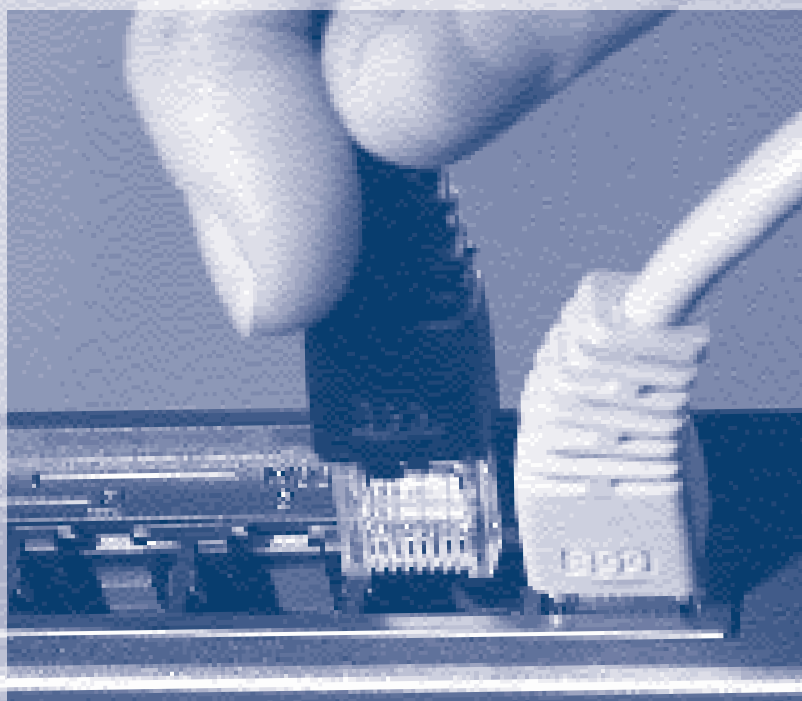


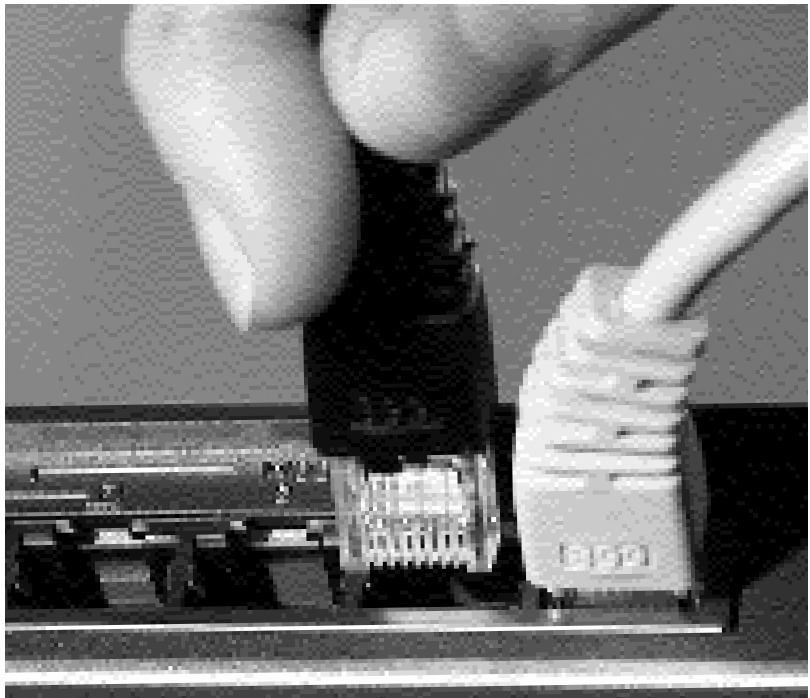
Datatilsynets årsberetning 2002



DATATILSYNET



Datatilsynets årsberetning 2002



Udgiver: Datatilsynet
Design: Kontrast design
Tryk: TrykNet
Beretningen er sat med Meta
Oplag: 400
November 2003
ISSN: 1601-5657
ISBN: 87-989860-0-7

Indhold

Til folketinget 5

Datatilsynets virksomhed i 2002 7

- Datatilsynets opgaver
- Datatilsynets organisation
- Persondataloven
- Datatilsynets hjemmeside
- Udveksling af oplysninger mellem myndigheder
- Statistiske oplysninger
- Udtalelser over lovforslag m.v.
 - *Ændring af arkivloven*
 - *Redegørelse om biobanker*
 - *Ændring af lov om offentlig sygesikring*
- *Forslag til en protokol om ændring af Europokonventionen*

Sager om behandling af personoplysninger 35

- Behandling af personoplysninger i videnskabeligt og journalistisk øjemed
- Fagforenings udsendelse af medlemsfortegnelse
- Fælles skadesregister for forsikringsbranchen
- Lokal-tv fra overvågningskameraer i indkøbscenter
- Offentliggørelse af situationsbilleder på internettet
- Sager om markedsføringsreglerne
 - *FDB's medlemsprogram*
- *Forskellige spørgsmål om indsigelsesreglen i lovens § 36, stk. 2*
 - *Samtykkekravet i bonusklubber*
- *TDC Forlags videregivelse af telefonbogsoplysninger*
- Sortliste over virksomheder i træbranchen
- Spørgsmål om frivillig registrering i et kreditoplysningsbureau
- Terminaladgang til Centralregisteret for Motorkøretøjer
- Transmission af live-video fra en pub
- Tv-overvågning i supermarkedskæde
- Videregivelse af oplysninger fra forskningsprojekter
- Videregivelse af oplysninger om indkomstforhold i forbindelse med ansøgninger om boligstøtte

Internationalt arbejde 75

Indledning
Europarådet
Den Europæiske Union
International konference for datatilsynsmyndigheder m.v.
Nordisk samarbejde

Sikkerhedsspørgsmål 91

Persondatalovens krav om datasikkerhed
OCES certifikater

Tilsynsvirksomhed

Generelt om Datatilsynets inspektioner
Gennemførelse af inspektioner
Formidling af resultater af inspektioner
Datatilsynets observationer ved inspektioner i 2002
Oversigt over udførte inspektioner i 2002





Til Folketinget

Hermed afgiver Datatilsynet sin årsberetning for 2002.

Beretningen afgives i henhold til § 65 i lov om behandling af personoplysninger (persondataloven), hvorefter Datatilsynet afgiver en årlig beretning om sin virksomhed til Folketinget.

Beretningen indeholder en beskrivelse af Datatilsynets aktiviteter i 2002, herunder referater af en række principielle sager om behandling af personoplysninger.

Hertil kommer et afsnit om det internationale arbejde, som Datatilsynet i årets løb har deltaget i, samt et afsnit om sikkerhedsspørgsmål, hvori de vigtigste aktiviteter vedrørende datasikkerhed omtales.

Endelig omtales i afsnittet om tilsynsvirksomhed de inspektioner (kontrolbesøg), som Datatilsynet har foretaget i årets løb.

København, september 2003

Hugo Wendler Pedersen
Formand for Datarådet

Janni Christoffersen
Direktør



Datatilsynets virksomhed i 2002

<i>Datatilsynets opgaver</i>	8
<i>Datatilsynets organisation</i>	10
<i>Persondataloven</i>	13
<i>Datatilsynets hjemmeside</i>	13
<i>Udveksling af oplysninger mellem myndigheder</i>	13
<i>Statistiske oplysninger</i>	15
<i>Udtalelser over lovforslag m.v.</i>	18
- Ændring af arkivloven	
- Redegørelse om biobanker	
- Ændring af lov om offentlig sygesikring	
- Forslag til en protokol om ændring af Europokonventionen	

Datatilsynets virksomhed i 2002

Datatilsynets opgaver

Datatilsynets arbejde består først og fremmest i administration af lov om behandling af personoplysninger (i daglig tale blot persondataloven). Tilsynet fører tilsyn med enhver behandling, der er omfattet af loven, bortset fra domstolenes behandlinger.

Blandt Datatilsynets forskellige aktiviteter i 2002 kan nævnes:

- Vejledning og rådgivning over for offentlige myndigheder, private personer og virksomheder
- Behandling af klager fra personer over f.eks. registrering, videregivelse eller manglende indsigt
- Udtalelser om lovforslag og bekendtgørelser m.v.
- Udtalelser om anmeldelser fra offentlige myndigheder
- Tilladelser i forbindelse med anmeldelser fra private virksomheder og forskere
- Forskellige former for tilladelser til offentlige myndigheder og virksomheder m.v.
- Sager på tilsynets eget initiativ, herunder inspektioner hos offentlige myndigheder samt hos en række private virksomheder og forskere
- Informationsmøder for offentlig og privat sektor (kaldet "Gå-hjem-møder")
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsynsmyndigheder
- Deltagelse i arbejdsgrupper
- Registertilsyn for Grønland

Ud over de sager, som rejses ved klager og forespørgsler, tager Datatilsynet også sager op på eget initiativ. Datatilsynet har i 2002 registreret en stigning i antallet af sager rejst på tilsynets eget initiativ. Der er således registreret 202 sager i 2002 mod 112 i 2001. Dette tal omfatter såvel inspektioner, der omtales nærmere nedenfor, som andre "egen driftsager". Sådanne sager rejses f.eks., når medierne omtaler en sikkerhedsbrist hos en myndighed eller virksomhed, eller hvis tilsynet selv bliver opmærksom på sikkerhedsfejl eller brud på persondataloven. Antallet af sager, som er rejst på baggrund af presseomtale o.l., eller fordi tilsynet på anden vis er blevet opmærksom på et forhold, er steget ganske markant - fra 18 i 2001 til 69 i 2002.

I 2002 har Datatilsynet gennemført flere inspektioner end i noget tidligere år. Datatilsynet har således foretaget i alt 116 inspektioner, heraf 30 hos statslige myndigheder, 47 i kommuner og amter (incl. offentlige sygehuse), 14 hos forskellige private virksomheder og 25 vedrørende privat forskning. Dette er en betydelig stigning i forhold til 2001, hvor Datatilsynet foretog 76 inspektioner.

Samtidig sker der i disse år en løbende udvikling af Datatilsynets inspektioner med hensyn til såvel form som indhold. Dette er nærmere beskrevet i afsnittet om tilsynsvirksomhed.

Datatilsynet skal efter persondataloven høres over udkast til bekendtgørelser, cirkulærer o.l. generelle retsfor skrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger. Tilsynet bliver også hørt over lovforslag på dette område. Datatilsynet oplever et stigende antal sager i denne kategori. Samtidig må det konstateres, at der ofte rejser sig vanskelige spørgsmål om forholdet mellem på den ene side de ønskede nye regler og på den anden side reglerne i persondataloven og databeskyttelsesdirektivet. I nogle tilfælde må tilsynet konstatere, at den foreslåede lovgivning vil medføre en forringelse af beskyttelsesniveauet i forhold til den enkelte borger.

Selve beslutningen om, hvorvidt lovgivningsinitiativer, der medfører indskrænkninger i privatlivets fred, skal fremmes, ligger selvsagt hos Folketinget. Det kan i den forbindelse konstateres, at en række lovforslag i de senere år er blevet gennemført, selv om tilsynet har påpeget, at ændringerne vil føre til indskrænkninger i privatlivets fred. Her kan nævnes forslaget fra Indenrigs- og Sundhedsministeriet om ændring af lov om offentlig sygesikring (Etablering af personlige elektroniske medicinprofiler og indførelse af mulighed for at opkræve gebyr for godkendelse af ernæringspræparater). Dette forslag gav efter Datatilsynets opfattelse indtryk af, at der vil blive indsamlet en stor mængde af data, som man kun i visse tilfælde vil have brug for. Datatilsynet fandt det derfor tvivlsomt, om der er den fornødne proportionalitet mellem indsamling af oplysninger om samtlige køb af medicin på recept hos apotekerne og opfyldelsen af de formål, der er fastsat i loven. Sagen omtales nærmere i afsnittet "Udtalelser over lovforslag".

Datatilsynet har også i 2002 behandlet mange anmeldelser og ansøgninger om tilladelser. Der er dog sket et fald i forhold til 2001, som i denne henseende var et usædvanligt år på grund af persondatalovens overgangsordninger. Anmeldelsesordningen er nærmere omtalt på Datatilsynets hjemmeside og i afsnittet "Anmeldelser fra myndigheder og virksomheder m.v." i Datatilsynets årsberetning for 2001.

Datatilsynets deltagelse i internationalt samarbejde er et område, der får et stadigt større omfang. Datatilsynet deltager bl.a. i samarbejdet i de fælles tilsynsmyndigheder nedsat i henhold til Schengen- og Europol-konventionerne, i Europarådets arbejde og i andre internationale arbejdsgrupper både på EU-niveau og verdensplan. I 2002 er Datatilsynet blevet bedt om at bidrage med en repræsentant i den fælles tilsynsmyndighed for Eurojust. Eurojust er en enhed bestående af nationale offentlige anklagere m.v., der udsendes af de enkelte medlemsstater. Formålet er at styrke bekæmpelsen af grov organise-

ret kriminalitet. Det formelle grundlag for enheden er Rådets afgørelse af 28. februar 2002 om oprettelse af Eurojust for at styrke bekæmpelse af grov kriminalitet.

Herudover har Datatilsynet opgaver i henhold til andre love, f.eks. modtager tilsynet anmeldelser i henhold til lov om massemediers informationsdatabaser. En oversigt over de redaktionelle informationsdatabaser, der har foretaget anmeldelse til Datatilsynet, findes på tilsynets hjemmeside.

Datatilsynet er også Registertilsyn for Grønland i medfør af de der gældende registerlove fra 1979, samt i et vist omfang for rigsmyndighederne på Færøerne.

Når andre myndigheder etablerer selvbetjeningssystemer på internet o.l., yder Datatilsynet vejledning om, hvordan sikkerheden skal være for at beskytte oplysningerne. I forbindelse med en række initiativer til fremme af elektronisk borgerservice i det offentlige, har tilsynet påtaget sig opgaven som central godkendelsesinstans. Tilsynet kan desuden konstatere, at indførelsen af digital forvaltning ofte rejser spørgsmål om udveksling af oplysninger mellem myndigheder. Dette spørgsmål behandles nærmere i et særskilt afsnit nedenfor.

Datatilsynets organisation

Datatilsynet består af et råd - Datarådet - og et sekretariat. Datatilsynet udøver sine funktioner i fuld uafhængighed, men har en finanslovmæssig og personalemæssig tilknytning til Justitsministeriet, som dog ikke har nogen instruktionsbeføjelse over for tilsynet.

Datatilsynets afgørelser efter lov om behandling af personoplysninger er endelige og kan ikke indbringes for anden administrativ myndighed. Afgørelserne kan derimod indbringes for domstolene, ligesom Datatilsynet i sin virksomhed er undergivet sædvanlig kontrol af Folketingets Ombudsmand.

Datarådet

Datarådet består af en formand og 6 andre medlemmer, der er udpeget af justitsministeren. Datarådet træffer først og fremmest afgørelse i sager af principiel karakter. Rådet fastsætter efter loven selv sin forretningsorden. Dette er sket i bekendtgørelse om forretningsorden for Datarådet (Bek. nr. 1178 af 15. december 2000). Forretningsordenen kan findes på datatilsynets hjemmeside samt i Lovtidende og i Retsinformation.

Datarådets medlemmer

Pr. 31. december 2002

Formand, højesteretsdommer Hugo Wendler Pedersen
Næstformand, advokat Janne Glæsel
Professor, dr. jur. Peter Blume
Direktør Jakob Lyngsø
Rådmand Birgit Ekstrøm
Overlæge Hans Henrik Storm
Fhv. formand for Forbrugerrådet Kirsten Nielsen

Medlemmerne er personligt udpeget i kraft af deres sagkundskab inden for bestemte sagsområder og er ikke repræsentanter for bestemte interesseorganisationer eller lignende.

Korrespondance til Datarådets medlemmer stiles til sekretariatet:
Datatilsynet, Borgergade 28, 5. sal, 1300 København K

Sekretariatet

Sekretariatet varetager Datatilsynets daglige forretninger. Sekretariatet ledes af en direktør.

Med udgangen af juli måned 2001 forlod Henrik Waaben stillingen som direktør i Datatilsynet til fordel for en stilling som landsdommer i Østre Landsret. Den 1. oktober 2002 tiltrådte cand. jur. Janni Christoffersen stillingen som direktør i Datatilsynet.

I forbindelse med persondatalovens gennemførelse havde tilsynet ansat flere medarbejdere, bl.a. for at kunne behandle de mange anmeldelser, som Datatilsynet har modtaget. Som følge af de besparelser, som tilsynet er pålagt, er antallet af medarbejdere i Datatilsynet fortsat for nedadgående. Ved redaktionens slutning i september 2003 er der således 24 fuldtidsansatte i tilsynet.

