



Brevdato: 12. juli 2006
Modtager: Louis Mølholm Security
J.nr. 2005-219-0295

Stikord: Biometri, fingeraftryk, personoplysninger, Datatilsynets praksis, smart card.

Vedrørende behandling af personoplysninger på biometrisk smart card

Ved e-post af 13. april 2005 har De rettet henvendelse til Datatilsynet og spurgt om brug af biometriske smart card for patienter, der lider af Parkinson's syge, vil være i overensstemmelse med persondataloven.

Ved e-post af 27. april 2005 har De sendt supplerende materiale til sagen.

Deres forespørgsel tager udgangspunkt i et projekt, der har fundet sted i Holland. Formålet med anvendelse af et smart card er efter det oplyste at effektivisere kommunikationen mellem forskellige parter i sundhedsvæsenet. De involverede parter er læger, apotekere, hospitaler, patienter og et forsikringsselskab.

Det biometriske kort er udstedt til klienterne og fungerer som nøgle i kommunikationen med adskillige software applikationer. Der er tale om et smart card med integreret fingeraftryksscanner, hvor registrering samt autentificering kun finder sted ved anvendelse af kortet, uden at data forlader kortet under processerne. Det vil sige, at matchværdien af personens fingeraftryk ikke vil blive lagret i en central database. På kortet lagres bl.a. oplysninger om receptdata, udleveret medicin samt persondata.

Det er endvidere oplyst, at systemet fungerer således, at hospitalets konsulterende neurolog er i stand til at indlæse og aflæse indholdet af kortet samt registrere fingeraftrykkets template (matchværdi) - denne er gemt på kortet sammen med receptinformation. Efter den først registrering er kun verifikation nødvendig, når det biometriske kort benyttes. Ved patientens besøg på apoteket aflæses receptdata på et kortet ved hjælp af apotekets applikation, men først efter at patientens autentificering med fingeren har fundet sted. Apoteket udleverer den foreskrevne medicin og gemmer informationen på kortet. Næste gang hos neurologen kan en komplet medicinliste aflæses fra kortet og gemmes. Alle professionelle, som er involveret, har også deres eget smart card, som fungerer som autorisation og challenge response for patientens kort.

De har oplyst, at De ønsker Datatilsynets udtalelse om, hvorvidt løsninger, hvor biometri gemmes på kort, er at foretrække frem for løsninger med databaser.

Datatilsynet skal – efter sagen har indgået i en drøftelse af biometri i Data-rådet – udtale følgende:

1. Persondatalovens regler for behandling af biometriske oplysninger

Persondataloven¹ gælder ifølge lovens § 1, stk. 1, for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Loven gælder tillige for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden, jf. § 1, stk. 2.

Ved *personoplysninger* forstås ifølge lovens § 3, stk. 1, enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).

Begrebet *behandling* omfatter ifølge lovens § 3, nr. 2, enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for. Ifølge lovens forarbejder omfatter dette eksempelvis indsamling, opbevaring, brug og videregivelse.

Det er Datatilsynets opfattelse, at der såvel i forbindelse med indsamling (indrolering) af fingeraftryk, som ved den efterfølgende brug (matchning) af templatens af aftrykket i forbindelse med den biometriske løsning, er tale om behandlinger af personoplysninger omfattet af persondataloven.

Et fingeraftryk eller en matematisk værdi af et fingeraftryk – en såkaldt template – må efter Datatilsynets opfattelse anses for en almindelig ikke-følsom oplysning omfattet af persondatalovens § 6.

Behandling af almindelige ikke-følsomme oplysninger skal ske i overensstemmelse med persondatalovens § 6, stk. 1, nr. 1-7. Behandling kan herefter bl.a. ske, hvis den registrerede har givet udtrykkeligt samtykke hertil, jf. § 6, stk. 1, nr. 1. Behandlingen kan endvidere finde sted, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, jf. § 6, stk. 1, nr. 3, eller hvis behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse, jf. § 6, stk. 1, nr. 7.

Oplysninger om udleveret medicin samt receptdata er efter Datatilsynets opfattelse oplysninger om helbredsmæssige forhold omfattet af persondatalovens § 7. Ifølge lovens § 7, stk. 1, må der ikke behandles oplysninger om bl.a. helbredsmæssige oplysninger. I lovens § 7, stk. 2 - 8, findes en række undtagelser til § 7, stk. 1. Bestemmelsen i stk. 1 finder f.eks. ikke anvendelse, hvis den registrerede har givet sit udtrykkelige samtykke til den pågældende behandling, jf. § 7, stk. 2, nr. 1.

