

PVN-2006-11 REMA 1000 – fingeravtrykk ved registrering av timer

Klage på Datatilsynets vedtak om at REMA 1000 må avslutte bruken av fingeravtrykk ved timeregistrering for de ansatte.

Personvernemndas avgjørelse av 9. mars 2007 (Jon Bing, Gro Hillestad Thune, Leikny Øgrim, Siv Bergit Pedersen, Jostein Halgunset, Hanne I Bjurstrøm, Tom Bolstad)

Datatilsynets referanse: 06/00180-7/AFL

1 Innledning

Personvernemnda har ved oversendelse fra Datatilsynet mottatt klage fra REMA 1000 på Datatilsynets vedtak om at REMA 1000 må avslutte bruken av fingeravtrykk i forbindelse med timeregistrering for de ansatte.

2 Saksgang

Datatilsynet mottok tidlig i 2006 spørsmål fra ansatte i REMA 1000 knyttet til selskapets bruk og planlagte bruk av fingeravtrykk. På bakgrunn av disse spørsmålene ble det 16.2.2006 sendt et brev til REMA 1000 hvor Datatilsynet redegjør for reglene i personopplysningsloven § 12 og ber om en tilbakemelding om den planlagte bruken.

I brev av 6.3.2006 redegjør butikkjeden for innføring av en timeregistreringsterminal som innebærer bruk av fingeravtrykk til verifisering av den ansattes identitet.

I brev av 10.4.2006 fattet tilsynet pålegg om at bruken av fingeravtrykk må opphøre. I brev av 9.5.2006 bekrefter REMA 1000 at bruken av fingeravtrykk er opphørt.

I brev av 18.5.2006 påklages Datatilsynets vedtak i saken.

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
Nydalen
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

3 Faktum

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

Datatilsynet fattet følgende vedtak:

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

4 Anførlene

Klager anfører at formålet med løsningen er å forenkle det administrative arbeidet for kjøpmennene knyttet til butikkens bemanningsplaner og utbetaling av lønn, herunder sikre at det utbetales korrekt lønn. I motsetning til stemplingskort og kode, gir bruken av fingeravtrykk ved timeregistreringen sikker identifisering av den ansatte.

Klager anfører at grunnlaget for behandlingen er i personopplysningsloven § 8 a eller alternativt § 8 f. Det er behov for sikker identifikasjon, jf personopplysningsloven § 12, av når de 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 til stede i hele åpningstiden.

Fingeravtrykk er nødvendig fordi det er mange ansatte, opptil 50 i hver butikk. 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. Slik manuell registrering er ikke 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, jf ordlyden i personopplysningsloven § 12. Klager anser at bruk av fingeravtrykk gir sikker identifisering. Dette endres ikke av at det valgte system også har andre administrative funksjoner.

Bruk av kort og kode medfører ikke nødvendigvis at registreringene er korrekt, fordi et slikt system åpner for så vel utilsiktede som tilsiktede feilregistreringer. Feiltasting kan medføre at ansatte får utbetalt feil lønn, fordi det blir registrert for kort eller for lang arbeidstid. Klager har erfaring med at de ansatte bruker hverandres koder og stemplingskort og at man derfor ikke får korrekte data om hvem som har vært på jobb. Kort har dessuten den ulempe at de ansatte relativt ofte mister eller glemmer kortet og at det kan bli ødelagt.

Datatilsynet tar feil når det hevder at nødvendighetskravet ikke er oppfylt når man ved andre metoder kan oppnå sikker identifisering i "tilstrekkelig grad". REMA 1000 kan kun akseptere helt sporadiske feilregistreringer. Loven kvalifiserer ikke 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 til de økonomiske konsekvenser av feilregistreringer.

Klager anfører at verken timeregistreringsterminalen eller programvaren lagrer et grafisk bilde av de ansattes fingeravtrykk. Fingeravtrykket blir lagret lokalt i terminalen i form av en streng med binærkoder som er generert via en algoritme. Det er ikke mulig å gjenskape fingeravtrykk på basis av denne. Det er opplyst at tidsterminalen og fingeravtrykket ikke kan benyttes til noen form for adgangskontroll. Binærkoden skal ikke overføres i nettverk.

Klager anfører til slutt at det ikke er problematisk i forhold til de ansattes personvern at det benyttes fingeravtrykk. Det er ikke fare for at opplysningen kommer på avveie. I forhold til bruk av stemplingskort eller kode som identifikasjonsmiddel, er den eneste forskjellen at bruk av fingeravtrykk sikrer at de registrerte dataene om tilstedeværelse i butikken faktisk er korrekte. Personopplysningslovens § 11 ivaretas gjennom hele systemet.