Datatilsynet har endvidere været nødsaget til at afstå en del af sit lejemål som følge af nedskæringerne.

Ansatte i sekretariatet

Pr. 31. december 2002

Direktør, cand. jur. Janni Christoffersen
Kontorchef, cand. jur. Lena Andersen
IT-chef, civilingeniør Ib Alfred Larsen
Konsulent, akademiingeniør Robert Hartmann Pedersen
Akademiingeniør Flemming Boysen, HD
IT-sikkerhedskonsulent Nils Rasmussen
Specialkonsulent, mag.art. Camilla Daasnes
Fuldmægtig, cand. jur. Bettina Vesterholm Agerskov
Fuldmægtig, cand. jur. Peter Ahleson
Fuldmægtig, cand. jur. Maiken Christensen Breüner (orlov)
Fuldmægtig, cand. jur. Kira Kolby Christensen
Fuldmægtig, cand. jur. Lena Bjerregaard Danvøgg
Fuldmægtig, cand. jur. Ditte Friis-Pedersen
Fuldmægtig, cand. jur. Anette Gramstrup
Fuldmægtig, cand. jur. Helene V. Grønfeldt
Fuldmægtig, cand. jur. Lene Engedal Kragelund
Fuldmægtig, cand. jur. Jakob Lundsager
Fuldmægtig, cand. jur. Charlotte Edholm Mortensen
Fuldmægtig, cand. jur. Lene Bang Rasmussen
Fuldmægtig, cand. jur. Camilla Vinkel Voss

Kontorfuldmægtig Kirsten Markussen
Kontorfuldmægtig Anne-Marie Müller
Kontorfuldmægtig Suzanne Stenkvis
Overassistent Pernille Jensen
Overassistent Mette Maj Leilund
Overassistent Berit Pedersen
Assistent Jette van der Loo

Stud. jur. Malene Lybæk Møller
Stud. jur. Maria Nymann (orlov)
Stud. jur. Marie Gjesing Fynsk
Stud. jur. Thomas Impgaard Sørensen

Persondataloven (lov nr. 429 af 31. maj 2000) trådte i kraft den 1. juli 2000. Se Datatilsynets årsberetning 2000 om baggrunden for og forarbejderne til persondataloven.

I tilknytning til persondataloven har Justitsministeriet udstedt en række bekendtgørelser.

Herudover har Datatilsynet udsendt en række vejledninger i tilknytning til persondataloven.

Loven, bekendtgørelserne og vejledningerne kan læses på Datatilsynets hjemmeside www.datatilsynet.dk.

På hjemmesiden er det også muligt at læse eller udskrive Datatilsynets informationspjece "Persondataloven", som Datatilsynet udsendte i forbindelse med persondatalovens ikrafttræden den 1. juli 2000. Datatilsynets årsberetninger samt Registertilsynets årsberetninger fra 1996 til 1999 er ligeledes tilgængelige i elektronisk form.

Datatilsynet har også i 2002 løbende udarbejdet nye tekster og informationsmateriale, som er offentliggjort på hjemmesiden. Datatilsynet har herudover offentliggjort interessante og principielle afgørelser på hjemmesiden.

Enhver kan tegne elektronisk abonnement på Datatilsynets hjemmeside. Abonnenterne modtager automatisk en e-post, når hjemmesiden opdateres. Ved udgangen af december 2002 var der i alt ca. 2.700 abonnenter på Datatilsynets hjemmeside.

I beretningsåret har Datatilsynet modtaget en del henvendelser om videregivelse af oplysninger mellem myndigheder i forbindelse med digitale løsninger, portaler o.l.

Det vil ofte være muligt at udveksle oplysninger elektronisk, men persondataloven sætter dog visse grænser. Oplysningerne må - kort fortalt - kun videregives, i det omfang videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe. På en række områder er det præciseret i særlovgivningen, hvilke oplysninger der kan udveksles. Hertil kommer, at oplysninger kan være indsamlet og registreret med henblik på varetagelse af et specifikt formål, som er af en sådan art, at anden brug af oplysningerne ikke vil kunne forenes hermed.

Persondataloven

Datatilsynets hjemmeside

Udveksling af oplysninger mellem myndigheder

Det er de dataansvarlige myndigheder, der i første række må tage stilling til, om videregivelse må og skal finde sted. Myndighederne har ud fra reglerne i loven og inden for rammerne af den anmeldelse, der er foretaget til Datatilsynet, ansvaret for, om bestemte oplysninger må registreres og videregives. Det er også myndigheden selv, der i det daglige skal sørge for, at der er den fornødne sikkerhed omkring databehandlingen. Dette var også situationen under registerlovgivningen, se eventuelt nærmere i Registertilsynets årsberetning for 1997 s. 14. Datatilsynet vejleder gerne om lovens regler og er i øvrigt kontrol- og tilsynsmyndighed.

Når en myndighed modtager oplysninger om en borger i elektronisk form, f.eks. ved terminaladgang eller via en portal, har myndigheden som hovedregel pligt til at meddele borgeren, at der er modtaget oplysninger om ham eller hende, jf. persondatalovens kapitel 8. Når myndigheder udveksler oplysninger, er det ofte hensigtsmæssigt at undersøge, om en myndighed, der alligevel skriver til borgeren, samtidig kan give information om de behandlinger af oplysninger, der vil ske hos myndigheder, som senere modtager oplysningerne. Selv om oplysningspligten påhviler modtageren af oplysningerne, kan den afgivende myndighed eventuelt hjælpe den senere modtager af oplysningerne med opfyldelsen af oplysningspligten. Afsenderen kan f.eks. tage højde for oplysningspligten ved at skrive et ekstra afsnit i et brev, der alligevel sendes til borgeren, eller ved at inkludere specifik tekst i en blanket, som borgeren ser og udfylder. Den nærmere udformning af et sådant samarbejde afhænger selvfølgelig af de konkrete omstændigheder på det pågældende område.

Persondatalovens regler om oplysningspligt er nærmere beskrevet i rettig-hedsvejledningen. (Datatilsynets vejledning af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger).

Checkliste for myndigheder, der vil etablere digital videregivelse

- Analysér, hvilke oplysninger der er behov for at videregive - kun de nødvendige oplysninger må stilles til rådighed!
- Vær opmærksom på, om oplysningerne er indsamlet og registreret til ét bestemt formål, som taler imod videregivelsen - hvis videregivelsen er uforenelig med det oprindelige formål, må oplysningerne ikke videregives!
- Check, at videregivelsen kan rummes inden for myndighedernes anmeldelser til Datatilsynet - hvis ikke indsend ændringsanmeldelse!
- Husk datasikkerheden!
- Tag højde for oplysningspligten - tilrettelæg eventuelt et samarbejde, hvor den afgivende myndighed løfter oplysningspligten for modtagerne!

Oplysningerne i dette afsnit er baseret på registreringerne af nye sager i tilsynets journalsystem i 2002. En del af tilsynets sagsbehandling er imidlertid fortsættelser af eksisterende sager. Dette er f.eks. tilfældet, når en anmeldelse ændres, eller en tilladelse forlænges. Disse sager er af praktiske årsager ikke omfattet af statistikken.

Datatilsynet registrerede 5.186 nye sager i perioden 1. januar 2002 til 31. december 2002. Disse sager fordeler sig som følger:

Datatilsynets egen administration m.v.	164
Lovforberedende arbejde	94
Forespørgsler og klager vedrørende private	420
Forespørgsler og klager vedrørende offentlige myndigheder	365
Anmeldelser for den private sektor	1.299
Anmeldelser for den offentlige forvaltning	2.412
Sager på Datatilsynets eget initiativ	202
Sikkerhedsspørgsmål	40
Internationale sager	154
Kompetence i henhold til anden lovgivning	36

I det følgende uddybes tallene for nogle af de nævnte kategorier.

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 420 sager med forespørgsler og klager vedrørende private dataansvarlige.

Fordelingen mellem klager og forespørgsler i de afsluttede sager var følgende:

Klager	ca. 25%
Forespørgsler	ca. 75%

Endvidere kan det oplyses, at i de afsluttede sager var ca. 39 % af klagerne berettigede, mens resten var uberettigede.

Sagerne var fordelt på følgende virksomhedstyper:

Almindelige virksomheder	62
Den finansielle sektor	42
Fagforeninger, a-kasser, pensionskasser m.v.	20
Telesektoren	22
Foreninger og organisationer	33
Sundhedssektoren (medicinalvirksomheder, klinikker, læger m.v.)	12
Kreditoplysningsbureauer	50

Advarselsregistre	21
Stillingsbesættende virksomheder	0
Ansøgninger om tilladelser	81
Diverse	76
Sager af generel karakter	1

Forespørgsler og klager vedrørende offentlige myndigheder

Datatilsynet registrerede i alt 365 sager med forespørgsler og klager vedrørende offentlige myndigheder.

Fordelingen mellem klager og forespørgsler i de afsluttede sager var følgende:

Klager	ca. 38%
Forespørgsler	ca. 62%

I de afsluttede sager var ca. 11 % af klagerne berettigede, mens resten var uberettigede.

Sagerne var fordelt således:

Statslige myndigheder	135
Amtskommuner	26
Kommuner	82
Ansøgning om tilladelser	113
Diverse	9
Sager af generel karakter	0

Anmeldelser for den private sektor

Datatilsynet registrerede i alt 1.299 sager om anmeldelser. Fordelingen af sagerne var følgende:

Forskning og statistik	938
Privates behandling af oplysninger om rent private forhold	137
Advarselsregistre	165
Spærrelister	1
Kreditoplysningsbureauer	4
Stillingsbesættende virksomheder	20
Edb-servicebureauer	32
Diverse sager af generel karakter	2

Anmeldelser for den offentlige forvaltning

Datatilsynet registrerede i alt 2.412 sager om anmeldelser. Fordelingen af sagerne var følgende:

Fællesanmeldelser	11
Kommuner	667
Amtskommuner	169
Statslige myndigheder	290
Tilslutninger til fællesanmeldelser fra kommuner	1.223
Tilslutninger til fællesanmeldelser fra amtskommuner	11
Tilslutninger til fællesanmeldelser fra statslige myndigheder	40
Diverse/sager af generel karakter	1

Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 202 sager oprettet på tilsynets eget initiativ. Sagerne var fordelt på følgende sagstyper:

Inspektion og kontrol vedrørende private	53
Inspektion og kontrol vedrørende offentlige myndigheder	76
Sager rejst på grundlag af presseomtale o.l.	69
Diverse/sager af generel karakter	4

Sikkerhedsspørgsmål

Datatilsynet registrerede i alt 40 sager under kategorien sikkerhedsspørgsmål. Fordelingen af sagerne var følgende:

Sager vedrørende private	14
Sager vedrørende offentlige myndigheder	26

Internationale sager

Datatilsynet registrerede i alt 154 internationale sager. Fordelingen af sagerne var følgende:

Forespørgsler fra udlandet om dansk lovgivning	58
Nordisk tilsynssamarbejde	1
Europarådet	7
EU	38
Konventioner	34
Datakommissærsamarbejdet	7
OECD	0
Diverse/sager af generel karakter	9

Udtalelser over lovforslag m.v.

Ændring af arkivloven

Kulturministeriet anmodede Datatilsynet om en udtalelse om udkast til ny arkivlov. Datatilsynet havde tidligere afgivet en udtalelse vedrørende betænkning nr. 1404/2001 om revision af arkivloven.

Tilsynets udtalelse, som blev afgivet efter behandling i Datarådet, gengives nedenfor.

Som anført i Datatilsynets udtalelse over betænkning nr. 1404/2001 om revision af arkivloven var det tilsynets opfattelse, at personoplysninger, som er tilvejebragt gennem arkivadgang, hvad enten det er før eller efter udløbet af tilgængelighedsfristen, skal behandles i overensstemmelse med reglerne i persondataloven.

Persondataloven bygger ifølge forarbejderne til loven på den forudsætning, at spørgsmål om arkivmæssig anvendelse (behandling) af personoplysninger afgøres efter arkivlovgivningen og ikke efter behandlingsreglerne i persondatalovens kapitel 4 (lovforslag nr. L 147 af 9. december 1999, særtrykket side 81, 2. spalte). I øvrigt finder de generelle regler i persondataloven, f.eks. om datasikkerhed, anvendelse på arkivmæssig behandling af personoplysninger, medmindre det databeskyttelsesretlige spørgsmål er reguleret i arkivlovgivningen. Som følge heraf gælder persondataloven - inden for sit anvendelsesområde - også efter tilgængelighedsfristens udløb, uanset at en arkivenhed eller gruppe af arkivenheder på det tidspunkt er offentligt tilgængelig.

De nye tilgængelighedsfrister i udkast til forslag til arkivlov gav ikke Datatilsynet anledning til bemærkninger.

Datatilsynet lagde i den forbindelse vægt på, at de foreslåede nedsættelser af tilgængelighedsfristerne reelt alene var på 5 år for så vidt angår oplysninger om enkeltpersoners private, herunder økonomiske, forhold. Endvidere var der efter lovforslagets § 23, stk. 2, og § 27, stk. 2 og 3, mulighed for at fastsætte en længere tilgængelighedsfrist for arkivenheder.

Lovforslaget gav i øvrigt ikke Datatilsynet anledning til bemærkninger.

Redegørelse om biobanker

Indenrigs- og Sundhedsministeriet anmodede Datatilsynet om bemærkninger til betænkning nr. 1414/2002 "Redegørelse om biobanker" og betænkningens lovforslag.

Tilsynets udtalelse, som blev afgivet efter behandling i Datarådet, gengives nedenfor.

Arbejdsgruppens kommissorium var: "Arbejdsgruppen skal, med udgangspunkt i Justitsministeriets lovforslag om behandling af personoplysninger/Europaparlamentet og Rådets direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, og under inddragelse af anden relevant lovgivning på sundheds- og forskningsområdet, undersøge behovet for særskilt regulering af sundhedsvidenskabelige informationsbanker (biobanker), særligt for så vidt angår oprettelse, opbevaring og efterfølgende anvendelse af indsamlet biologisk materiale, hvad enten dette materiale er indsamlet i behandlings- eller forskningsøjemed.

Arbejdsgruppen skal endvidere særligt vurdere behovet for mulige overgangsordninger for eksisterende biologiske samlinger.

Arbejdsgruppen skal i sine overvejelser lægge til grund, at der sker en rimelig afbalancering af hensynet til den vævsafgivende persons integritet, dvs. adgang til at give samtykke, over for samfundets behov for forskning, dvs. muligheden for at benytte de informationer, der er bundet til personhenførbart væv, uden specifik indhentelse af (fornyte) samtykke fra patienten.

Hvis arbejdsgruppen finder, at der er behov for supplerende at regulere biobanker, skal arbejdsgruppen udarbejde forslag til en sådan regulering."

En biobank er i redegørelsen defineret som en struktureret samling af menneskeligt biologisk materiale, der er tilgængeligt efter bestemte kriterier, og hvor oplysningerne, der er bundet i det biologiske materiale, kan henføres til enkeltpersoner.

Arbejdsgruppen havde tidligere spurgt Datatilsynet om en biobank - defineret som ovenfor - er et manuelt register omfattet af persondataloven. Datatilsynet afgav i den forbindelse en udtalelse, hvor det blev fremhævet, at det gav anledning til tvivl, om en biobank kan anses for et manuelt register efter persondatalovens § 1, stk. 1, med den følge, at behandling af oplysninger i biobanker på det offentlige område også er omfattet af loven. Tilsynet fremhævede endvidere, at det imidlertid fremgår af persondatalovens forarbejder, at der gives tilsynsmyndigheden mulighed for at udvise et rimeligt og konkret skøn i forbindelse med fastlæggelsen af det manuelle registerbegreb. Det anføres bl.a., at den nærmere afgrænsning af registerbegrebet må finde sted gennem tilsynsmyndighedens praksis.

Datatilsynet udtalte herefter, at tilsynet fandt det rimeligt, at en biobank - defineret som angivet af arbejdsgruppen - anses for omfattet af persondatalo-

vens registerbegreb. Det blev i den forbindelse tillagt betydning, at der herved opnås en styrkelse af beskyttelsen af og retssikkerheden for de registrerede personer i biobankerne. Samtidig sikres en ensartet regulering af biobanker i den private og den offentlige sektor.

Arbejdsgruppens konklusion var, at persondataloven i samspil med den relevante sundheds- og forskningslovgivning på tilstrækkelig vis regulerer de fleste sider af biobankerne.