¹ Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger som ændret i lov nr. 280 af 25. maj 2001. Loven kan ses på Datatilsynets hjemmeside www.datatilsynet.dk under punktet "Lovgivning".

I den forbindelse bemærkes, at den registreredes samtykke i lovens § 3, nr. 8, er defineret som enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Herudover indeholder persondataloven i § 5 grundlæggende principper for den dataansvarliges behandling af oplysninger, som altid skal iagttages. Det følger således af § 5, stk. 1, at oplysninger skal behandles i overensstemmelse med god databehandlingskik. Det betyder ifølge lovens forarbejder, at behandlingen skal være rimelig og lovlig.

Af lovens § 5, stk. 2, fremgår, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål.

Ifølge lovens § 5, stk. 3, skal oplysninger, der behandles, være relevante og tilstrækkelige og må ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil de senere behandles.

2. Tilsynets praksis om behandling af biometriske oplysninger

2.1. I 1988² behandlede Registertilsynet en forespørgsel fra en virksomhed om, hvorvidt anvendelse af et biometrisk fingeraftryksbaseret adgangskontrolsystem ville være i overensstemmelse med registerlovgivningen.

Det var oplyst, at systemet tænkes anvendt som adgangskontrol til områder, hvor et specielt højt sikkerhedsniveau var påkrævet f.eks. computerrum, banker, politiafdelinger mv.

Autorisationen af personer til det beskyttede område skulle ske ved, at systemets fingeraftrykslæser foretog en skanning af én af personens fingre, og at der på grundlag heraf dannedes en matematisk kode, der blev lagret i systemet sammen med én af den autoriserede valgt kode. Når den således autoriserede person herefter ønskede adgang til det beskyttede område, indtastedes den valgte kode, og fingeren blev skannet på ny. Ved hjælp af den indtastede kode blev den ved autorisationen lagrede matematiske kode fundet, og der blev foretaget en sammenligning med det nye aflæsningsresultat. Såfremt der kunne konstateres overensstemmelse, blev der givet adgang. Det var oplyst i sagen, at det var muligt at udskrive de lagrede matematiske koder, men at disse på ingen måde kunne konverteres til det oprindelige fingeraftryk, og at dette var tilfældet, uanset om man måtte have adgang til og forståelse for den anvendte teknologi.

Registertilsynet udtalte, at den lagring af valgte koder med tilhørende matematiske koder, der skete ved autorisation, indebar en registrering af personoplysninger som nævnt i lovens § 1, og at registreringens lovlighed herefter ville afhænge af en vurdering af, hvorvidt registreringsbetingelserne i lovens § 3, stk. 1, var opfyldt. Registertilsynets fandt, at anvendelse af systemet som adgangs-

² Sagen er omtalt i Registertilsynets årsberetning 1988 s. 57.

kontrol til områder, hvor der er behov for en særlig skærpet kontrol ikke ville være i strid med lov om private registre mv. § 3, stk. 1.

Endeligt bemærkede Registertilsynet, at reglerne i lov om offentlige myndigheders registre ville skulle iagttages, såfremt offentlige myndigheder agtede at anvende udstyr af den omhandlede art.

2.2. I sagen³ vedrørende BornholmsTrafikkens nye ID-kort udtalte Datatilsynet, at behandling af oplysninger om kunders fingeraftryk i ID-kortet kunne finde sted inden for rammerne af persondatalovens regler.

Sagen vedrørte BornholmsTrafikkens udstedelse af "Bornholmerkortet", som er et personligt chipkort, der indeholder en "værdi" af kundens fingeraftryk. I forbindelse med påbegyndelse af rejsen kører kunden kortet gennem en kortlæser og sætter samtidig sin finger på en scanner, og hvis scanneren kan matche kundens fingeraftryk med værdien i chippen på kortet, gives der adgang for kunden. Oplysninger om de udregnede værdier blev efter det oplyste ikke opbevaret i forbindelse med lagringen af oplysninger på kortet eller i forbindelse med scanning af kort og fingeraftryk ved check-in. Der var således ikke en central database med disse oplysninger.