5 Datatilsynets vurdering

Datatilsynet anser at et fingeravtrykk, også når dette benyttes til å utarbeide et template, er å anse som et entydig identifikasjonsmiddel og bruken skal følge reglene i 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 og samlet oversendelsesbrev til Personvernemnda.

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 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 § 12. Det er opplyst at de ansatte skal benytte en ansattkode eller ID-nummer i tillegg til fingeravtrykk. Identifisering skjer ved hjelp av ansattkoden, mens fingeravtrykket fungerer som legitimasjon eller verifisering av påstått identitet i systemet. Formålet med § 12 er nettopp å forhindre slik bruk av entydige identifikasjonsmidler.

Datatilsynet mener at lovens krav til nødvendighet heller 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. Man kan oppnå tilstrekkelig sikker identifisering sett hen til formålet ved å benytte ansattnummer, ID-nummer, i kombinasjon med en personlig kode eller passord. Det er mulig at passord kommer på avveie med eller uten den ansattes vilje. Tilsynet antar imidlertid at dette kun skjer sporadisk. Selv om samfunnet er tjent med at svindel bekjempes, fremstår bruk av fingeravtrykk verken som nødvendig eller forholdsmessig i denne sammenheng.

Når det gjelder feiltasting, mener Datatilsynet at dette antakelig skjer noe oftere, men at hver enkelt ansatt er forpliktet til å kontrollere sin lønnsutbetaling og gi tilbakemelding dersom det er oppstått en feil.

Når det gjelder anførselen om at fingeravtrykkskontroll er nødvendig fordi manuell kontroll er for ressurskrevende og umoderne og at arbeidsgiver ikke er til stede hele åpningstiden, vil Datatilsynet bemerke at dette ikke er tilstrekkelig for å oppfylle nødvendighetskriteriet.

6 Personvernemndas 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.

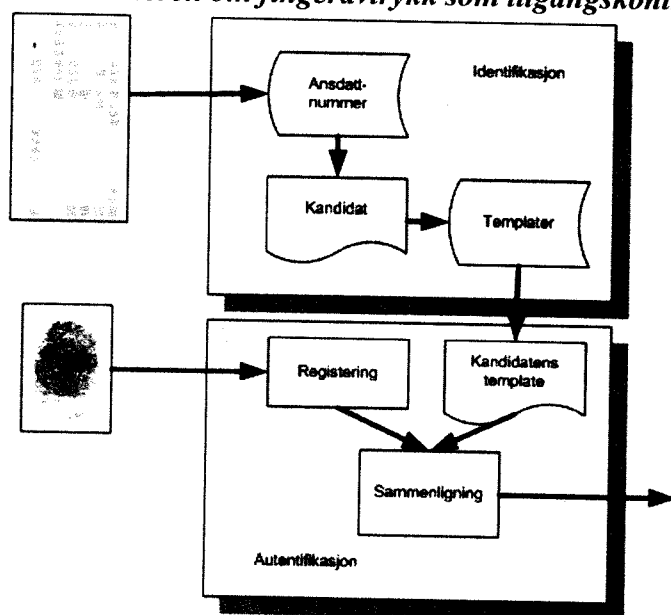
I svensk og dansk rett finnes det ingen bestemmelse tilsvarende den norske personopplysningsloven § 12 – for øvrig finnes det heller ingen bestemmelse som tilsvarende den norske personopplysningsloven § 12 i personverndirektivet. I Sverige og Danmark benytter man derfor de vanlige reglene, tilsvarende 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. To av behandlingsgrunnlagene som § 8 gir anvisning på er *litra a*) å oppfylle en avtale med den registrerte, og *litra f*) den behandlingsansvarlige skal vareta en berettiget interesse og hensynet til den registrertes personvern overstiger ikke denne interessen. Personvernemnda legger til grunn at arbeidsavtalen skal oppfylles ved å utbetale korrekt lønn til de ansatte. 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 tilgangskontroll



Ved bruk av fingeravtrykk for å gi tilgang til en terminal, erstatter lesing (skanning) av fingeravtrykket bruk av passord, eventuelt både brukernavn og passord. Brukeren har på forhånd registrert avtrykk av en eller flere fingrer ved å trekke fingeren over en smal skanner (optisk leser) integrert i terminalen. Ved første gangs registrering trekkes som regel fingeren flere ganger over skanneren 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 et "template".¹ Dette templatet lagres så i enheten for tilgangskontroll. Det er gjerne et lite antall punkter som velges ut. I saken er det ikke opplyst hvor mange punkter som registreres, men det er opplyst at det er så få punkter at det ikke er mulig å regenerere fingeravtrykket ved hjelp av templatet. Om det skal være mulig, må det registreres nok punkter til at det kan regenereres et bilde – en vanlig telefaks har en oppløsning på 9000 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 benytte terminalen, trekkes fingeren over leseren på ny. Punkter registreres etter regelen, og det beregnes en verdi. Denne sammenlignes med den registrerte

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

verdi, dvs templatet. For å godkjennes, må den beregnede verdien ligge innenfor en definert grense for avvik. Hvis avlesningen er vellykket, det vil si at fingeravtrykk og ansattnummer stemmer overens, kan timeregistreringen begynne.