Arbejdsgruppen havde således vurderet, at de respektive eksisterende loves regler med hensyn til oprettelse, nedlæggelse, kontrol og tilsyn med biobanker samt regler om vævsafgivende personers rettigheder, fandtes tilstrækkelige til sikring af hensynet til patientens selvbestemmelser og integritet, afbalanceret overfor hensynet til forskning og samfund.

Arbejdsgruppen havde dog fundet, at der på to områder er behov for ny lovgivning:

1. Selvbestemmelse over biologisk materiale, der afgives i forbindelse med undersøgelse og behandling, må særligt reguleres ved, at nye regler indføres i lov om patienters retsstilling. Herved gives der patienten mulighed for at "sige fra" over for et centralt register: "Vævsanvendelsesregisteret" med hensyn til ikke-behandlingsrelateret anvendelse af afgivet biologisk materiale samtidig med, at der gives patienten ret til destruktion og betinget ret til udlevering af afgivet biologisk materiale.
2. Det skal sikres, at alle forskningsprojekter, herunder også registerforskningsprojekter, hvori biologisk materiale indgår, anmeldes til og godkendes af en videnskabsetisk komité. Dette kræver en ændring af lov om et videnskabsetisk komitéssystem og behandling af biomedicinske forskningsprojekter.

Der lægges således op til, at en patient kan beslutte, at biologisk materiale, som patienten afgiver eller har afgivet i forbindelse med undersøgelse og behandling, kun må anvendes til undersøgelse og behandling af den pågældende selv og til formål, der har en umiddelbar tilknytning hertil. En sådan beslutning skal registreres i Vævsanvendelsesregisteret. Herved er patienten sikret mod, at det afgivne biologiske materiale anvendes til f.eks. forskning eller kommercielle formål, idet den sundhedsperson, der er ansvarlig for opbevaringen af det biologiske materiale, skal søge oplysninger i registeret, hvis der påtænkes en ikke-behandlingsrelateret anvendelse af det biologiske materiale.

Denne ret til at "sige fra" over for Vævsanvendelsesregisteret suppleres med ret til destruktion og betinget ret til udlevering af afgivet biologisk materiale.

Ønsker en patient, at det afgivne biologiske materiale skal destrueres, skal dette - praktisk talt altid - imødekommes. Ønsker en patient, at det afgivne biologiske materiale skal udleveres til vedkommende, skal patienten kunne godtgøre en særlig interesse herfor, for at materialet kan udleveres.

I lovforslaget foreslås indsat et nyt kapitel 3 i lov om patienters retsstilling, hvorefter patienten tildeles følgende rettigheder:

1. Mulighed for at sige fra med hensyn til ikke-behandlingsrelateret anvendelse af afgivet biologisk materiale over for et centralt register "Vævsanvendelsesregisteret".
2. Ret til destruktion af afgivet biologisk materiale.
3. Ret til udlevering af afgivet biologisk materiale, hvis patienten har en særlig interesse heri.

Disse tre hovedelementer i lovforslaget tager ifølge de almindelige bemærkninger udgangspunkt i patientens selvbestemmelsesret over det afgivne biologiske materiale, ligesom der samtidig er tilstræbt en løsning, der for de involverede personer er let at overskue og enkel at administrere. Modellen er således et udtryk for arbejdsgruppens afvejning af de to modstående hensyn - hensynet til patientens individbeskyttelse og hensynet til samfundets interesse i drift af sundhedsvæsenet og udførelse af sundhedsvidenskabelig forskning.

Datatilsynet noterede sig, at arbejdsgruppens lovforslag vil medføre en præcisering af den registreredes ret til at gøre indsigelse over for en behandling af oplysninger vedrørende den pågældende. Reglerne giver dermed en mere tydelig ret for den registrerede til at sige fra over for en behandling.

Datatilsynet fandt det hensigtsmæssigt, at der fastsættes særlige regler for behandling af oplysninger indeholdt i biologisk materiale, når henses til materialets specielle natur, herunder materialets originalitet, og den overskudsinformation og det fremtidige informationspotentiale, der er i det biologiske materiale.

I rapportens beskrivelse af persondatalovens regulering er det anført, at rækkevidden af lovens § 7, stk. 5, om almindelig patientbehandling m.v. ikke i alle detaljer er klarlagt i Datatilsynets praksis. Det er således ikke afklaret, hvor længe oplysningerne kan bevares, og om det kan anses for nødvendigt med henblik på de formål, som er nævnt i paragraffen, at anvende personhenførbare patientoplysninger i forbindelse med undervisning o.l.

I arbejdsgruppens lovforslag, de almindelige bemærkninger punkt 7, s. 224f, henvises til persondatalovens § 7, stk. 5, hvorefter behandling af oplysninger om helbredsmæssige forhold kan ske, hvis behandlingen af oplysninger er

nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysninger foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

I bemærkningerne er bl.a. anført følgende:

"Kvalitetssikring, metodeudvikling og undervisning af sundhedspersoner er efter Indenrigs- og Sundhedsministeriets opfattelse opgaver, der naturligt løses af sundhedsvæsenet i tilknytning til patientbehandling, og er derfor aktiviteter, der falder inden for rammerne af patientretsstillingslovens § 3 om patientbehandling. Denne bestemmelse tager sigte på at dække al behandlingsvirksomhed i bred forstand, der foregår inden for sundhedsvæsenet, og dermed også de almindelige og rutinemæssige aktiviteter, der foregår som et integreret led heri eller i tæt tilknytning hertil: kvalitetssikring, metodeudvikling og undervisning af sundhedspersoner. Som følge heraf må behandling af personoplysninger i form af anvendelse af biologisk materiale i forbindelse med kvalitetssikring, metodeudvikling og undervisning af sundhedspersoner antages at være omfattet af persondatalovens § 7, stk. 5.

Dette betyder, når persondatalovens § 7, stk. 5, anvendes på biologisk materiale, at kvalitetssikring, metodeudvikling og undervisning af sundhedspersoner kan finde sted, uden at patienten særligt skal inddrages heri." (Redegørelsens s. 225)

Dette rejste efter Datatilsynets opfattelse spørgsmålet om, hvorvidt "kvalitetssikring, metodeudvikling og undervisning af sundhedspersonale" er omfattet af persondatalovens § 7, stk. 5, eller eventuelt skal finde sted med hjemmel i persondatalovens § 10 vedrørende videnskabelige eller statistiske undersøgelser eller med samtykke efter persondatalovens § 7, stk. 2, nr. 1.

Oplysninger om helbredsmæssige forhold må som udgangspunkt ikke behandles, jf. persondatalovens § 7 stk. 1.

Bestemmelsen i stk. 1 finder i følge § 7, stk. 2, nr. 1, ikke anvendelse, hvis den registrerede har givet sit udtrykkelige samtykke til en sådan behandling. Efter lovens § 7, stk. 5, finder bestemmelsen i stk. 1 endvidere ikke anvendelse, hvis behandlingen af oplysninger er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Oplysninger om helbredsmæssige forhold må desuden behandles i medfør af lovens § 10, stk. 1, hvis dette alene sker med henblik på at udføre statistiske

eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelserne. Oplysninger, der behandles i medfør af lovens § 10, må som følge af bestemmelsens stk. 2 ikke senere behandles i andet end statistisk eller videnskabeligt øjemed og må som følge af stk. 3 kun videregives til tredjemand efter forudgående tilladelse fra tilsynsmyndigheden.

I betænkning 1345/97 om behandling af personoplysninger beskrives på s. 247f, hvilke typer af aktiviteter der er omfattet af bestemmelsen i direktivets art. 8, stk. 3, (som lovens § 7, stk. 5, er fastsat i lyset af). Omfattet af bestemmelsen i direktivets artikel 8, stk. 3, må antages at være behandling af oplysninger, som er nødvendig af hensyn til varetagelsen af aktiviteter inden for sundhedssektoren. Der er navnlig tale om aktiviteter, som foretages på sygehuse, klinikker og hos læger, men bestemmelsen omfatter også særlige institutioner i privat eller offentlig regi, hjemmesygepleje samt tildeling af hjælpemidler og lignende tiltag, som udgør en opfølgning på behandling. Herudover omfattes behandling af oplysninger med henblik på varetagelsen af de administrative opgaver, som er nødvendige i forbindelse med forvaltningen af sådanne institutioner.

Det anføres endvidere, at udtrykket "forebyggende medicin" må forstås som omfattende forebyggende behandling, f.eks. vaccinerings og rutineundersøgelser og lignende undersøgelser, som ikke er begrundet i en konkret mistanke om, at den undersøgte lider af en bestemt sygdom.

Det anføres endvidere, at "Sygepleje eller patientbehandling" - ud over almindelig behandling hos privat praktiserende læger og på hospitaler - må antages at omfatte fysioterapi, kiropraktik og lignende professionel assistance i forbindelse med afhjælpning af symptomer på og årsager til sygdomstilstande. Bestemmelsen må i hvert fald antages at omfatte aktiviteter, som foretages af de grupper af personer, der i dag er underkastet et krav om offentlig autorisation, herunder f.eks. fodterapeuter, fysioterapeuter, ergoterapeuter, jordemødre, optikere, kliniske diætister, tandplejere og læger.

Vurderingen af, om en given behandling vil kunne ske inden for rammerne af persondataloven, herunder dennes § 7, stk. 5, skal i første række foretages af den dataansvarlige. Datatilsynet har taget til efterretning, at behandling af personoplysninger med henblik på "*kvalitetssikring og metodeudvikling*" efter arbejdsgruppens opfattelse kan ske med hjemmel i persondatalovens § 7, stk. 5.

Undervisning af sundhedspersoner vil efter Datatilsynets opfattelse efter omstændighederne kunne ske med hjemmel i persondatalovens § 7, stk. 5, sålænge der er tale om undervisning af personer, som er underlagt tavshedspligt, f.eks. personale på et sygehus eller lignende.

Efter Datatilsynets opfattelse er nødvendighedsbetingelsen i persondatalovens § 7, stk. 5, ikke opfyldt for så vidt angår undervisning på universiteter og tilsvarende undervisningssteder, hvis behandlingen af oplysninger sker i en for eleverne personhenførbart form. Anvendelse af biologisk materiale til undervisning på universiteter og tilsvarende undervisningssteder kan derfor kun ske uden samtykke, hvis materialet anvendes i en for eleverne ikke-personhenførbart form.

Ændring af lov om offentlig sygesikring

Indenrigs- og Sundhedsministeriet anmodede Datatilsynet om eventuelle bemærkninger til forslag til lov om ændring af lov om offentlig sygesikring (Etablering af personlige elektroniske medicinprofiler og indførelse af mulighed for at opkræve gebyr for godkendelse af ernæringspræparater).

Tilsynets udtalelse, som blev afgivet efter behandling i Datarådet, gengives nedenfor.

Af den foreslåede regel i § 7 i, stk. 1, fremgik, at Lægemiddelstyrelsen fører et elektronisk register over de enkelte medicinbrugeres køb m.v. af lægemidler og hertil knyttede oplysninger (personlige elektroniske medicinprofiler).

Persondatalovens § 5, som bygger på artikel 6 i databeskyttelsesdirektivet, indeholder en række grundlæggende principper for den dataansvarliges behandling af oplysninger.

Persondatalovens § 5, stk. 2, indeholder bl.a. et krav om, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål. Lovens § 5, stk. 3, indeholder et krav om, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Det angivne formål med registeret - sikring af kvaliteten af behandlingen af patienter - var efter Datatilsynets opfattelse i sig selv sagligt og anerkendelsesværdigt.

Datatilsynet kunne imidlertid konstatere, at der med lovforslaget ville blive oprettet et register over samtlige medicinbrugere i Danmark - i første omgang kun over dem, der køber medicin på recept på apotekerne. Der ville dog stadig være tale om en meget stor mængde af data.

Selv om oplysningerne i den elektroniske medicinprofil givetvis ville være nyttige i visse tilfælde, måtte det efter Datatilsynets opfattelse antages, at re-

gisteret tillige ville komme til at indeholde store mængder data, som man aldrig ville få brug for.

Hertil kom, at det umiddelbart kunne forekomme tvivlsomt, om alle de formål, som nævntes i lovbemærkningerne, ville kunne opfyldes alene ved hjælp af registeret. F.eks. ville en manglende efterlevelse af den foreskrevne behandling ikke umiddelbart kunne afværges ved hjælp af registeret. For meget indtagelse af et bestemt produkt ville heller ikke kunne forebygges ved hjælp af registeret.

Sammenfattende gav forslaget således indtryk af, at der ville blive indsamlet en stor mængde af data, som man kun i visse tilfælde ville have brug for.

Datatilsynet fandt det på den baggrund tvivlsomt, om der var den fornødne proportionalitet mellem indsamling af oplysninger om samtlige køb af medicin på recept hos apotekerne og opfyldelsen af de formål, der var fastsat i forslaget.

Ud fra hensynet til privatlivets fred var det derfor Datatilsynets opfattelse, at et register med elektroniske medicinprofiler kun burde oprettes, hvis vægtige samfundsmæssige interesser talte herfor. Datatilsynet fandt ikke at burde udtale sig om, hvorvidt dette var tilfældet.

Det fulgte af lovforslagets § 7 i, stk. 2, at den registrerede har adgang til oplysninger, der er registreret om vedkommende i den elektroniske medicinprofil, og har krav på at få urigtige oplysninger berigtiget.

Det fremgik af bemærkningerne, at den registrerede efter lov om behandling af personoplysninger har en række rettigheder, herunder retten til indsigt. Det fremgik, at indsigtsretten ikke kun vedrører de oplysninger, der direkte er registreret om vedkommende, men bl.a. også indebærer krav på indsigt i data-behandlingens formål.

Det anførtes endvidere, at det foreliggende lovforslag ikke indebar nogen begrænsninger i de rettigheder, som den registrerede har i denne henseende i medfør af lov om behandling af personoplysninger. Lovforslagets bestemmelse om, at den enkelte medicinbruger ville få adgang til at læse oplysningerne i sin personlige elektroniske medicinprofil, ville tværtimod give den registrerede en udvidet indsigt i de registrerede oplysninger i forhold til persondatalovens regler, idet systemet med den elektroniske medicinprofil indebærer, at medicinbrugeren ville få direkte elektronisk indsigt i registeret.

Ifølge persondatalovens § 31, stk. 1, skal den dataansvarlige efter begæring fra en person give meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig

måde gives meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

I det omhandlede lovforslag blev der lagt op til, at borgerne/den enkelte medicinbruger skulle kunne få indsigt via den offentlige sundhedsportal. Modellen forudsætter, at medicinbrugerne har adgang til en entydig personlig "elektronisk nøgle" i form af en digital signatur.

Datatilsynet gjorde opmærksom på, at det fremgår af side 15 i Datatilsynets rettighedsvejledning, at der efter bestemmelsen i § 31, stk. 1, ikke kan stilles særlige krav til en begæring om indsigt.

Det ville derfor ikke være tilstrækkeligt til opfyldelse af persondatalovens indsigtsregler, hvis de registrerede kun kunne fremsætte begæring om indsigt elektronisk.

For så vidt angår sidste led af § 7 i, stk. 2, om berigtigelse af urigtige oplysninger henledte Datatilsynet opmærksomheden på, at persondataloven i såvel § 5 som i § 37 indeholder regler om bl.a. berigtigelse af urigtige oplysninger, og at reguleringen er mere detaljeret end i det omhandlede lovforslag.

Datatilsynet gjorde opmærksom på, at tilsynet gik ud fra, at det *ikke* var hensigten at fravige persondataloven på de punkter, der omfattedes af den foreslåede bestemmelse i § 7 i, stk. 2. Tilsynet foreslog derfor, at bestemmelsen blev udeladt, og at der i stedet, f.eks. i bemærkningerne til lovforslaget, henvistes til persondatalovens regler.

Det fremgik af lovforslagets § 7 i, stk. 4, at apotekere og apotekspersonale har adgang til de oplysninger, der er registreret om en medicinbruger, når denne har givet sit udtrykkelige samtykke.

Datatilsynet gjorde opmærksom på, at i persondataloven forstås der ifølge lovens § 3, nr. 8, ved "Den registreredes samtykke: Enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling." Denne definition svarer til en tilsvarende definition i databeskyttelsesdirektivet.

Tilsynet bemærkede, at tilsynet gik ud fra, at der med samtykke i lovforslaget menes det samme som i persondataloven og databeskyttelsesdirektivet, og foreslog, at dette blev overvejet præciseret i bemærkningerne.

Det fremgik af bemærkningerne til lovforslaget (s. 11), at det ville være Lægemiddelstyrelsen, der er ansvarlig for indsamling af data og kvaliteten af data i medicinprofilen samt apotekernes adgang til registeret, mens den driftsansvarlige for den offentlige sundhedsportal er ansvarlig for, at det er de rigtige personer, der har adgang til oplysningerne i den elektroniske medicinprofil, dog undtaget apotekerne.

