfor de vanlige reglene, tilsvarende den norske personopplysningsloven §§ 11, jf 8.

6.1 Grunnkrav til behandling av personopplysninger

Etter personopplysningsloven § 11, 1. ledd *litra* a, jf § 8, må det foreligge et behandlingsgrunnlag før personopplysninger kan behandles. Et av behandlingsgrunnlagene som § 8 gir anvisning på er samtykke. Det kan hevdes at samtykke er innhentet ved at bruk av teknologien er frivillig. Medlemmene avgir fingeravtrykket frivillig, de gjør dette selv ved første gangs besøk på treningssenteret, og det er mulig å velge teknologien vekk. Vilkåret i personopplysningsloven § 8, 1. ledd, er dermed oppfylt.

Spørsmålet er videre om de øvrige kravene i personopplysningsloven § 11 er oppfylt. Det gjelder særlig personopplysningsloven § 11 *litra* b og c, om at opplysningene bare brukes til formål som er saklig begrunnet i den behandlingsansvarliges virksomhet og at de ikke brukes senere til formål som er uforenelig med det opprinnelige formålet. Personvernemnda legger til grunn at disse vilkårene også er oppfylt.

6.2 Generelt om fingeravtrykk som adgangskontroll



Ved bruk av fingeravtrykk for å gi adgang til treningssenter har brukeren på forhånd registrert avtrykk av en eller flere fingrer ved å trekke fingeren over en smal skanner (optisk leser). Ved første gangs registrering trekkes som regel fingeren flere ganger inntil maskinen finner at avtrykket avleses på samme måte hver gang og godkjenner registrering.

Avtrykket behandles av registreringsenheten. Først velges det ut visse punkter fra mønsteret i fingeravtrykket etter en regel som kan variere fra enhet til enhet. Disse punktene vil ha ulike verdier alt etter utseendet til de deler av mønsteret som faller sammen med punktene.

Disse verdiene behandles så etter en regneregul (en algoritme) som danner en "template",¹ denne templatens lagres så i enheten for tilgangskontroll. Det er gjerne et lite antall punkter som velges ut, i saken er det opplyst at det benyttes 50 punkter. Dette er for få punkter til at det er mulig å regenerere fingeravtrykket ved hjelp av templatens. Om det skal være mulig, må det registreres nok punkter til at det kan regenereres et bilde – en vanlig telefaks har en oppløsning på 90 000 punkter per kvadrattomme, som gir et inntrykk av hva som kreves for å lagre avtrykket som et "bilde". Men punktene er tilstrekkelig til at sannsynligheten for at to ulike fingrer skal generere samme template er svært små, også sammenlignet med sannsynligheten for at en uvedkommende skal finne frem til et passord valgt av bruker.

Når brukeren skal trene, trekkes fingeren over leseren på ny. Punkter registreres etter regelen, og det beregnes en verdi. Denne sammenlignes med den registrerte verdi, dvs templatens. For å godkjennes, må den beregnede verdien ligge innenfor en definert grense for avvik, ellers avvises forsøket på å få adgang.

Dette er en forenklet og prinsipiell fremstilling av bruken. I saken benyttes en teknikk som svarer til dette. I praksis er det både raskt og enkelt for brukeren å få adgang på denne måten.

¹ På norsk brukes gjerne uttrykket "mal" for det engelske "template", men i vedtaket er det brukt samme terminologi som i sakens dokumenter.

6.3 Personopplysningsloven § 12

Personopplysningsloven § 12, 1. ledd lyder:

Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.

Det følger av forarbeidene (Ot prp nr 92 (1998-99) side 114, 1. spalte):

Bestemmelsen gir en generell regulering av bruk av fødselsnummer og andre entydige identifikasjonsmidler som for eksempel fingeravtrykk og andre biometriske data. Slike identifikasjonsmidler bør ikke benyttes i utrengsmål. Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f.eks navn, adresse og kundennummer ikke er tilstrekkelig. Det vil også ha betydning hvor viktig sikker identifisering er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt.

Spørsmålet for Personvernemnda er om personopplysningsloven § 12 kommer til anvendelse i denne saken.