Det var Datatilsynets opfattelse, at BornholmsTrafikkens behandling af oplysninger i forbindelse med udstedelse af kortet og i forbindelse med, at kunden identificerer sig ved check-in, kunne ske i medfør af persondatalovens § 6, stk. 1, nr. 1, 2 og 7. Datatilsynet lagde i den forbindelse vægt på, at kunden frivilligt har valgt at benytte rabatkortet "Bornholmerkortet", samt at den udregnede værdi alene opbevares på kundens eget kort, og hverken værdien eller fingeraftrykket opbevares eller lagres andre steder. Endvidere fandt Datatilsynet, at behandlingen ikke var i strid med proportionalitetsprincippet.

2.3. Vedrørende behandling af personoplysninger i et biometrisk adgangssystem i et motionscenter, hvor de biometriske oplysninger blev lagret i en central database, har Datatilsynet i en specifik sag udtalt, at den konkrete behandling ikke ville kunne ske inden for rammerne af persondatalovens regler⁴.

Henvendelsen vedrørte et adgangssystem til et motionscenter, hvor medlemmer af motionscenteret ved indgangen får aflæst sit fingeraftryk på en scanner, der udregner en matchværdi, som efterfølgende holdes op mod motionscenterets medlemsdatabase. Udregningen af matchværdien sker i scanneren, og scanningen af fingeraftrykket forlader således ikke scanneren. Oplysningerne bliver behandlet med medlemmets samtykke og slettes, når et medlemskab ophører. Som baggrund for systemet var anført, at mange motionscentre i dag benytter sygesikringsbeviset som adgangskort, men at dette rummer en række ulemper. Der kan eksempelvis ikke gives adgang, hvis medlemmet har glemt sit kort, ligesom der er en risiko for misbrug, idet kortet ikke er forsynet med billede. Et egentligt medlemskort med billede kan imødegå problemet med misbrug,

³ Sagen er omtalt i Årsberetning 2003 side 85.

⁴ Udtalelsen kan ses på www.datatilsynet.dk under punktet "Værd at vide" – "Udtalelser i 2000-2004" under brevdato 26. november 2004.

men det er tidskrævende at kontrollere alle billeder, ligesom det ikke eliminerer ulempen ved at glemme kortet.

Det var Datatilsynets umiddelbare vurdering, at den i sagen beskrevne behandling ikke vil kunne ske inden for rammerne af persondatalovens regler. Datatilsynet lagde herved vægt på, at formålet med behandlingen ikke synes at stå mål med, hvor indgribende en behandling der var tale om. Hensynet til at etablere en adgangskontrol i et motionscenter uden brug af kort kunne efter Datatilsynets umiddelbare opfattelse ikke retfærdiggøre behandlingen af matchværdier i en central database. Det var Datatilsynets vurdering, at det ønskede formål kunne forfølges med mindre indgribende midler.

2.4. Datatilsynet har besvaret en forespørgsel om brug af en billeddatabase i forbindelse med adgangskontrol til Tivoli⁵. Datatilsynet udtalte i den forbindelse, at Tivolis indsamling og registrering af billeder ikke generelt kunne ske i medfør af persondatalovens § 6, stk. 1, nr. 2 eller nr. 7. Datatilsynet lægger herved vægt på, at den behandling af personoplysninger, som Tivoli ønsker, ikke fuldt ud kan anses for nødvendig af hensyn til opfyldelse af en aftale, jf. § 6, stk. 1, nr. 2, ligesom tilsynet ikke finder at kunne udelukke, at der i konkrete tilfælde kan være modstående hensyn, som overstiger Tivolis interesse i behandlingen, jf. § 6, stk. 1, nr. 7. Datatilsynet antog således, at der ville være personer, som ville føle ubehag ved at skulle have deres billede registreret, og som ville foretrække en anden løsning, selv om det medfører ulemper for den pågældende.

Datatilsynet fandt derfor, at Tivoli bør basere sin behandling af digitale billeder af årskortholdere på et samtykke fra årskortholderen til, at Tivoli tager et billede af den pågældende og opbevarer det i en database, jf. herved persondatalovens § 6, stk. 1, nr. 1, for derved også at sikre den enkelte abonnent mulighed for i stedet at anvende billedlegitimation i forbindelse med årskortet.