Efter Datatilsynets opfattelse omfatter sikkerhedsforanstaltninger omkring databehandlinger som de omhandlede bl.a. en række forpligtelser for den eller de dataansvarlige omkring autorisationer og adgangskontrol. Kravene der udspringer af persondatalovens § 41, stk. 3, er nærmere fastsat i sikkerhedsbekendtgørelsens §§ 11, 12 og 16.

Da en dataansvarlig ikke ved at benytte en databehandler kan frigøre sig for sin forpligtelse til at træffe de fornødne sikkerhedsforanstaltninger, foreslog Datatilsynet, at den omhandlede formulering udgik eller blev ændret. Om forholdet mellem den dataansvarlige og databehandleren kunne i øvrigt henvises til persondatalovens § 42.

I tilknytning hertil bemærkede Datatilsynet, at de enkelte privatpraktiserende læger, sygehuse og apotekere, som får adgang til systemet, efter Datatilsynets opfattelse som udgangspunkt må anses for dataansvarlige for de behandlinger af oplysninger, som de foretager i forbindelse med deres opslag i registeret, samt for den videre behandling af oplysningerne, som sker hos de nævnte.

Datatilsynet gjorde opmærksom på, at det følger af persondatalovens § 43, stk. 1, at forinden iværksættelse af en behandling af oplysninger, som foretages for den offentlige forvaltning, skal den dataansvarlige eller dennes repræsentant foretage anmeldelse til Datatilsynet, medmindre behandlingen ikke omfatter oplysninger af fortrolig karakter. En sådan behandling kan uden anmeldelse endvidere omfatte identifikationsoplysninger, herunder personnummer, og oplysninger om betaling til og fra en offentlig myndighed.

Hvis behandlingen omfatter oplysninger, der er omfattet af § 7, stk. 1, og § 8, stk. 1, skal der, forinden behandling, som er omfattet af anmeldelsespligten i § 43, iværksættes, indhentes en udtalelse fra Datatilsynet, jf. persondatalovens § 45, stk. 1, nr. 1.

I det omfang de behandlinger, der var beskrevet i lovforslaget, foretages for den offentlige forvaltning, vil behandlingerne således skulle anmeldes til Datatilsynet, og der vil skulle indhentes forudgående udtalelse fra tilsynet, inden behandlingerne iværksættes.

For så vidt angår de selvstændige behandlinger af oplysninger, der hidrører fra systemet, og som brugerne i den private sektor foretager, følger det af persondatalovens § 49, stk. 1, nr. 8, at bl.a. behandlinger af oplysninger, der foretages af læger og apotekere, er undtaget fra anmeldelsespligt i det omfang, oplysningerne alene anvendes til brug ved denne virksomhed, og behandlingen af oplysningerne ikke sker for et privat sygehus.

Datatilsynet henledte opmærksomheden på persondatalovens § 57. Efter denne bestemmelse skal der indhentes en udtalelse fra Datatilsynet i forbindelse med udfærdigelse af bekendtgørelser, cirkulærer eller lignende generelle retsfor skrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger.

Forslag til en protokol om ændring af Europol-konventionen

Justitsministeriet anmodede Datatilsynet om en udtalelse om et dansk forslag til en protokol om ændring af Europol-konventionen med tilhørende grundnotat. Justitsministeriet har senere fremsendt et arbejdsdokument af 21. oktober 2002 (EUROPOL 76) indeholdende visse ændringsforslag til det oprindelige forslag.

Tilsynets udtalelse til ovennævnte materiale gengives nedenfor.

1. Ifølge forslag til ny artikel 2 om Europols kompetence skulle betingelserne om, at der skal være konkrete indicier for, at der foreligger en kriminel struktur eller organisation, bortfalde. Det blev endvidere foreslået at lade den specifikke opregning af kriminalitetstyper, der ses i den nugældende konvention med tilhørende bilag, udgå, således at alle grove internationale kriminalitetsformer ville være omfattet af mandatet.

Datatilsynet bemærkede hertil, at det følger af den gældende konventions artikel 14, stk. 3, at Europol ved indsamlingen, behandlingen og anvendelsen af personoplysninger skal overholde principperne i Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger samt Europarådets Ministerråds politirekommandation.¹

Af politirekommandationens princip 2.1 fremgår, at politiets indsamling af personoplysninger kun kan ske, hvis det er nødvendigt for at forebygge en reel fare eller for at bekæmpe en specifik forbrydelse.

Det følger heraf, at politiet ikke kan foretage en generel og ubegrænset dataindsamling. Indsamling af personlige oplysninger til politimæssige formål er begrænset til de tilfælde, hvor den er nødvendig med henblik på forebyggelse.

¹ Europarådets Ministerudvalgs rekommandation No. R (87) 15 af 17. september 1987.

se af en konkret fare eller bekæmpelse af en specifik strafbar handling.

Datatilsynet lagde til grund, at politiets dataindsamling også fremover ville skulle ske i overensstemmelse med dette princip og pegede derfor på muligheden for fortsat at lade dette fremgå direkte af bestemmelsen.

Tilsynet hæftede sig endvidere ved, at der med den foreslåede artikel 2 blev lagt op til en meget bred og forenklet afgrænsning af Europols mandat. Datatilsynet udtrykte forståelse for behovet for fleksibilitet og råderum for at sikre et effektivt samarbejde, men fandt at behovet herfor nøje må afvejes i forhold til både nationale og internationale databeskyttelsesmyndigheders samt enkelt individers mulighed for at efterprøve, hvorvidt en given handling falder ind under Europols kompetence.

Datatilsynet henstillede derfor til ministeriets overvejelse, om der under en eller anden form kunne indføres mere objektive kriterier for afgrænsningen af Europols kompetence.

Det fulgte af forslaget til artikel 2, stk. 4, at det var de nationale myndigheder, der skulle vurdere, hvorvidt en form for kriminalitet skal betragtes som grov international kriminalitet. Datatilsynet lagde til grund, at Europol selv sagt også er ansvarlig for, at en given databehandling, som organisationen var ansvarlig for, falder ind under Europols kompetenceområde.

2. Ifølge forslag til ændring af artikel 3 skulle der for at lette gennemførelsen af den politimæssige efterforskning uden om Europolkonventionen, kunne meddeles de nationale enheder alle relevante oplysninger eller gives analytisk støtte til sådan efterforskning i overensstemmelse med national ret i den medlemsstat, der anmodede herom og under denne medlemsstats eneansvar.

Datatilsynet bemærkede til spørgsmålet om Europols støtte til medlemsstaterne uden om Europol-konventionen - kendt under begrebet Member States Operational Project with Europol Support (MSOPES) - at den fælles kontrolinstans for Europol (JSB) i en udtalelse af 8. november 2001 udtalte, at man finder, at anvendelse af analysedatabaser i MSOPES-sammenhæng ikke kan ske inden for rammerne af Europol-konventionen.

Datatilsynet opfattede det foreliggende forslag således, at man herved vil skabe hjemmel til, at Europol kan bistå medlemsstaternes politimyndigheder med analytisk støtte, uden at regelsættet i konventionens artikel 10 iagttages.

Datatilsynet pegede på, at indførelsen af et "flerstrengt system", hvor Europol kan være involveret i analysearbejdet både på grundlag af artikel 3 og

artikel 10, må formodes at føre til en mere uigennemsigtig retsstilstand, herunder i relation til databeskyttelse.

3. Af forslaget til artikel 4 fulgte, at de nationale kompetente myndigheder ville få mulighed for bl.a. at videregive oplysninger og efterretninger direkte til Europol, uden at dette nødvendigvis skulle foregå gennem den nationale enhed.

Omvendt ville de nationale enheders eksklusive kompetence blive bibeholdt, bl.a. for så vidt angår videregivelse af oplysninger til Europol med henblik på lagring i edb-baserede datasamlinger (nuværende artikel 4, stk. 4, nr. 6) - dvs. Europols Informationssystem (artikel 7-9) samt analyse databaser med tilhørende indexsystem (artikel 10-12).

Datatilsynet gik således ikke ud fra, at Europol ville kunne lagre (behandle) oplysninger i de edb-baserede datasamlinger, hvis oplysningerne er modtaget direkte fra de nationale kompetente myndigheder uden om den nationale enhed.

Tilsynet noterede sig i øvrigt, at arbejdsdokumentet EUROPOL 76 indeholder yderligere ændringsforslag vedrørende denne bestemmelse, som ikke var færdigbehandlede i arbejdsgruppen.

4. Det var foreslået at tilføje et nyt stykke til bestemmelsen i artikel 6, hvorefter der gives Europol hjemmel til at behandle oplysninger som såkaldt "baggrundsmateriale".

På det foreliggende grundlag stod det ikke Datatilsynet klart, hvad der menes med udtrykket "baggrundsmateriale". Datatilsynet fandt derfor ikke på daværende tidspunkt at kunne foretage en endelig vurdering af denne del af forslaget. Tilsynet noterede sig, at arbejdsdokument EUROPOL 76 indeholdt yderligere ændringsforslag vedrørende denne bestemmelse, som ikke var færdigbehandlede i arbejdsgruppen.

5. Det fulgte af forslaget til artikel 9, at kompetente (nationale) myndigheder skulle have adgang til at foretage direkte søgninger i Europols Informationssystem.

Udvidelse af den personkreds, der kan søge i systemet, aktualiserede efter Datatilsynets opfattelse behovet for et højt sikkerhedsniveau, jf. nedenfor vedrørende forslaget til artikel 16.

6. Det fulgte af forslaget til artikel 10, nr. 9, at analysegruppen i visse situationer skulle kunne invitere repræsentanter for tredjelande eller eksterne organisationer til at deltage som observatører, samt at der kunne ske videregivel-

se af oplysninger i databaserne til repræsentanterne i overensstemmelse med gældende samarbejdsaftale.

Datatilsynet bemærkede hertil, at det ikke stod tilsynet klart, hvorvidt det påtænkes at give repræsentanterne fra 3. lande eller eksterne organisationer adgang til at foretage direkte søgninger i analysedatabaserne. Hvis dette var tilfældet, pegede Datatilsynet på, at der kunne være behov for at revidere de eksisterende samarbejdsaftaler.

7. Forslaget vedrørende artikel 12 vedrørte procedurereglerne for åbning af analysedatabaser. Ifølge forslaget ændredes JSB's rolle fra proaktiv (udtalelse inden åbning) til reaktiv (mulighed for efterfølgende udtalelse inden for en konkret angiven frist).

Uanset at det fra Datatilsynets deltagelse i arbejdet i JSB er tilsynets erfaring, at JSB sjældent har bemærkning til udkast til oprettelsesbestemmelser for analysedatabaser, kunne en ændring af JSB's rolle fra proaktiv til reaktiv, principielt indebære en potentiel forringelse af databeskyttelsesniveauet.

Datatilsynet havde imidlertid forståelse for, at der var et praktisk behov for at ændre de eksisterende regler vedrørende analysedatabaser. Datatilsynet kunne derfor på linie med JSB foreslå, at der eventuelt blev udarbejdet særlige standardoprettelsesbestemmelser inden for bestemte områder (f.eks. menneskesmugling), der på forhånd godkendes af JSB.

Anvendelse af sådanne standarder ville efter omstændighederne kunne udgøre et fornuftigt kompromis mellem Europols behov for at reagere relativt hurtigt og JSB's rolle som proaktiv tilsynsmyndighed.

For så vidt angik forslaget artikel 12, stk. 2, var det Datatilsynets umiddelbare opfattelse, at det måtte være en naturlig følge af en eventuel beslutning om lukning, at denne fik virkning ex tunc.

8. Ifølge forslaget til artikel 16 ændredes de nugældende konkrete regler om logning (hver tiende søgning for så vidt angår analysedatabaser og alle søgninger for så vidt angår Europols Informationssystem) til en generel regel, der forpligtede Europol til at indføre mekanismer "...der gør det muligt at føre effektiv kontrol med lovligheden af søgningerne i de edb-baserede datasamlinger, der er omhandlet i artikel 6".

Baggrunden for denne ændring var ikke beskrevet i det materiale, som Datatilsynet havde modtaget.

Datatilsynet bemærkede, at Datatilsynet (tidligere Registertilsynet) i flere sammenhænge har påpeget, at der af hensyn til muligheden for at sikre tilsynet

med databehandling - samt i præventivt øjemed - så vidt muligt bør indføres præcise og konkrete regler vedrørende logning.

Det var derfor Datatilsynet opfattelse, at reglerne om logning principielt burde fremgå af (selve) konventionen, om end reglerne kunne uddybes i administrativt fastsatte bestemmelser.

Under alle omstændigheder fandt Datatilsynet, at der fra dansk side burde arbejdes for, at sikkerhedsniveauet er så højt som muligt, gerne svarende til det niveau, der i Danmark er fastsat i sikkerhedsbekendtgørelsen². Datatilsynet pegede i den forbindelse særligt på kravet om totallogning.

9. Ifølge de gældende regler for udveksling af oplysninger med tredjelande er det bl.a. en betingelse, at det pågældende tredjeland sikrer et tilstrækkeligt højt beskyttelsesniveau, jf. konventionens artikel 18, stk. 1, nr. 2.

Datatilsynet opfattede ændringsforslaget således, at der blev givet mulighed for at fravige dette udgangspunkt, idet der i de generelle regler kunne fastsættes mulighed for - i undtagelsestilfælde - at fravige udgangspunktet.

Ifølge forslaget til artikel 18, stk. 2, nr. 3, var det endvidere ikke nødvendigt at foretage en vurdering af beskyttelsesniveauet i det pågældende tredjeland, hvis den medlemsstat, der gav de pågældende oplysninger til Europol, gav tilladelse til videregivelse.

Det følger af de nugældende generelle regler for Europols videregivelse af personoplysninger (Rådets Retsakt af 12. marts 1999 med senere ændringer), at man både i tilfælde, hvor der foreligger en aftale, og i nødsituationer skal tage hensyn til lovgivningen og den administrative praksis på databeskyttelsesområdet i det pågældende tredjeland.

Datatilsynet bemærkede endvidere, at det følger af politirekommandationens princip 5.4 b, at det - hvis der ikke foreligger en særlig aftale om udveksling af oplysninger - bl.a. er en betingelse for udveksling af oplysninger, at der tages hensyn til nationale beskyttelsesregler.

Af dette princip kan udledes, at den, der videregiver oplysninger, forudgående må foretage en vurdering af, hvorvidt "modtagerlandet" set i lyset af den konkrete situation har et tilfredsstillende databeskyttelsesniveau på politiområdet. Hvis dette ikke er tilfældet, vil en videregivelse efter omstændighederne kunne være i strid med politirekommandationen.

Datatilsynet kunne ikke på det foreliggende grundlag se, hvorledes man påtænkte at udnytte hjemlen i forslagets artikel 18, stk. 2, nr. 3, men henledte Justitsministeriets opmærksomhed på ovenstående principper.

² Jf. § 19 i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

10. Ifølge forslaget til artikel 21 skulle den gældende opbevaringsfrist udvides for så vidt angår oplysninger lagret i henhold til artikel 10, stk. 1, fra 3 til 5 år. Samtidig hermed blev det foreslået at udvide revisionsfristen fra 1 til 3 år.

Datatilsynet havde ikke afgørende indvendinger mod en absolut opbevaringsfrist på 5 år for så vidt angår oplysninger i analysedatabaser. Tilsynet forudsatte selvsagt, at den enkelte opbevaring skete ud fra konkrete sagligt begrundede hensyn.

Det var Datatilsynets opfattelse, at en udvidelse af revisionsfristen til 3 år kunne forekomme noget lang, uanset at visse praktiske hensyn kunne tale for en sådan udvidelse.

Efter en samlet vurdering henstillede Datatilsynet, at det overvejes at bibeholde en revisionsfrist på 1 år. En revisionsfrist på 1 år fremgår i øvrigt også af dokument EUROPOL 76.

Samlet set var det Datatilsynets opfattelse, at forslaget - hvis det blev gennemført i sin helhed - vil medføre væsentlige ændringer i Europol-konventionen. Datatilsynet opfordrede derfor generelt til, at behovet for de foreslåede ændringer nøje blev afvejet overfor de databeskyttelsesretlige konsekvenser, som forslaget ville have.

Datatilsynet henviste i øvrigt til JSB's udtalelse vedrørende det danske forslag.