Betegnelsen "identifikasjonsmiddel" kan ha ulike tolkninger. For det første kan et identifikasjonsmiddel være "noe" som brukes for å gjenfinne opplysninger om én enkelt, på forhånd kjent person i en stor mengde med data, typisk en database. I en database vil det være en "nøkkel", denne nøkkelen vil måtte være entydig, ellers vil opplysninger om flere personer kunne forveksles. Fødselsnummer er en slik entydig identifikasjonsnøkkel. For det annet kan et identifikasjonsmiddel benyttes til autentisering etter at identifiseringen har funnet sted. Identifisering kan skje på en måte, for eksempel ved fødselsnummer. Når kandidaten for autentisering er funnet, skal man sikre at sannsynligheten for identitet er høy, i alle fall høyere enn den man får ved bruk av navn og fødselsdato. Nemnda har i sak PVN-2006-10 (Esso Norge) kommet til at personopplysningsloven § 12 dekker begge former for bruk av "identifikasjonsmiddel" når bruk av fingeravtrykk til autentisering er en del av et system for sikker identifisering.

Nemnda er i utgangspunktet av den oppfatning at fødselsnummer og fingeravtrykk ikke nødvendigvis kan sammenlignes. Loven forutsetter at fødselsnummer kan brukes som "entydig identifikasjonsmiddel". Med "entydig" sikter loven åpenbart til noe mer enn at identifikasjonen er entydig i forhold til det enkelte system. En identifikasjon må selvsagt være entydig innen systemets rammer, ellers vil den ikke kunne benyttes til oppslag. I denne forstand vil for eksempel en kundeidentifikasjon (KID) også være entydig i forhold til systemet for de aktuelle kunder. Når loven krever at identifikasjonsmiddelet må være entydig, kreves det altså noe *mer*. Nemnda legger til grunn at loven må tolkes slik at identifikasjonsmiddelet må være egnet til bruk som identifikasjon i *flere* systemer. Fødselsnummeret vil i denne forstand være et entydig identifikasjonsmiddel, fordi det er en nøkkel til å gjenfinne informasjon i flere ulike systemer. Fingeravtrykk vil også være et entydig identifikasjonsmiddel i denne forstand fordi samme avtrykk kan brukes for å få tilgang til flere system. Fødselsnummeret vil være velegnet til identifikasjon, men er helt uegnet til autentisering (legitimasjon). Fingeravtrykket kan derimot brukes til begge deler.

Som den innledende presentasjonen (ovenfor i pkt 6.2) illustrerer, vil det internt i systemet ikke nødvendigvis brukes en nøkkel som er identisk med fingeravtrykket eller fødselsnummeret. Fingeravtrykket konverteres til en template, og denne templatene er i seg selv ikke et entydig identifikasjonsmiddel. Også et fødselsnummer kan behandles av et system slik at systemet selv bruker (og viser) et kryptert eller pseudonymisert nummer.

Personvernemnda forstår loven slik at den med "identifikasjonsmiddel" sikter til hva brukeren presenterer til systemet – et fingeravtrykk (som så behandles av systemets adgangskontroll) eller et fødselsnummer (som også kan f eks krypteres). Fingeravtrykket vil kunne brukes til å få tilgang til flere systemer, mens de ulike systemene i praksis vil konvertere det avleste avtrykket til ulike templer. Dette forhindrer ikke at fingeravtrykket anses som et "entydig identifikasjonsmiddel" i lovens forstand.

I det aktuelle systemet i denne saken vil fingeravtrykket avleses av en enhet i adgangskontrollen. Denne avlesningen behandles med sikte på å komme frem til en representasjon. Denne representasjonen bygger på avlesning av visse punkter i fingeravtrykket bestemt av den innebygde logikken i enheten. Representasjonen kan så sammenlignes med de templer som er lagret for fingeravtrykket til autoriserte brukere. Hvis sammenligningen ligger innenfor den forhåndsdefinerte margin for avvik, vil (1) brukeren være identifisert, og (2) brukeren være autentisert. Brukeren får dermed adgang til treningssenteret.

To av nemndas medlemmer (Leikny Øgrim og Jostein Halgunset) ønsker å opprettholde sin særmerknad. Det vises til PVN-2006-11 (Rema 1000).

6.4 Foreligger det "saklig behov", og er metoden "nødvendig for å oppnå slik identifisering"

Personopplysningsloven § 12 åpner for at man kan bruke entydige identifikasjonsmidler hvis særlige forhold foreligger.