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 tilgang på denne måten.

6.3 Personopplysningsloven § 12

6.3.1 Fingeravtrykk som "entydig identifikasjonsmiddel"

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 (98-99) 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" er ikke klar. Det 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 et "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 og fingeravtrykk 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 den ansatte taste sitt ansattnummer eller ID-nummer (identifiseringsfasen). Deretter avleses fingeravtrykket av en enhet integrert i terminalen (autentiseringsfasen). 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 det templatet som er lagret for fingeravtrykket til en autorisert bruker. Hvis sammenligningen ligger innenfor den forhåndsdefinerte margin for avvik, vil (1) brukeren være identifisert, og (2) brukeren være autentisert, det vil si at fingeravtrykk og ansattnummer stemmer overens. Nemnda viser til PVN-2006-10 (Esso Norge) for en nærmere beskrivelse av bruk av fingeravtrykk til autentisering.

En særmerknad:

To av nemndas medlemmer (Leikny Øgrim og Jostein Halgunset) har et avvikende syn på hvilken vekt som skal legges på forarbeidenes uttalelse om at personopplysningsloven § 12 gjelder *"bruk av fødselsnummer og andre entydige identifikasjonsmidler som for eksempel fingeravtrykk og andre biometriske data"*. Medlemmene mener det er uheldig å låse lovtolkningen på grunnlag av en kort bemerkning i lovforarbeidene, som åpenbart ikke er bygget på en nærmere vurdering av hvilke ulike måter fingeravtrykk kan brukes på og som derfor framstår som svært summarisk og lite nyansert. Fødselsnummer og fingeravtrykk er prinsipielt såpass forskjellige størrelser at de ikke kan betraktes som beslektet annet enn i noen spesielle anvendelser. Når *"fingeravtrykk og andre biometriske data"* i lovforarbeidene omtales som *"andre entydige identifikasjonsmidler"* enn *"fødselsnummer"*, må man derfor anta at forfatteren her har siktet til situasjoner hvor fingeravtrykk benyttes på en måte som har likhetstrekk med den måte fødselsnummer benyttes på, og hvor man altså teoretisk kunne velge mellom å bruke det ene eller det andre. Dette er ikke tilfelle i den foreliggende saken. Fingeravtrykk kan benyttes til å verifisere at det er riktig person som forsøker å logge seg på en datamaskin. Fødselsnummeret kan ikke brukes til dette formålet. Ut fra dette virker det ikke som personopplysningsloven § 12 er ment å skulle regulere situasjoner som den vi her har med å gjøre.

Om man likevel skulle komme til at fingeravtrykk prinsipielt er å oppfatte som *"entydig identifikasjonsmiddel"*, fordi det i noen situasjoner kan brukes analogt med fødselsnummer, og at det derfor faller innenfor personopplysningsloven § 12 uansett konkret anvendelse, vil man likevel ikke kunne oppfatte templatet av fingeravtrykk på denne måten. Det er vanskelig å se noen mulighet til å bruke template av fingeravtrykk som erstatning for fødselsnummer, eller omvendt. Det er ikke mulig å etablere noen en-til-en-relasjon mellom en fysisk person og et template. Argumentet om at templatet etableres ved hjelp av fingeravtrykksmønsteret og at registreringsprosedyren derfor innebærer behandling av fingeravtrykk, og altså behandling av *"entydig identifikasjonsmiddel"*, selv om templatet i seg selv ikke er entydig, virker søkt. I personopplysningsloven § 2 defineres *"behandling"* som *"innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter"*. Men siden fingeravtrykket som sådan verken samles inn eller registreres, skjer det i henhold til lovens definisjon heller ingen behandling. Konklusjonen må derfor bli at personopplysningsloven § 12 ikke kommer til anvendelse i den foreliggende saken. Personvernemndas argumentasjon går ikke nærmere inn på dette.

6.3.2 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 er metoden ønsket for å sikre at de ansatte registrerer timene sine korrekt og for å hindre misbruk i form av at de ansatte bruker hverandres stemplingskort og koder. Hovedformålet med innføringen av fingeravtrykksleser er å forhindre at de ansatte deler passordet sitt med hverandre og dermed fører timer på andre enn seg selv. Fingeravtrykkspålogging ved timeregistrering skal skje for å verifisere at ansattnummer og fingeravtrykk stemmer overens (autentisering).