Sager om behandling af personoplysninger

<i>Behandling af personoplysninger i videnskabeligt og journalistisk øjemed</i>	36
<i>Fagforenings udsendelse af medlemsfortegnelse</i>	39
<i>Fælles skadesregister for forsikringsbranchen</i>	40
<i>Lokal-tv fra overvågningskameraer i indkøbscenter</i>	42
<i>Offentliggørelse af situationsbilleder på internettet</i>	44
<i>Sager om markedsføringsreglerne</i>	46
<i>- FDB's medlemsprogram</i>	
<i>- Forskellige spørgsmål om indsigelsesreglen i lovens § 36, stk. 2</i>	
<i>- Samtykkekravet i bonusklubber</i>	
<i>- TDC Forlags videregivelse af telefonbogsoplysninger</i>	
<i>Sortliste over virksomheder i træbranchen</i>	56
<i>Spørgsmål om frivillig registrering i et kreditoplysningsbureau</i>	58
<i>Terminaladgang til Centralregisteret for Motorkøretøjer</i>	59
<i>Transmission af live-video fra en pub</i>	61
<i>Tv-overvågning i supermarkedskæde</i>	63
<i>Videregivelse af oplysninger fra forskningsprojekter</i>	68
<i>Videregivelse af oplysninger om indkomstforhold i forbindelse med ansøgninger om boligstøtte</i>	69

Sager om behandling af personoplysninger

Behandling af personoplysninger i videnskabeligt og journalistisk øjemed

Udtalt, at Datatilsynet ikke kunne meddele tilladelse til videregivelse af personoplysninger indhentet i videnskabeligt eller statistisk øjemed, idet oplysningerne hos modtageren ikke alene skulle anvendes med henblik på videnskabelige eller statistiske undersøgelser, men også i journalistisk øjemed. Endvidere udtalt, at tilsynet ikke kunne meddele tilladelse til det anmeldte projekt, idet de anmeldte behandlinger ikke fandtes at opfylde betingelserne i persondataloven for behandlinger, der foretages til videnskabelige eller statistiske formål (Datatilsynet j.nr. 2002-41-2492 og 2002-3311-0175)

Datatilsynet modtog anmeldelse af en videnskabelig undersøgelse af psykiatrisk tvang i psykiatrien.

Det fremgik af anmeldelsen, at anmelderen var journalist på et dagblad, og at projektet skulle gennemføres med henblik på offentliggørelse af resultater i dagbladet. Projektet ville omfatte oplysninger om ca. 10.000-15.000 psykiatriske patienter og behandlere i den offentlige sundhedssektor.

Om patienterne ville der indgå identifikationsoplysninger, helbredsoplysninger og oplysninger om tvangsanvendelse mod patienten samt baggrund herfor.

Om behandlerne (ansvarlige overlæger, læger samt plejepersonale) ville der indgå identifikationsoplysninger, stillingsbetegnelse samt oplysninger om deltagelse i tvang over for psykiatriske patienter.

I forbindelse med anmeldelsen blev der ansøgt om Datatilsynets tilladelse til at offentliggøre oplysninger om navn, stillingsbetegnelse og ansættelsessted på offentligt ansat personale på psykiatriske afdelinger, der var impliceret som myndighedspersoner i tvangsanvendelse.

Oplysningerne skulle indhentes fra Sundhedsstyrelsens "Register over anvendelse af tvang i psykiatrien", som er oprettet udelukkende i videnskabeligt eller statistisk øjemed.

Persondataloven indeholder i § 10 visse særregler for behandling til videnskabelige eller statistiske formål.

Efter § 10, stk. 1, må der ske behandling af de oplysninger som er nævnt i § 7, stk. 1, eller § 8, dvs. følsomme oplysninger, herunder helbredsoplysninger, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelserne.

Af bemærkningerne til denne bestemmelse fremgår, at såfremt en behandling tillige har andre formål, vil behandlingen skulle vurderes efter bestemmelserne i henholdsvis § 7, stk. 2-4, og § 8, stk. 1-2 og stk. 4-5.

Ifølge § 10, stk. 2, må de af stk. 1 omfattede oplysninger ikke senere behandles i andet end statistisk eller videnskabeligt øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages i statistisk eller videnskabeligt øjemed, jf. § 6.

De af § 10, stk. 1 og 2, omfattede oplysninger må ifølge § 10, stk. 3, kun videregives til tredjemand efter forudgående tilladelse fra tilsynsmyndigheden.

Efter at sagen havde været behandlet på et møde i Datarådet, tilkendegav Datatilsynet, at tilsynet på baggrund af sagens oplysninger måtte lægge til grund, at den anmeldte behandling af personoplysninger ikke alene skulle finde sted med henblik på videnskabelige eller statistiske undersøgelser, men tillige skulle ske med journalistiske formål for øje.

Det var herefter Datatilsynets opfattelse, at de anmeldte behandlinger ikke kunne ske i medfør af reglerne i persondatalovens § 10 om behandlinger, der foretages til videnskabelige eller statistiske formål. Det var endvidere Datatilsynets opfattelse, at behandlingen af de omhandlede helbredsoplysninger ikke uden de registrerede personers udtrykkelige samtykke kunne ske inden for rammerne af lovens § 7.

På dette grundlag fandt Datatilsynet ikke at kunne give tilladelse i henhold til persondatalovens § 50, stk. 1, nr. 1, til det anmeldte projekt.

Datatilsynet bemærkede i øvrigt, at enhver videregivelse af oplysninger, som indgår i et videnskabeligt projekt, herunder almindelige oplysninger omfattet af lovens § 6, kun kan ske med respekt af persondatalovens § 10, stk. 2 og 3. Oplysningerne må således ikke videregives i andet end statistisk eller videnskabeligt øjemed og kun efter forudgående tilladelse fra Datatilsynet. Uanset om oplysningerne er af følsom eller fortrolig art, vil Datatilsynet således ikke kunne give tilladelse til en offentliggørelse, der muliggør identifikation af de pågældende personer, idet en sådan offentliggørelse efter tilsynets opfattelse ikke kan siges alene at tjene et videnskabeligt eller statistisk øjemed.

Afslutningsvis bemærkede Datatilsynet, at da Sundhedsstyrelsens register over tvang i psykiatrien er oprettet udelukkende i statistisk og videnskabeligt øjemed, kunne tilsynet ikke give Sundhedsstyrelsen tilladelse efter persondatalovens § 10, stk. 3, til at videregive oplysninger til behandlinger, der ikke alene finder sted i statistisk eller videnskabeligt øjemed.

I en lignende sag modtog Datatilsynet en anmodning fra et amt om tilladelse til efter § 10, stk. 3, 1. punkt, at videregive oplysninger vedrørende amtets gødningsregnskab til DICAR, Dansk Institut for Computerstøttet Journalistik.

DICAR havde anmodet om en komplet kopi af gødningsregnskabet for amtets landmænd, som var identificeret ved bl.a. navn og adresse. Oplysningerne var efter det oplyste tidligere indhentet af amtet med Datatilsynets tilladelse fra "Det Forskningsrelaterede Jordbrugsregister FRJOR". FRJOR er et forskningsregister ved Danmarks Jordbrugsforskning.

Det fremgik af sagen, at DICAR skulle benytte de omhandlede data som grundlag for analyser, som kunne bruges i journalistisk form, enten via aviser, radio eller tv. Instituttet havde oplyst, at det var afgørende at modtage en komplet kopi af gødningsregnskabet med personrelaterede oplysninger, idet dette var nødvendigt for at kunne lave de korrekte analyser af landmændenes gødningsforbrug.

DICAR havde desuden oplyst, at instituttet var indforstået med, at det ikke måtte offentliggøre data, der kunne henføres til den enkelte landmand. Instituttet havde i den forbindelse forestillet sig at lave analyser fordelt på kommuner, de gamle sogne eller postnumre. Imidlertid oplyste DICAR, at offentliggørelsen af data om en konkret landmand, ville kunne ske med vedkommende landmands accept.

Efter at sagen havde været behandlet på et møde i Datarådet, udtalte Datatilsynet, at da oplysningerne i det omhandlede udtræk indgik i en behandling udelukkende i statistisk og videnskabeligt øjemed, måtte amtet ikke videregive oplysningerne i andet end statistisk eller videnskabeligt øjemed, jf. persondatalovens § 10, stk. 2, og dette kun efter forudgående tilladelse fra Datatilsynet, jf. persondatalovens § 10, stk. 3.

På baggrund af sagens oplysninger måtte Datatilsynet lægge til grund, at DICAR's behandling af oplysninger i gødningsregnskaberne for landmænd i amtet *ikke* alene skulle ske til videnskabelige eller statistiske formål, men navnlig i journalistisk øjemed.

Datatilsynet fandt på dette grundlag, at videregivelse af det omhandlede udtræk ville være i strid med reglerne i lovens § 10, stk. 2, og tilsynet kunne derfor ikke meddele amtet tilladelse til videregivelse efter persondatalovens § 10, stk. 3.

Afslutningsvis udtalte Datatilsynet, at hvis amtet imidlertid tillige var i besiddelse af de omhandlede oplysninger i en administrativ sammenhæng, ville en videregivelse kunne finde sted, i det omfang behandlingsreglerne i personda-

talovens § 6, stk. 1, skønnes opfyldt, herunder inden for rammerne af interesseafvejningsreglen i § 6, stk. 1, nr. 7.

Udtalt, at udsendelse af en medlemsfortegnelse på elektronisk medie alene kan ske, hvis fagforeningen har indhentet hvert enkelt medlems samtykke. Dette gælder også for udsendelse af en medlemsfortegnelse i en ikke-elektronisk form (Datatilsynets j.nr. 2002-214-0046)

Fagforenings udsendelse af medlemsfortegnelse

Sagen vedrørte en henvendelse fra Ingeniørforeningen i Danmark (IDA), som spurgte, hvorvidt persondataloven satte grænser for foreningens påtænkte udsendelse af en elektronisk medlemsfortegnelse. IDA anmodede samtidig Datatilsynet om at oplyse, hvorvidt udgivelsen af medlemsfortegnelsen alternativt kunne ske på et ikke-elektronisk medie.

Det blev under sagens behandling oplyst, at IDA var en fagforening, som organiserede ca. 60.000 medlemmer.

Sagen blev behandlet på et møde i Datarådet.

Datatilsynet bemærkede indledningsvis, at der ved udgivelse af en medlemsfortegnelse, som principielt ville kunne udgives til 60.000 medlemmer, ville være tale om videregivelse (offentliggørelse) af oplysninger om det enkelte medlem.

Det følger af persondatalovens § 7, stk. 1, at der som udgangspunkt ikke må behandles (f.eks. videregives) oplysninger om bl.a. fagforeningsmæssige tilhørsforhold.

Da IDA er en fagforening, ville der ved udsendelse af en medlemsfortegnelse ske videregivelse af oplysninger omfattet af persondatalovens § 7, stk. 1.

Efter Datatilsynets opfattelse kunne ingen af bestemmelserne i § 7, stk. 2, nr. 2-4, eller de øvrige undtagelsesregler i § 7, stk. 3-8, anvendes som hjemmelsgrundlag for udsendelse af den omhandlede medlemsfortegnelse til medlemmerne.

Udsendelse af den nævnte medlemsfortegnelse kunne herefter - efter Datatilsynets opfattelse - alene ske, hvis IDA forinden indhentede hvert enkelt medlems samtykke i overensstemmelse med lovens § 7, stk. 2, nr. 1, jf. § 3, nr. 8.

Datatilsynet bemærkede endvidere, at udsendelse af en medlemsfortegnelse i en ikke-elektronisk form - f.eks. en trykt fortegnelse - efter omstændigheder-

ne ville være omfattet af persondataloven enten i medfør af § 1, stk. 1, eller § 1, stk. 2, hvorfor de ovenfor nævnte betragtninger også fandt anvendelse for så vidt angik udsendelse af en sådan medlemsfortegnelse. Datatilsynet lagde i den forbindelse til grund, at der i den ikke-elektroniske medlemsfortegnelse anvendes en form for systematik eller struktur, der gør det muligt at finde frem til personoplysninger.

Ingeniørforeningen i Danmark har efterfølgende bekræftet over for Datatilsynet, at eventuelle fremtidige udgivelser af en medlemsfortegnelse alene vil indeholde oplysninger om de medlemmer, der har givet deres samtykke til optagelse i medlemsfortegnelsen.

Fælles skadesregister for forsikringsbranchen

Fundet, at et landsdækkende skadesregister alene vil kunne oprettes, hvis der foreligger samtykke hertil fra forsikringstagerne (Datatilsynets j.nr. 2002-213-0120)

På baggrund af en forespørgsel fra Forsikring & Pension anmodede Justitsministeriet Datatilsynet om en udtalelse om, hvorvidt, og i givet fald under hvilke betingelser, forsikrings erhvervet ville kunne oprette et landsdækkende skadesregister efter de gældende regler i persondataloven. Registeret skulle indeholde oplysninger om de skader, den enkelte forsikringstager har anmeldt til sit/sine forsikringsselskaber inden for de sidste fem år.

Formålet med registeret skulle være at give forsikringsskaberne et bedre grundlag for konkret at træffe beslutning om, hvorvidt omstændighederne omkring en anmeldt skade skulle undersøges nærmere. Samtidig påregnedes selve eksistensen af registeret at kunne forebygge forsikringsvindelse. Det var ikke hensigten at anvende registeret i tegningsituationen eller til at søge oplysninger i om den enkelte kunde.

Baggrunden for ønsket om et sådant register var, at forsikringsvindelens har et stort og stigende omfang. Forsikring & Pension oplyste, at alene på privatforsikringsområdet inden for skadesforsikring skyldes 10 pct. af erstatningsudbetalingerne forsikringsvindelse, hvilket beløber sig til over 1 mia. kr. årligt.

Datatilsynet behandlede sagen på et møde i Datarådet. Tilsynet konstaterede, at Registertilsynet under den tidligere gældende lov om private registre fik forelagt forsikrings erhvervets ønske om etablering af et fælles skadesregister. Sagen er omtalt i Registertilsynets årsberetning for 1996, side 78.

Efter forelæggelse for Registerrådet udtalte Registertilsynet, at oprettelsen af et register med et indhold og et omfang som det påtænkte ikke var i overensstemmelse med lov om private registre § 3, stk. 1, uanset at formålet

med registeret måtte anses for anerkendelsesværdigt og et naturligt led i normal forsikringsvirksomhed.

Tilsynet lagde i den forbindelse navnlig vægt på, at registeret ville blive landsdækkende, meget stort og indeholdende data om en meget betydelig del af samtlige forsikrede i Danmark, at langt hovedparten af de registrerede ville være registreret, selv om de ikke på nogen måde havde gjort sig skyldig i et ulovligt eller mistænkeligt forhold, at registeret måtte antages kun for en meget lille del af de registrerede at ville kunne afsløre egentligt forsikringsmisbrug, og at det efter tilsynets opfattelse reelt ikke kunne sikres, at registeret ikke ville blive anvendt til at sortere ærlige, men uheldige kunder fra.

Datatilsynet bemærkede herefter, at spørgsmålet også blev taget op under behandlingen af det 1. lovforslag til persondataloven (lovforslag nr. L 82 af 30. april 1998). Folketingets Retsudvalg spurgte således, om justitsministeren var enig i, at forslaget § 6, nr. 2, (som svarer til den nugældende § 6, stk. 1, nr. 2) ikke indeholdt hjemmel til oprettelse af et skadesregister. Efter Justitsministeriets opfattelse ville Rådet for Dansk Forsikring & Pension alene kunne oprette et skadesregister af den karakter, som Registertilsynet tog stilling til i 1996, hvis der foreligger samtykke hertil fra forsikringstagerne.

Ifølge bemærkningerne til § 6 i lovforslag nr. L 147 af 9. december 1999 bygger behandlingsreglerne i persondataloven § 6, § 7 og § 8 på den forudsætning, at reglerne i videst muligt omfang skal administreres på den måde, at der ikke - uden samtykke - registreres og videregives personoplysninger i videre udstrækning end efter den gældende registerlovgivning.

Idet Datatilsynet lagde til grund, at der ikke er tale om behandling af detaljerede oplysninger om eventuel personskades art og omfang, men alene af oplysninger om skadestype og den berørte forsikringsbranche (som beskrevet i sagen fra 1996), og at der således ikke vil være tale om følsomme oplysninger omfattet af persondatalovens §§ 7-8, udtalte Datatilsynet, at lovligheden af et landsdækkende skadesregister efter tilsynets opfattelse skal vurderes i forhold til persondatalovens § 6 samt § 11, stk. 2 (sidstnævnte for så vidt angår registrering af personnumre). Endvidere skal lovens grundlæggende regler i § 5 om bl.a. sagligt formål og proportionalitet tages i betragtning.

Under henvisning til de forhold, som Registertilsynet tidligere har tillagt vægt, og til det af Justitsministeriet anførte i forbindelse med besvarelsen af Retsudvalgets spørgsmål fandt Datatilsynet, at et landsdækkende skadesregister som beskrevet alene ville kunne oprettes, hvis der foreligger samtykke hertil fra forsikringstagerne.