2.5. Datatilsynet har udtalt, at behandling af oplysninger om en matematisk beregnet værdi – en såkaldt template - af flypassagerers fingeraftryk ved check-in af bagage, ville kunne ske, hvis passageren i overensstemmelse med den i sagen nærmere beskrevne procedure har givet sit udtrykkelige samtykke hertil, jf. persondatalovens § 6, stk. 1, nr. 1.

Det var tillige Datatilsynets opfattelse, at den behandling flyselskabet foretager af oplysninger om passagernes fingeraftryk ikke er i strid med sagligheds- og proportionalitetsprincippet, jf. § 5, stk. 2 og 3. Datatilsynet lagde herved vægt på, at der alene er tale om opbevaring (behandling) af en matematisk værdi af passagernes fingeraftryk (en såkaldt template) i en kortere periode, og at templaten ikke vil blive sammenstillet med andre identifikationsoplysninger om passageren - der vil således ikke ske en egentlig identificering af den enkelte person ud over behandlingen af dennes template.

⁵ Udtalelsen kan ses på www.datatilsynet.dk under punktet "Værd at vide" – "Udtalelser i 2006" under brevdato 24. januar 2006.

Datatilsynet lagde endvidere vægt på, at passagerer, der ikke ønsker at få sit fingeraftryk aflæst, har mulighed for at benytte en alternativ løsning - i form af manuel ID kontrol i forbindelse med bagageindlevering og påstigning.

2.6. I en anden sag om opbevaring og videregivelse af ansattes template af fingeraftryk, hvor behandlingen skete i en central database, har Datatilsynet udtalt, at denne behandling kunne ske indenfor rammerne af persondatalovens § 6, stk. 1, nr. 7. Datatilsynets fandt, at hensynet til den omhandlede virksomheds interesse i at sikre entydige identifikation af de personer, der gives adgang til såvel pengecentralen som pengeskabe vejer tungere end de ansattes interesse i, at oplysningerne om den ansattes template ikke behandles. Datatilsynet lagde vægt på, at der er tale om adgangskontrol til områder, hvor der opbevares store værdier, samt at det tillige er i den ansattes interesse, at risikoen for misbrug af dennes identitet så vidt muligt nedbringes.

Tilsynet lagde endvidere vægt på, at der alene er tale om behandling af en template af den ansattes fingeraftryk, at det efter det oplyste ikke vil være muligt at anvende templaten til at genskabe personens fulde fingeraftryk, og at templaten ikke kan anvendes i andre systemer.

For så vidt angik virksomhedens videregivelse af de ansattes template til virksomhedens kunde, var det tillige Datatilsynets opfattelse, at dette kunne ske i overensstemmelse med den af virksomheden beskrevne fremgangsmåde. Datatilsynet lagde herved vægt på, at der alene er tale om videregivelse af de ansattes template, og at løsningen indebærer en administrativ lettelse i forhold til de ansatte, såvel som risikoen for mistanke i forbindelse med identitetsmisbrug formindskes, hvilket tillige er i de ansattes interesse.

Datatilsynet henledte opmærksomheden på, at det er en forudsætning for Datatilsynets vurdering, at der indgås en skriftlig aftale mellem den omhandlede virksomhed og virksomhedens kunde, der skal modtage oplysninger om de ansattes template, som sikrer, at persondatalovens regler opfyldes.

3. På baggrund af Deres henvendelse kan Datatilsynet oplyse, at det er tilsynets opfattelse, at en løsning inden for det danske sundhedsvæsen må tage udgangspunkt i de eventuelle krav, de danske sundhedsmyndigheder måtte have til en sådan løsning. Uden involvering af disse myndigheder har Datatilsynet ikke grundlag for at foretage en vurdering af løsningen på området.

For så vidt angår valget mellem løsninger, hvor der sker en lagring af biometriske oplysninger i henholdsvis en database eller på et smart card, skal Datatilsynet bemærke, at løsninger med lagring på et smart card, set i lyset af hensynet til beskyttelse af personoplysninger, ofte vil være at foretrække, da den registrerede i sådanne tilfælde har oplysningerne i sin varetægt. Som den ovenfor refererede praksis viser, kan der imidlertid også foreligge tilfælde, hvor der er et sagligt behov for behandling af oplysninger i en database, og hvor hensynet til de registrerede ikke overstiger hensynet til den dataansvarliges interesse heri.

Datatilsynet skal for god ordens skyld gøre opmærksom på, at tilsynet forventer at offentliggøre dette brev på sin hjemmeside.