I denne saken begrunnes bruken av fingeravtrykk med at medlemmene skal slippe å ta med medlemskort. Videre sikrer man at de personer som er medlem, har gyldig medlemskap, og metoden forebygger misbruk av personlige medlemskap.

Slik Personvernemnda ser det, er fordelene med slik bruk av fingeravleser at det er enkelt, praktisk og brukervennlig. Man behøver ikke å huske medlemskortet.

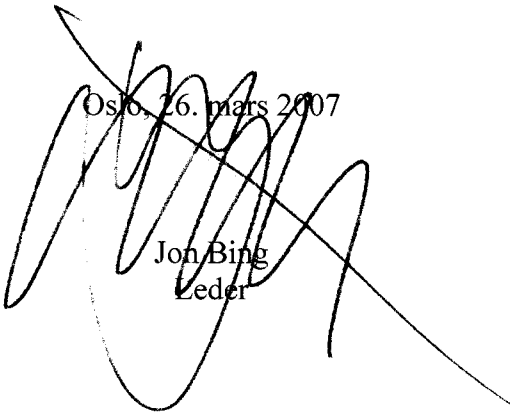
Imidlertid opplever enkelte personer bruk av fingeravtrykk som et inngrep i sin integritet. Dette kan ha sammenheng med at fingeravtrykk tradisjonelt sett er blitt brukt av politiet i forbindelse oppklaring av straffbare forhold. Det at politiet benytter fingeravtrykk i alvorlige kriminalsaker kan gi en opplevelse av mistenkeliggjøring når man må avgi fingeravtrykk i ulike dagligdagse situasjoner. Andre ulemper ved fingeravtrykksleser er at fingeravtrykkene legges igjen som spor i det daglige liv og det er fare for at dataene kan brukes til andre formål enn de formål de opprinnelig ble samlet inn for.

Personvernemnda er kommet til at treningssenteret kan sies å ha et saklig behov for sikker identifisering ved adgangskontrollen. Spørsmålet er imidlertid om kravet til nødvendighet er oppfylt. Det følger av forarbeidene at bruk av entydige identifikasjonsmidler ikke skal tillates dersom "andre og mindre sikre identifikasjonsmidler, som for eksempel navn, adresse og kundenummer" er tilstrekkelig. Etter nemndas syn kan treningssenteret benytte seg av "andre og mindre sikre identifikasjonsmidler" som likevel tilfredsstiller treningssenterets behov. Nemnda aksepterer argumentet om at bruk av fingeravtrykksleser gir medlemmene en enkel inngang og treningssenteret en god adgangskontroll. Dette er imidlertid ikke nok. I følge forarbeidene kreves det noe mer. Det må i tillegg være slik at det ikke kan tas i bruk en løsning som *ikke* forutsetter bruk av et entydig identifikasjonsmiddel, og som gir samme sikkerhet. Nemnda legger til grunn at det finnes tilfredsstillende alternativer som er sikkert nok for treningssenterets formål og behov. Nemnda viser til eksemplene i Datatilsynets vedtak.

Etter en konkret vurdering er Personvernemnda kommet til at i denne situasjonen er ikke bruk av fingeravtrykksleser nødvendig for å oppnå sikker identifisering. Den planlagte bruken er derfor ikke tillatt, jf personopplysningsloven § 12.

7 Vedtak

Klagen tas ikke til følge.



Oslø, 16. mars 2007

Jon Bing
Leder

Sammendrag til bruk ved publisering:

PVN-2006-09 Oslo trimsenter – fingeravtrykkspålogging. Klage over at Datatilsynet stanset bruk av fingeravtrykksleser i adgangskontrollen ved treningssenteret Oslo trimsenter.

Datatilsynet mente at det kunne sies å foreligge et saklig behov for sikker identifisering i tilknytning til adgangskontrollen, men at lovens krav til nødvendighet ikke var oppfylt.

Personvernemnda var enig i Datatilsynets vurdering og tok ikke klagen til følge. Nemnda mener at treningssenteret kan benytte seg av ”andre og mindre sikre identifikasjonsmidler”, som likevel er sikkert nok til å tilfredsstille treningssenterets behov.