Lokal-tv fra overvågningskameraer i indkøbscenter

Fundet, at et konkret tv-projekt havde såvel et kunstnerisk som et journalistisk øjemed, og at det faldt uden for Datatilsynets kompetence at tage stilling til projektets eventuelle behandlinger af personoplysninger (Datatilsynets j.nr. 2002-321-0155)

Radio- og tv-nævnet anmodede om Datatilsynets stillingtagen til et tv-projekt, som indebar, at man med et kunstnerisk og socialt formål ville sende live-dokumentar udsendelser fra Vollsmose-området i Odense.

Baggrunden for henvendelsen var ifølge det oplyste, at Radio- og tv-nævnet som ankeinstans på lokalradio- og tv-området havde modtaget en klage fra Lokal-tv foreningen Frekvens over Odense Lokal radio- og tv-nævns afslag på foreningens ansøgning om programtilladelse til det pågældende projekt.

Det var tanken med projektet, at der via allerede eksisterende overvågningskameraer opsat i et indkøbscenter - Center Øst - skulle etableres kabelforbindelser til beboelsesområderne Bøge-, Ege- og Birkeparken med henblik på at transmittere billeder fra centerets kameraer dagligt i en nærmere tidsmæssigt afgrænset periode. Billederne ville desuden blive gengivet på storskærme i centeret. Kameraerne ville blive tydeligt markeret, og selve billedzonen ville blive optrukket og indrammet på gulvet, således at det var muligt at færdes i centeret uden at komme i tv.

Projektet skulle skabe en platform for live-dokumentar udsendelser, hvor beboerne selv bidrog med indholdet, og indholdet blev holdt åbent og varierende fra udsendelse til udsendelse. Ifølge foreningen lod den planlagte programvirksomhed sig bedst beskrive som "Public access", der inddrog borgerne i produktionen. Foreningen ville imødekomme de mediesvage grupper ved at give dem mulighed for at være med til at skabe et offentligt TV-forum. Foreningen ønskede herved at gøre beboerne opmærksomme på områdets skjulte ressourcer ved at gentænke og se med nye øjne på nærmiljøet.

Forinden henvendelsen til Datatilsynet havde Radio- og tv-nævnet rettet henvendelse til Justitsministeriet og spurgt, om den eksisterende overvågning var i overensstemmelse med lov om forbud mod tv-overvågning m.v. Justitsministeriet lagde i sit svar til grund, at den eksisterende overvågning var omfattet af § 2, nr. 1, i lov om forbud mod tv-overvågning m.v., som indeholder en undtagelse fra lovens forbud i § 1, stk. 1. Justitsministeriet havde imidlertid samtidig gjort opmærksom på, at lov om forbud mod tv-overvågning alene regulerer *selve adgangen* til at foretage filmisk overvågning, mens spørgsmålet om, på hvilken måde optagelserne af en (lovlig) tv-overvågning kan behandles og opbevares m.v., skal afgøres efter reglerne i persondataloven.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at med hensyn til billeder, hvor der ikke foreligger andre oplysninger end selve

fotografiet til at identificere den pågældende, vil billedet blive betragtet som personhenførbart og dermed omfattet af persondataloven, hvis billedet bliver forevist til personer, der vil kunne genkende den fotograferede. Datatilsynet fandt på den baggrund, at den beskrevne behandling var omfattet af persondataloven, jf. lovens § 1, stk. 1, idet en transmission af video fra overvågningskameraerne til lokal-tv og via storskærme efter tilsynets opfattelse indebar en tilgængeliggørelse af de pågældende optagelser for en så bred personkreds, at det var sandsynligt, at nogen ville kunne genkende de filmede personer.

Datatilsynet fandt endvidere, at selve overvågningen og transmissionen af billeder herfra på storskærme og på lokal-tv ville kunne udgøre en elektronisk behandling omfattet af persondatalovens § 1, stk. 1. Dette ville under alle omstændigheder være tilfældet, hvis der gøres brug af digitale kameraer.

Datatilsynet henviste herefter til persondatalovens § 2, stk. 10, hvoraf fremgår, at for behandling af oplysninger, som i øvrigt udelukkende finder sted i journalistisk øjemed, gælder alene bestemmelserne i persondatalovens §§ 41, 42 og 69. Det samme gælder for behandling af oplysninger, som udelukkende sker med henblik på kunstnerisk eller litterær virksomhed.

§ 2, stk. 10, er efter sin ordlyd ikke indskrænket i forhold til lovens behandlingsbegreb. Datatilsynet oplyste på den baggrund, at det er Datatilsynets opfattelse, at bestemmelsen normalt må omfatte *al anden* behandling, der udelukkende sker med henblik på journalistisk eller kunstnerisk øjemed, og som ikke er omfattet af lovens § 2, stk. 6-9.

Yderligere vil bestemmelsen i lovens § 2, stk. 2, medføre, at et periodisk skrift eller et radio- eller tv-program, der indebærer udveksling af meningstilkendegivelser omfattet af ytringsfriheden, er undtaget fra persondataloven, uanset om der er tale om journalistisk eller kunstnerisk virksomhed. Det følger således af persondatalovens § 2, stk. 2, at loven ikke finder anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10.

Det var i den forbindelse Datatilsynets opfattelse, at det konkrete tv-projekt måtte formodes netop at indbefatte menings- og tankeudvekslinger som omtalt i menneskerettighedskonventionens artikel 10. Datatilsynet lagde herved vægt på, at programmet skulle anvendes til at stille spørgsmålstejn ved byplanlæggeres anvendelse og opbygning af rum og beboelsesområder.

Datatilsynet fandt endvidere, at det var uden betydning for vurderingen i forhold til persondatalovens § 2, stk. 10, at der i forbindelse med det konkrete tv-projekt anvendtes allerede eksisterende overvågningskameraer til brug for

transmissionen af udsendelserne, eller at billederne ligeledes blev gengivet på storskærme.

Idet Datatilsynet fandt, at det konkrete tv-projekt måtte anses at have et kunstnerisk såvel som et journalistisk øjemed, jf. persondatalovens § 2, stk. 10, lå det således uden for Datatilsynets kompetence at tage stilling til projektets eventuelle behandling af personoplysninger. Projektet ville herefter alene være omfattet af bestemmelserne i lovens §§ 41, 42 og 69.

Da det af en særskilt henvendelse fra lokal tv-foreningen Frekvens til Datatilsynet fremgik, at projektet som helhed også havde et socialt sigte, og at tv-projektet baserede sig på en rapport - "Ögon över Vollsrose", som blev udarbejdet i uddannelsesøjemed, samt at det af indledningen til rapporten var anført, at der var tale om et oplæg til videre kommunikation og forskning, henledte Datatilsynet lokal tv-foreningens opmærksomhed på anmeldelsesreglerne m.v. i persondatalovens § 48 og § 50 for det tilfældes skyld, at der efterfølgende skulle behandles eventuelle følsomme oplysninger i videnskabeligt øjemed.

For en god ordens skyld henledte Datatilsynet endelig opmærksomheden på persondatalovens § 2, stk. 6-8, om behandlinger omfattet af lov om massemediers informationsdatabaser samt om andre informationsdatabaser omfattet af medieansvarslovens § 1, nr. 1-3. Heraf fremgår, at loven under nærmere fastsatte betingelser heller ikke gælder for sådanne informationsdatabaser.

Offentliggørelse af situationsbilleder på internettet

Fundet, at harmløse situationsbilleder i visse tilfælde kan offentliggøres på internettet uden samtykke. Billeder af ansatte eller kunder kan dog normalt kun offentliggøres med samtykke (Datatilsynets j.nr. 2002-216-0109)

Offentliggørelse på internet af billeder af genkendelige personer betragtes som en elektronisk behandling af personoplysninger. Dette gælder, uanset om billedet er ledsaget af en tekst, der identificerer den pågældende.

Offentliggørelsens lovlighed skal bedømmes efter reglerne i loven, navnlig § 6, stk. 1, herunder interesseafvejningsreglen i § 6, stk. 1, nr. 7. Endvidere skal de grundlæggende principper i lovens § 5 om god databehandlingskik, saglighed og proportionalitet tages i betragtning. Det er i første række den dataansvarlige selv, der skal foretage vurderingen i de konkrete situationer.

Datatilsynets praksis vedrørende offentliggørelse af billeder på internet:

Situationsbilleder

Situationsbilleder defineres i denne sammenhæng som billeder, hvor en aktivitet eller en situation er det egentlige formål med billedet. Det kan f.eks. være gæster til en rockkoncert, legende børn i en skolegård eller besøgende i en zoologisk have.

Modsætningen hertil er portrætbilleder, hvor formålet er at afbilde en eller flere bestemte personer, jf. mere herom nedenfor.

Udgangspunktet er, at situationsbilleder kan offentliggøres uden samtykke med hjemmel i interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7.

Da der er tale om en helhedsvurdering af formålet med offentliggørelsen, skal offentliggørelse ske under skyldig hensyntagen til karakteren af billedet, herunder den sammenhæng, hvori billedet optræder og formålet med offentliggørelsen. Det afgørende kriterium er, at den afbildede ikke med rimelighed må kunne føle sig udstillet, udnyttet eller krænkede, f.eks. i markedsførings- eller andet kommercielt øjemed. Billederne skal således være harmløse.

Eksempler på situationsbilleder, der som udgangspunkt kan offentliggøres uden samtykke:

- Billeder optaget under en fritidsklubs udfoldelse af aktiviteter
- Billeder optaget af unges ophold på en efterskole eller anden privat skole
- Billeder optaget ved en kommunal skoles juleafslutning

Billeder kan dog være af en sådan beskaffenhed, at det må antages at virke krænkende for de afbildede. Dette kunne f.eks. være, hvis to genkendelige personer afbildes i intime situationer.

En indsigelse mod et offentliggjort billede vil derudover konkret kunne bevirke, at interesseafvejningen falder ud til fordel for den registrerede.

Følgende situationsbilleder vil normalt ikke kunne offentliggøres uden samtykke:

- Billeder optaget af ansatte på arbejde i en privat virksomhed eller hos en offentlig myndighed
- Billeder af kunder i en forretning, i banken, på posthuset m.v.
- Besøgende på en bar, natklub, diskotek eller lignende

Portrætbilleder

Som altovervejende hovedregel kræver det samtykke at offentliggøre portrætbilleder på internet.

Dette er begrundet i, at en sådan offentliggørelse vil kunne medføre ulemper for de registrerede, idet nogle mennesker vil kunne føle ubehag ved, at sådanne billeder, eventuelt sammen med oplysninger om navn m.v., gøres offentligt tilgængeligt for alle, der har adgang til internet, og at denne ulempe vejer tungere end interessen i offentliggørelsen, jf. interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7.

Hvis en skole f.eks. ønsker at offentliggøre portrætbilleder eller klassebilleder af eleverne på sin hjemmeside, må det kun ske, hvis der inden offentliggørelsen indhentes et udtrykkeligt samtykke fra hver enkelt elev, eller dennes forældre afhængig af elevens alder.

På Datatilsynets hjemmeside findes flere tekster om offentliggørelse på internet.

Sager om markedsføringsreglerne

FDB's medlemsprogram

Udtalt, at FDB - på baggrund af et samtykke - kunne udsende markedsføringsmateriale til personlige medlemmer af henholdsvis de enkelte brugsforeninger, Coop Danmark, FDB og eksterne samarbejdspartnere (Datatilsynets j.nr. 2001-216-0068)

I forbindelse med en kommende omstrukturering spurgte FDB om dennes eventuelle konsekvenser i forhold til persondataloven.

Det fremgik af sagen, at FDB fra 1. januar 2002 skulle fusionere sine dagligvareaktiviteter med sine svenske og norske søsterorganisationer i et fælles-ejet selskab - Coop Norden AB. Efter omstruktureringen skulle FDB ikke drive dagligvarehandel direkte, men gennem ovennævnte selskab. FDB skulle dog videreføre de aktiviteter, der ikke havde med dagligvareaktiviteter at gøre.

Datatilsynet behandlede sagen i Datarådet.

Datatilsynet havde på det foreliggende grundlag ikke bemærkninger til FDB's administration af bonusprogrammet. Efter Datatilsynets opfattelse kunne FDB på baggrund af samtykkeerklæringen registrere og samkøre oplysninger om medlemmernes køb hos FDB, brugsforeningerne samt de til enhver tid tilknyttede partnere i medlemssamarbejdet, til brug for beregning af medlemsbonus og dividende.

I øvrigt vil disse behandlinger formentlig også uden samtykke kunne ske i medfør af lovens § 6, stk. 1, nr. 2, i hvert fald i det omfang, handlingerne

af personoplysninger er nødvendige for, at FDB kunne drive og administrere medlemsprogrammet og hermed opfylde de forpligtelser, der påhviler FDB.

I relation til persondatalovens markedsføringsregler medførte FDB's særlige organisation efter Datatilsynets opfattelse ikke, at FDB ikke skal anses for en virksomhed. Uanset at dagligvarehandelen og medlemsprogrammet varetages af forskellige enheder i FDB-"koncernen", har medlemsprogrammet efter Datatilsynets opfattelse også et væsentligt erhvervmæssigt sigte, idet det medvirker til at tiltrække og fastholde kunder i "koncernens" butikker. Hertil kommer, at FDB fortsat har aktiebesiddelsen i en række selskaber, der ikke vedrører dagligvarehandel.

Det var derfor Datatilsynets opfattelse, at FDB efter persondataloven skal betragtes som en *virksomhed*.

Datatilsynet foretog en vurdering af rækkevidden af den samtykkeerklæring, som FDB's medlemmer ved indmeldelsen havde underskrevet. Dette skete bl.a. i lyset af Sø- og Handelsrettens dom i sagen om Interessebank Danmark (Sø- og Handelsrettens dom af 15. marts 2002).

Det var herefter Datatilsynets opfattelse, at FDB på baggrund af samtykkeerklæringens formulering kan udsende markedsføringsmateriale til de personlige medlemmer af henholdsvis de enkelte brugsforeninger, Coop Danmark, FDB og eksterne samarbejdspartnere. Tilsynet fandt således, at det i samtykkeerklæringen indeholdte udtryk "ydelse af medlemsfordele" må forstås som tillige omfattende udsendelse af materiale om disse.

Datatilsynet understregede, at samtykkeerklæringen alene giver FDB adgang til selv at anvende medlemsoplysningerne til at sende materiale ud i de omhandlede situationer. Medlemsoplysningerne må således *ikke videregives*.

For yderligere information om Datatilsynets praksis vedrørende medlems- og bonusklubber henvises til tilsynets hjemmeside www.datatilsynet.dk - under punktet Værd-at-vide.

Forskellige spørgsmål om indsigelsesreglen i lovens § 36, stk. 2

Datatilsynet har bl.a. udtalt sig om følgende spørgsmål:

Tidsfrister i indsigelsesproceduren

Det følger af persondatalovens § 6, stk. 2-4, at en virksomhed ikke må videregive oplysninger om en forbruger til en anden virksomhed til brug ved markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i

dette øjemed, medmindre forbrugeren har givet sit samtykke hertil. Videregivelse og anvendelse kan dog ske uden samtykke, hvis der er tale om generelle kundeoplysninger.

I de tilfælde, hvor videregivelse eller anvendelse af generelle kundeoplysninger kan ske uden samtykke, skal indsigelsesreglerne i § 36 iagttages. Heraf følger, at hvis kunden ikke har fremsat indsigelse direkte over for virksomheden, skal virksomheden - hver gang den ønsker at videregive kundeoplysninger til andre virksomheder til brug for markedsføring eller anvende kundeoplysninger på vegne af en anden virksomhed - checke i CPR, om kunden har frabedt sig henvendelser i markedsføringsøjemed. Er dette tilfældet, må oplysningerne ikke videregives eller anvendes til dette formål. Hvis kunden ikke gennem en markering i CPR har frabedt sig henvendelser, skal virksomheden endvidere - inden oplysningerne videregives eller anvendes - give kunden tydelig og forståelig meddelelse om indsigelsesretten. Virksomheden skal i den forbindelse give kunden en nem adgang til inden for en frist på to uger at fremsætte indsigelse mod, at videregivelse eller anvendelse finder sted. Videregivelse eller anvendelse må ikke finde sted, før det er konstateret, at forbrugeren ikke har fremsat indsigelse inden udløbet af fristen på 2 uger.

Der ses hverken i persondataloven eller i lovens forarbejder at være noget krav om, at videregivelsen af oplysningerne til en virksomhed eller anvendelsen på vegne af en anden virksomhed skal ske umiddelbart efter indsigelsesfristens udløb. Ligeledes ses der hverken i loven eller i forarbejderne fortolkningsbidrag til vurdering af, hvor lang tid der kan gå fra indsigelsesfristens udløb, til den egentlige behandling af oplysningerne sker.