Personvernemnda mener at lovens vilkår om saklig behov er oppfylt. Det foreligger et saklig behov for sikker identifisering i forbindelse med timeregistrering. I forbindelse med lønnsutbetaling er det viktig både for bedriften og den ansatte at korrekt timeregistrering er utført og at feilregistreringer forhindres.

Spørsmålet blir, slik Personvernemnda ser det, hvorvidt kravet til nødvendighet er oppfylt. Etter forarbeidene skal ikke bruk av entydige identifikasjonsmidler tillates dersom "andre og mindre sikre identifikasjonsmidler, som for eksempel navn, adresse og kundennummer" er tilstrekkelig. Datatilsynet har sett det slik at tilfredsstillende sikkerhet kan oppnås ved bruk av ansattnummer eller ID-nummer, i kombinasjon med en personlig kode eller passord.

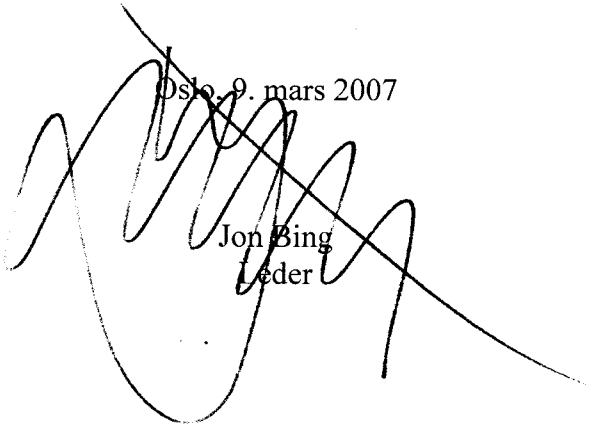
Personvernemnda tar utgangspunkt i at fingeravtrykksleser skal benyttes for å hindre at de ansatte bruker hverandres koder eller deler passordet sitt og fører timer på andre enn seg selv. Etter nemndas syn innebærer en innføring av fingeravtrykksleser ved timeregistrering en unødvendig mistenkeliggjøring av de ansatte. Innføring av fingeravtrykksleser vil naturlig bli oppfattet som en strengere form for kontroll av de ansatte enn ordinær timeregistrering ved stempling og lignende. Slik innføring av fingeravtrykksleser vil gi et sterkere signal om at man ikke kan stole på de ansatte enn de mer tradisjonelle løsningene. Etter nemndas mening vil et slikt system bidra til å svekke, heller enn å styrke, tillitsforholdet mellom ansatt og arbeidsgiver.

Etter nemndas oppfatning kan REMA 1000 benytte seg av "andre og mindre sikre identifikasjonsmidler" som likevel tilfredsstiller butikkjedens behov. Nemnda aksepterer argumentet om at bruk av fingeravtrykksleser gir butikkjeden en god og sikker kontroll. 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 tilfredsstillende sikkerhet. Nemnda legger til grunn at det finnes adekvate alternativer som er sikre nok for butikkjedens formål og behov. Nemnda viser til eksemplene i Datatilsynets vedtak.

Personvernemnda er etter en konkret vurdering kommet til at det i denne situasjonen foreligger et saklig behov for sikker identifisering, men at den valgte metoden ikke er nødvendig for å oppnå dette. Den planlagte bruken er derfor ikke tillatt, jf personopplysningsloven § 12.

7 Vedtak

Klagen tas ikke til følge.



Oslo, 9. mars 2007

Jon Bing
Leder

Sammendrag til bruk ved publisering:

PVN-2006-11 (REMA 1000). Fingeravtrykkspålogging.
REMA 1000 har påklaget Datatilsynets vedtak om at REMA 1000 må avslutte bruken av fingeravtrykk i forbindelse med timeregistrering for de ansatte. Registrering i terminalen skjer ved at den ansatte taster sitt ansattnummer eller ID-nummer. Deretter blir vedkommende bedt om å legge en finger på leseplaten eller sensoren for å verifisere at det er tastet riktig nummer. 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 § 12. Identifisering skjer ved hjelp av ansattkoden, mens fingeravtrykket brukes til autentisering, noe som faller utenfor § 12. Datatilsynet mener at lovens krav til nødvendighet heller ikke er oppfylt. Personvernemnda har i sak PVN-2006-10 (Esso Norge) kommet til at personopplysningsloven § 12 dekker begge former for bruk av et "identifikasjonsmiddel" når bruk av fingeravtrykk til autentisering er en del av et system for sikker identifisering. Personvernemnda mener at det foreligger et saklig behov for sikker identifisering i forbindelse med timeregistrering. Imidlertid finner nemnda at nødvendighetsvilkåret ikke er oppfylt. Etter nemndas oppfatning kan REMA 1000 benytte seg av "andre og mindre sikre identifikasjonsmidler" som likevel tilfredsstiller butikkjedens behov. Klagen tas derfor ikke til følge.