En forbruger, som modtager en meddelelse i henhold til § 36 om indsigelsesretten samt mulighed for at gøre indsigelse inden for 2 uger, må efter Datatilsynets opfattelse have en berettiget forventning om, at en eventuel videregivelse til eller anvendelse på vegne af en anden virksomhed finder sted ikke alt for længe efter indsigelsesperiodens udløb.

Det er derfor Datatilsynets opfattelse, at videregivelsen eller anvendelsen på vegne af en anden virksomhed skal ske inden for *en rimelig tid* efter indsigelsesfristens udløb.

Datatilsynet har i den forbindelse endvidere henvist til persondatalovens § 5, stk. 1, hvorefter oplysninger skal behandles i overensstemmelse med god databehandlingsskik.

Datatilsynet har understreget, at overvejelserne om, hvor lang tid efter indsigelsesproceduren den egentlige behandling kan vente, ikke i videregivelsessituationer medfører indskrænkninger i modtagervirksomhedens adgang til at anvende de modtagne oplysninger til markedsføring af egne produkter i form

af tidsfrister for, hvornår markedsføringen kan ske efter modtagelsen af oplysningerne. I det omfang modtagervirksomheden har modtaget oplysningerne på lovlig vis til brug for markedsføring, er denne virksomheds direkte markedsføring ikke omfattet af persondataloven, men af markedsføringsloven.

Indsigelsesmeddelelse sammen med markedsføringsmateriale

Efter persondatalovens § 36, stk. 2, skal meddelelsen til forbrugeren være *tydelig og forståelig*, ligesom forbrugeren skal gives *en nem adgang* til inden for en frist på to uger at fremsætte indsigelse mod videregivelsen eller "anvendelsen på vegne af".

Persondatalovens § 36, stk. 2, udelukker som udgangspunkt ikke, at meddelelsen om indsigelsesmuligheden indeholder andre oplysninger, så længe meddelelsen er tydelig og forståelig, og forbrugeren gives *en nem adgang* til at fremsætte indsigelse.

Datatilsynet har imidlertid ikke fundet det muligt på forhånd at udtale sig med tilstrækkelig sikkerhed om, hvorvidt to foreslåede modeller for iagttagelse af indsigelsesproceduren i alle tilfælde vil være i overensstemmelse med bestemmelsen i persondatalovens § 36, stk. 2.

Tilsynet kunne således ikke på det foreliggende grundlag tage stilling til, om forbrugeren ved de omhandlede fremgangsmåder på tilstrækkelig tydelig og forståelig vis ville blive oplyst om sin ret til at gøre indsigelse, og om forbrugeren i det konkrete tilfælde ville kunne danne sig et tilstrækkeligt overblik over konsekvenserne af sit valg.

Datatilsynet bemærkede herved, at det i første omgang er den dataansvarlige, som skal afgøre, om betingelserne i § 36, stk. 2, er opfyldt. Datatilsynet vil i forbindelse med en konkret klagesag kunne efterprøve den dataansvarliges vurdering.

Datatilsynet vil i forbindelse med sin vurdering af udformningen af indsigelsesmeddelelsen tillige hense til den generelle bestemmelse i persondatalovens § 5, stk. 1.

Samtykkekravet i bonusklubber

Ændret praksis, således at en medlems- eller bonusklub o.l. kan anvende kundeoplysninger på vegne af eksterne samarbejdspartnere til markedsføring - selv om samarbejdspartnerne ikke er kendt af forbrugeren ved samtykkets afgivelse (Datatilsynets j.nr. 2002-631-0088)

Den 15. marts 2002 afsagde Sø- & Handelsretten dom i den sag, som Forbrugerombudsmanden i foråret 2001 anlagde mod Interessebank Danmark (et samarbejde mellem Post Danmark og TDC Forlag A/S).

Sagen drejede sig hovedsageligt om, hvorvidt det samtykke, som afgives af forbrugerne ved tilmelding til Interessebank Danmark til at modtage adresse-rede reklamer fra ikke identificerede erhvervsdrivende inden for forbrugerens interesseområder, opfylder kravene til en anmodning i markedsføringslovens § 6 a, stk. 3, og dermed fritager de erhvervsdrivende datakøbere fra at checke i CPR, om forbrugeren har frabedt sig henvendelser i markedsføringsøjemed.

Ved tilmelding til Interessebank Danmark afgiver forbrugeren oplysning om, hvilke interesseområder den pågældende har, og forbrugeren afgiver samtidig følgende samtykke over for Interessebank Danmark:

"Jeg er indforstået med, at Post Danmark til brug for Interessebank Danmark på egne og TDC Forlag A/S' vegne indsamler, behandler, registrerer og opbevarer oplysningerne i dette skema samt videregiver oplysningerne til TDC Forlag A/S, som ligeledes behandler, registrerer og opbevarer oplysningerne.

Jeg er ligeledes indforstået med, at TDC Forlag A/S på egne og Post Danmarks vegne videregiver mit navn og min adresse til virksomheder inden for mit interesseområde til brug for disse virksomheders markedsføring over for mig. Herved får jeg mulighed for at modtage tilbud og informationer fra virksomheder om områder, der interesserer mig og min familie."

Under sagen gjorde Forbrugerombudsmanden bl.a. gældende, at en forbrugers samtykke til modtagelse af adresseret reklamemateriale fra ikke nærmere angivne erhvervsdrivende ikke opfylder kravene til en anmodning i markedsføringslovens § 6 a, stk. 3, idet samtykket ikke er tilstrækkeligt informeret og konkretiseret, og idet forbrugeren ikke kender rækkevidden af samtykket. Forbrugerombudsmanden gjorde endvidere gældende, at et samtykke efter § 6 a, stk. 3, skal være givet over for den konkrete erhvervsdrivende, som udsender materialet, og at de erhvervsdrivende kunder derfor ikke på baggrund af det over for Interessebank Danmark afgivne samtykke lovligt kan markedsføre sig over for de forbrugere, der har frabedt sig markedsføringshenvendelser enten ved markering i CPR eller direkte over for den erhvervsdrivende.

Sø- & Handelsretten frifandt i det hele Interessebank Danmark. Retten fandt således ikke, at markedsføringslovens § 6 a, stk. 3, indeholder bestemmelser om, over for hvem anmodningen skal være fremsat, og bestemmelsen udelukker derfor ikke, at Interessebank Danmark indhenter et samtykke til vide-

regivelse af oplysninger om forbrugerne til andre erhvervsdrivende med henblik på direkte markedsføring.

Sø- & Handelsretten fandt endvidere, at forbrugerens samtykke til videregivelse af oplysningerne var tilstrækkeligt konkretiseret og informeret, selv om forbrugerne ikke kender navnene på de erhvervsdrivende, der kan sende forbrugeren reklamer.

På baggrund af Sø- & Handelsrettens dom i Interessebank Danmarksagen blev spørgsmålet om en eventuel revision af Datatilsynets praksis behandlet på et møde i Datarådet.

Datatilsynet fandt, at dommen bør have en afsmittende effekt på en række medlems- og bonusklubber o.l., hvor personer melder sig ind for at opnå rabatter og medlemsfordele hos forskellige virksomheder.

Henset til formålet med medlems- og bonusklubber er det Datatilsynets opfattelse, at et medlem vil kunne give samtykke til, at en medlems- eller bonusklub anvender oplysninger om medlemmet på vegne af de eksterne samarbejdspartnere til udsendelse af markedsføringsmateriale om dennes varer eller tjenesteydelser - uden at de fremtidige samarbejdspartnere behøver at være navngivne i samtykkeerklæringen. Det er dog en forudsætning, at der er en naturlig sammenhæng mellem klubkonceptet og de ydelser, der markedsføres over for forbrugerne, således at forbrugerne alene modtager markedsføringsmateriale om varer eller tjenesteydelser med en vis tilknytning til medlems- eller bonusklubbens interesseområde.

Når en medlems- eller bonusklub indhenter samtykke, skal der fortsat gives tilstrækkelig information til, at den samtykkende kan overskue konsekvenserne heraf. Dette betyder, at der skal gives en så præcis information som muligt på det pågældende tidspunkt, således at personen reelt kan overskue, hvad det er, der gives samtykke til. De samarbejdspartnere, der er kendt på tidspunktet for samtykkets afgivelse, skal angives præcist, ligesom der bør gives information om, at der senere kan komme nye samarbejdspartnere til, samt hvis muligt informeres om typen af fremtidige samarbejdspartnere.

Herudover skal der i medfør af princippet om god databehandlingsskik i persondatalovens § 5, stk. 1, gives information til medlemmerne ved optagelse af nye samarbejdspartnere, således at medlemmerne har mulighed for at fremsætte en indsigelse mod den pågældende behandling efter persondatalovens § 35 eller § 36, stk. 1.

Datatilsynet fandt fortsat, at en egentlig videregivelse til nye samarbejdspartnere med henblik på markedsføring baseret på samtykke må forudsætte, at samarbejdspartneren er nævnt i samtykkeerklæringen. Hvis der ikke foreligger

et sådant udtrykkeligt samtykke, må virksomheden følge indsigelsesprocedu-
ren i lovens § 36, og videregivelsen må kun omfatte generelle kundeoplys-
ninger.

Begrundelsen for Datatilsynets opfattelse er, at en videregivelse indebærer en
ikke uvæsentlig risiko for krænkelse af medlemmernes integritet, idet person-
lige oplysninger herved spredes til en større kreds. Datatilsynet fandt på den-
ne baggrund ikke anledning til at lempe praksis, når det drejer sig om sam-
tykke til videregivelse.

TDC Forlags videregivelse af telefonbogsoplysninger

*Udtalt, at videregivelse af berigede telefonbogsoplysninger skal ske i over-
ensstemmelse med markedsføringsreglerne i persondatalovens § 6, stk. 2-4,
og § 36 (Datatilsynets j.nr. 2002-212-0101)*

I forbindelse med en konkret klage over TDC Forlags videregivelse af oplys-
ninger om navn og adresse til Topdanmark blev det oplyst, at TDC Forlag i
henhold til lov om konkurrence- og forbrugerforhold på teleområdet § 34
indhenter nummeroplysninger fra teleoperatører. Denne samling af nummer-
oplysningsdata kaldes for Database Danmark, og oplysningerne fra databasen
anvendes til bl.a. udgivelse af telefonbøger i papirformat, cd-rom med titlen
Navn & Numre samt på internettet (tjenesten De Gule Sider). Nummeroplys-
ningerne på cd-rom blev beriget med oplysning om personens køn og oplys-
ning om, hvorvidt den pågældende bor i en etageejendom eller et etplanshus
m.v.

TDC Forlag solgte abonnemeter på Database Danmark (udtræk af hele data-
basen), således at en abonnent med jævne mellemrum kunne få opdateret
sine oplysninger ved hjælp af dette produkt. I den konkrete klagesag havde
Topdanmark gennem sit abonnement på Database Danmark fået oplysninger
om klager. Herudover kunne virksomheder abonnere på udtræk fra Database
Danmark. Udtrækkene kunne bestilles efter bestemte kriterier, f.eks. geogra-
fisk eller efter stillingsbetegnelse. TDC oplyste, at mange af udtrækkene til
virksomhederne måtte formodes at være til markedsføring.

Under sagen fremkom der endvidere oplysning om, at TDC Forlag udbød et
produkt med opdatering af kundedatabaser (datamining), således at der i
kundedatabaserne indgik de seneste oplysninger om kunderne. Behovet her-
for opstod, når oplysningerne var forældede.

Distributionen af nummeroplysningsdata blev ifølge det oplyste foretaget af
DM-huset, som ikke var en selvstændig juridisk enhed, men en afdeling in-
den for TDC Forlag.

Efter lov om konkurrence- og forbrugerforhold på telemarkedet § 34 skal udbydere af telenet eller teletjenester, der videretildeler abonnementsnumre til slutbrugere, afgive nummeroplysningsdata til alle, der ønsker det.

Ifølge § 34, stk. 2, forstås ved nummeroplysningsdata oplysninger om abonnementsnumre, der er tildelt slutbrugere, indeholdende navn, adresse, eventuelle oplysninger om stilling, abonnementsnummeret og den kategori af tjeneste, abonnementsnummeret anvendes til.

Endelig følger det af § 34, stk. 3, at en slutbruger kan kræve, at den pågældendes nummeroplysningsdata ikke oplyses i forbindelse med udbud af nummeroplysningstjenester. Krav herom indebærer ligeledes, at slutbrugers nummeroplysningsdata ikke må videregives til andre.

Sagen blev behandlet på et møde i Datarådet, hvorefter Datatilsynet udtalte, at TDC Forlag ikke kunne betragtes som teleoperatør, ligesom oplysningerne i Database Danmark omfattede mere, end hvad der efter § 34, stk. 2, skal forstås ved nummeroplysningsdata. TDC Forlags behandling af data skulle derfor efter Datatilsynets opfattelse vurderes efter de almindelige behandlingsregler i persondataloven.

Oplysninger i telefonbøger samt forskellige produkter baseret på Database Danmark er omfattet af persondatalovens § 6. Efter persondatalovens § 6, stk. 1, nr. 5, kan behandling af personoplysninger bl.a. ske, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse. Efter persondatalovens § 6, stk. 1, nr. 7, må registrering, videregivelse og anden behandling af personoplysninger endvidere ske, 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.

Efter Datatilsynets opfattelse kunne elektroniske såvel som manuelle telefonbøger udgives med hjemmel i § 6, stk. 1, nr. 5, og § 6, stk. 1, nr. 7, ligesom der efter § 6, stk. 1, nr. 7, kunne tegnes abonnemeter på oplysninger fra Database Danmark.

Uanset om en virksomhed fra en manuel eller elektronisk telefonbog kunne anvende de oplysninger, der er nævnt i lov om konkurrence- og forbrugerforhold på telemarkedet § 34, stk. 2, til markedsføringsformål, medførte dette efter Datatilsynets opfattelse som udgangspunkt ikke, at forholdet skulle betragtes som en videregivelse til markedsføringsformål. Modtagerens anvendelse af oplysningerne ville derimod skulle vurderes selvstændigt efter relevante bestemmelser i persondataloven eller andre love, herunder markedsføringsloven.

Datatilsynet måtte imidlertid konstatere, at TDC Forlag i elektroniske produkter berigede telefonbogsoplysningerne med forskellige oplysninger, f.eks. om de registrerede personers køn eller om bopælsforhold (etageejendom, et-planshus m.v.), der ikke pligtmæssigt skulle gives efter § 34, stk. 2, og som gjorde produktet yderligere anvendelig til markedsføring

På det foreliggende grundlag måtte det efter Datatilsynets opfattelse have formodningen for sig, at enhver videregivelse af oplysninger, der var berigede i forhold til de oplysninger, der var nævnt i § 34, stk. 2, måtte anses for omfattet af persondatalovens § 6, stk. 2-4, og § 36.

Efter Datatilsynets opfattelse gjorde tilsvarende forhold sig gældende med hensyn til TDC Forlags videregivelse af udtræk af oplysninger fra Database Danmark. Ved salg af sådanne udtræk måtte formodningen efter Datatilsynets opfattelse ligeledes være for, at der skete videregivelse til brug ved markedsføring, og at reglerne i persondatalovens § 6, stk. 2-4, og § 36 derfor skulle iagttages.

Datatilsynet tilkendegav dog, at der i begge situationer ville kunne videregives oplysninger efter de almindelige regler i lovens § 6, stk. 1, hvis TDC Forlag kunne afkræfte formodningen om, at videregivelse skete med henblik på markedsføring. Forlaget ville i sådanne tilfælde normalt kunne videregive oplysningerne i medfør af persondatalovens § 6, stk. 1, nr. 7.

Videregivelsen med henblik på markedsføring er omfattet af persondatalovens § 6, stk. 2-4, samt § 36.

Det følger af persondatalovens § 6, stk. 2-4, at en virksomhed ikke må videregive oplysninger om en forbruger til en anden virksomhed til brug ved markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, medmindre forbrugeren har givet sit samtykke hertil. Videregivelse og anvendelse kan dog ske uden samtykke, hvis der er tale om generelle kundeoplysninger.

I de tilfælde, hvor videregivelse eller anvendelse af generelle kundeoplysninger kan ske uden samtykke, skal reglerne i § 36 iagttages. Heraf følger, at hvis kunden ikke har fremsat indsigelse direkte over for virksomheden, skal virksomheden - hver gang den ønsker at videregive kundeoplysninger til andre virksomheder til brug for markedsføring eller anvende kundeoplysninger på vegne af en anden virksomhed - undersøge i CPR, om kunden har frabedt sig henvendelser i markedsføringsøjemed. Er dette tilfældet, må oplysningerne ikke videregives eller anvendes til dette formål. Hvis kunden ikke gennem en markering i CPR har frabedt sig henvendelser, skal virksomheden endvidere - inden oplysningerne videregives eller anvendes - give kunden tydelig og forståelig meddelelse om indsigelsesretten. Virksomheden skal i den forbin-

delse give kunden en nem adgang til inden for en frist på to uger at fremsætte indsigelse mod, at videregivelse eller anvendelse finder sted. Videregivelse eller anvendelse må ikke finde sted, før det er konstateret, at forbrugeren ikke har fremsat indsigelse inden udløbet af fristen på 2 uger.

Datatilsynet udtalte under sagen, at de omhandlede oplysninger måtte anses for generelle kundeoplysninger, jf. persondatalovens § 6, stk. 3, og oplysningerne måtte derfor som udgangspunkt kunne videregives uden samtykke.

Spørgsmålet var dog, om proceduren i § 36, stk. 2, skulle iagttages, når oplysningerne i forvejen var offentligt tilgængelige.

Datatilsynet henviste i den forbindelse til § 36, stk. 2, som ikke efter sin ordlyd skelner mellem offentligt tilgængelige oplysninger og oplysninger, som ikke er offentligt tilgængelige, ligesom bemærkningerne i lovforslag L 147 af 9. december 1999 til persondataloven ikke i forbindelse med indsigelsesproceduren i § 36 udtaler sig særskilt om oplysninger, som er offentligt tilgængelige.

Af bemærkningerne til § 36 i det tidligere lovforslag L 44 til persondataloven fremgår det derimod, at oplysningspligten ikke gælder i forhold til personer, som indgår i offentligt tilgængelige registre, der føres for offentlige myndigheder, selv om det eventuelt er muligt ud fra en given sammenhæng eller ved sammenstilling med oplysninger fra andre kilder at danne sig et billede af, hvilke potentielle interesser de registrerede måtte have. Hvad særligt angår adresserings- og kuverteringsbureauer finder bestemmelsen anvendelse i det omfang, personerne i bureauets registre er dets egne kunder (forbrugere), f.eks. kunder i forbindelse med bureauets eventuelle andre forretningsaktiviteter, og er optaget i registeret i denne egenskab. Bestemmelsen vil således ikke kunne omgås ved, at en virksomhed eller myndighed etablerer sig som adresserings- eller kuverteringsbureau.

Såvel en ordlydsfortolkning som ændringerne i bemærkningerne til § 36 i L 147 førte efter Datatilsynets opfattelse til, at § 36 må antages at finde anvendelse, uanset om oplysningerne i forvejen er offentligt tilgængelige.

For så vidt angik TDC Forlags opdatering af kundedatabaser udtalte Datatilsynet, at der ikke efter tilsynets opfattelse blev tilført nye oplysninger til modtagervirksomheden, men snarere en ajourføring af allerede eksisterende oplysninger i virksomheden.

På dette grundlag var det Datatilsynets opfattelse, at der ikke skete videregivelse med henblik på markedsføring. Datatilsynet lagde herved vægt på, at den dataansvarlige efter den grundlæggende regel i persondatalovens § 5, stk. 4, 1. pkt., har pligt til at sørge for den fornødne ajourføring af oplysninger, som behandles.

Datatilsynet anmodede TDC om at oplyse, hvad TDC Forlag agtede at foretage sig i anledning af tilsynets afgørelse.

TDC oplyste efterfølgende, at TDC Forlag var ophørt med videresalg af elektroniske telefonbogsdata indeholdende oplysninger ud over de data, der er nævnt i § 34 i lov om konkurrence- og forbrugerforhold på telemarkedet. Database Danmark, Navne & Numre m.v. blev herefter kun solgt indeholdende oplysninger svarende til § 34-data.

Det blev endvidere oplyst, at TDC Forlag var ophørt med at videresælge udtræk/dele af oplysninger fra Database Danmark med henblik på markedsføring. Dog fortsatte forlaget med salg af udtræk fra elektroniske telefonbogsdata, i det omfang de købende virksomheder forpligtede sig til ikke at anvende data til markedsføring.

Sortliste over virksomheder i træbranchen

Udtalt, at en miljøorganisations behandling af oplysninger om virksomheder på hjemmesiden www.tropetrae.dk ikke var omfattet af persondatalovens § 50, stk. 1, nr. 2, om advarselsregistre. Bl.a. inddraget hensynet til ytringsfriheden i vurderingen (Datatilsynets j.nr. 2001-2221-0019)

Dansk Træforening klagede på vegne af en medlemsvirksomhed til Datatilsynet over, at der på hjemmesiden www.tropetrae.dk var oprettet en sortliste i strid med persondatalovens regler for advarselsregistre.

Nepenthes er en miljøorganisation, der arbejder for bæredygtig brug af verdens skove. Målet for Nepenthes er, at alle tropiske træprodukter, som findes på det danske marked, kommer fra forsvarlig skovdrift, hvor der er taget såvel naturhensyn som hensyn til lokale og indfødte befolkningers behov.

På hjemmesiden www.tropetrae.dk havde Nepenthes bl.a. anført følgende: "Lad være med at købe havemøbler hos forhandlere, der ikke gør noget for at skaffe havemøbler, som er FSC-mærkede, og som altså ikke tager deres ansvar for at modvirke fældningen af verdens regnskove (se den sorte liste)", og "Danske virksomheder skal ikke kunne tjene penge på at sælge ryddet regnskov".

På hjemmesiden havde Nepenthes inddelt importører og forhandlere af havemøbler i tropisk træ i en hvid-, grå- og sortliste. På den sorte liste optrådte virksomheder, som havde mindre end 5 % havemøbler af tropisk træ, som var FSC-certificeret. Virksomheder, som ikke ønskede at fortælle Nepenthes om deres målsætninger eller om deres andel af FSC-træ, var også placeret her.

Efter at sagen havde været behandlet på et møde i Datarådet, udtalte Datatilsynet, at hensynet til ytringsfriheden skal tages i betragtning ved vurderingen af, om oplysninger omfattet af persondataloven må offentliggøres f.eks. på internettet. Der skal således foretages en konkret afvejning af på den ene side hensynet til beskyttelsen af privatlivet og på den anden side hensynet til informations- og ytringsfriheden med henblik på at sikre, at persondatalovens regler ikke unødigt medfører indskrænkninger i disse frihedsrettigheder. Efter bestemmelsen i persondatalovens § 2, stk. 2, finder loven ikke anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10.

Behandlingen på Nepenthes' hjemmeside www.tropetrae.dk ville som udgangspunkt være omfattet af persondatalovens § 50, stk. 1, nr. 2, hvis behandlingen skete med henblik på videregivelse, og videregivelsen skete med henblik på at advare mod forretningsforbindelse med de registrerede.

Datatilsynet konstaterede, at oplysningerne blev videregivet, idet de var tilgængelige for enhver på Nepenthes' hjemmeside.

Herefter foretog Datatilsynet en vurdering af, hvorvidt denne videregivelse skete med det primære formål at advare mod forretningsforbindelse med de registrerede virksomheder.

Det overordnede formål med hjemmesiden måtte efter Datatilsynets opfattelse antages at være at henlede opmærksomheden på FSC-mærkede træprodukter, herunder havemøbler. Endvidere var hjemmesiden tænkt som en forbrugerguide til det danske havemøbelmarked. Datatilsynet måtte endvidere forstå det af Nepenthes anførte således, at formålet var at tilkendegive organisationens synspunkter. Herudover var det et formål med hjemmesiden at lægge et vist pres på virksomhederne til at forhandle FSC-certificeret træ og at opfordre forbrugerne til at undlade at købe tropisk træ, som ikke var FSC-certificeret.

Datatilsynet fandt derfor at kunne lægge til grund, at det overordnede formål med hjemmesiden var forbrugerinformation - som led i Nepenthes' indsats for bæredygtig brug af verdens skove.

Efter Datatilsynets opfattelse burde der til opfyldelse af dette formål på hjemmesiden kunne offentliggøres oplysninger om, hvor FSC-certificeret træ kunne købes, uden at der er tale om et advarselsregister. Efter tilsynets opfattelse ville der endvidere kunne gives information om, hvilke procentdele af de nævnte virksomheders havemøbler af tropisk træ, der var FSC-certificeret, og virksomhederne ville kunne deles ind i grupper afhængigt af dette, uden at der forelå et advarselsregister.

Datatilsynet overvejede, om Nepenthes' offentliggørelse af oplysninger om en række virksomheder på en sortliste, fordi virksomhederne ikke besvarede organisationens spørgsmål eller medvirkede i organisationens undersøgelser medførte, at der forelå en behandling omfattet af persondatalovens § 50, stk. 1, nr. 2.

Selv om denne offentliggørelse ikke udelukkende kunne siges at tjene informationsformål, måtte den ses som et led i organisationens samlede kampagne. Hertil kom, at der efter Datatilsynets opfattelse må gives vide rammer for den politiske/ideologiske debat vedrørende emner af almen samfundsmæssig interesse. Hensynet til ytringsfriheden talte således med betydelig vægt imod at anse denne del af videregivelsen på hjemmesiden for et advarselsregister.

I sin endelige afgørelse fandt Datatilsynet således, at der ved afgørelsen om, hvorvidt Nepenthes' hjemmeside i sin aktuelle form var omfattet af persondatalovens § 50, stk. 1, nr. 2, måtte lægges afgørende vægt på, at hjemmesiden var etableret som led i Nepenthes' politiske arbejde for bevarelse og bæredygtig brug af verdens skove, at hjemmesidens overordnede formål - som led i dette arbejde - var at give forbrugerinformation og at henlede opmærksomheden på FSC-mærkede træprodukter, og at det af hjemmesiden klart fremgik, at virksomhedernes indplacering på forskellige lister udelukkende var begrundet i Nepenthes' ideologiske/politiske målsætninger på området.

På baggrund af en samlet konkret vurdering, hvori tillige hensynet til ytringsfriheden var indgået, fandt Datatilsynet således ikke, at der var tale om behandling omfattet af persondatalovens § 50, stk. 1, nr. 2, om advarselsregistre.

Som følge heraf blev et tidligere meddelte påbud til Nepenthes om at ophøre med at videregive oplysninger på den sorte liste ophævet.

Spørgsmål om frivillig registrering i et kreditoplysningsbureau

Frivillig registrering kunne ikke ske inden for rammerne af de gældende regler om kreditoplysningsbureauers virksomhed (Datatilsynets j.nr. 2001-2211-0087)

RKI Kredit Information A/S (RKI) anmodede Datatilsynet om at vurdere, om bureauet lovligt kunne registrere og videregive oplysninger om navn og adresse på personer, der ønskede at lade sig registrere frivilligt.

Baggrunden for RKI's forespørgsel var ifølge det oplyste, at bureauet modtog flere og flere henvendelser fra privatpersoner, som ønskede at lade sig registrere frivilligt i RKI. De personer, som ønskede frivillig registrering, var personer, der i perioder ikke var i stand til at overskue konsekvenserne af indkøb

eller låntagning, f.eks. skizofrene og ludomaner. Herudover havde også personer, der havde mistet legitimation, udtrykt ønske om frivillig registrering for at forhindre gældsstiftelse ved misbrug af legitimationen.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at frivillig registrering af skizofrene, ludomaner eller personer, der havde mistet legitimation, ikke kan betragtes som oplysninger, som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed. Datatilsynet henviste herved til, at en frivillig registrering ikke nødvendigvis er udtryk for manglende betalingsevne. Datatilsynet lagde endvidere vægt på, at formålet med de frivillige registreringer ikke var at advare bureauets abonnenter mod, at den registrerede var en "dårlig betaler", således som det normalt er tilfældet. Formålet med registreringen måtte derimod snarere antages at være hensynet til den pågældende selv, der på den måde søgte at opnå en form for sikkerhed mod yderligere gældsstiftelse.

Datatilsynet fandt således ikke, at der kunne ske frivillig registrering inden for rammerne af persondatalovens § 20, stk. 1.

Datatilsynet udtalte endvidere, at frivillig registrering efter omstændighederne kunne være i strid med det absolutte forbud mod behandling af oplysninger om rent private forhold i persondatalovens § 20, stk. 2. Datatilsynet lagde herved vægt på, at en del af de personer, der ønskede frivillig registrering, er ude af stand til at varetage deres økonomiske anliggender som følge af et svækket fysisk eller psykisk helbred. En frivillig registrering ville således kunne afsløre oplysninger om rent private forhold.

På denne baggrund fandt Datatilsynet ikke, at frivillig registrering kunne ske inden for rammerne af de gældende regler om kreditoplysningsbureauers virksomhed.

Udtalt, at finansieringsselskaber og pengeinstitutter kan få terminaladgang til det Centrale Motorkøretøjsregister (Datatilsynets j.nr. 2002-321-0168)

Rigspolicechefen anmodede Datatilsynet om en vejledende udtalelse om, hvorvidt der kunne gives terminaladgang til det Centrale Register for Motorkøretøjer til finansieringsselskaber og disses advokat og til pengeinstitutter.

Finansieringsselskaber og pengeinstitutter havde anmodet om terminaladgang for derved at opnå væsentlige lettelser i deres administration af bl.a. finansieringsaftaler med underpant i motorkøretøjer. Det fremgik af sagen, at Rigspolicechefen jævnligt videregiver oplysninger fra det Centrale Register for Motorkøretøjer enkeltvis til de pågældende virksomheder. Det fremgik tillige, at

Terminaladgang til Centralregisteret for Motorkøretøjer

Rigspolitichefen havde en række betænkeligheder ved at imødekomme ansøgningerne, dels fordi de nødvendige oplysninger kan indhentes fra andre kilder, som f.eks. fra køretøjets registrerede ejer/bruger eller fra Bilbogen, dels fordi terminaladgangen dermed ville ske til en række formål, der ligger uden for det område, til hvilket Rigspolitichefen efter sin hidtidige praksis havde givet terminaladgang.

Sagen blev behandlet på et møde i Datarådet. Datatilsynet udtalte herefter indledningsvis, at videregivelse af oplysninger fra det Centrale Register for Motorkøretøjer skal bedømmes efter persondatalovens §§ 5 og 6, idet registreret efter Datatilsynets opfattelse ikke indeholder oplysninger af fortrolig eller følsom karakter.

Videregivelsens lovlighed skal vurderes konkret ud fra interesseafvejningsreglen i lovens § 6, stk. 1, nr. 7, samt de grundlæggende principper i lovens § 5 om god databehandlingsskik, saglighed og proportionalitet. Det er i første omgang den dataansvarlige selv, der skal foretage denne vurdering.

Datatilsynet fandt, at den beskrevne videregivelse af oplysninger kunne ske inden for rammerne af persondatalovens § 6, stk. 1, nr. 7, samt at der kunne indrømmes finansieringsselskaber samt pengeinstitutter terminaladgang til det Centrale Register for Motorkøretøjer. Datatilsynet lagde i den forbindelse navnlig lagt vægt på karakteren af de oplysninger, som ville blive omfattet af terminaladgangen, herunder at disse i høj grad er sammenfaldende med oplysninger, som er offentligt tilgængelige via Bilbogen.

Særligt vedrørende etablering af terminaladgang for finansieringsselskabernes advokatforbindelse bemærkede Datatilsynet, at en eventuel terminaladgang kunne ske i det omfang, de virksomheder, som advokatfirmaet repræsenterer i inkassosagerne, selv ville kunne opnå terminaladgang. Datatilsynet henlede i den forbindelse særligt opmærksomheden på persondatalovens § 41, stk. 1, og stk. 3.

Endelig bemærkede Datatilsynet, at tilsynet ved vurderingen af, hvorvidt terminaladgang kunne ske inden for rammerne af persondatalovens § 6, stk. 1, nr. 7, havde forudsat, at der træffes de fornødne foranstaltninger for at sikre, at der kun etableres adgang til de oplysningstyper, som er nødvendige, for at virksomheden kan forfølge den berettigede interesse, som begrunder videregivelsen, at det sikres - f.eks. gennem det aftalemæssige grundlag mellem Rigspolitichefen og virksomhederne - at terminaladgangen kun benyttes til varetagelsen af de saglige formål, som ligger til grund for etableringen af terminaladgangen, samt at Rigspolitichefen gennem efterfølgende kontrol skaber sikkerhed for, at betingelserne for terminaladgangen overholdes.

Offentliggørelse af "live" optagelser fra en pub på internettet kan alene ske, hvis de involverede personer har givet deres udtrykkelige samtykke. Anbefalet, at de videobilleder, der bliver transmitteret, samtidig bliver vist på en skærm i baren (Datatilsynets j.nr. 2002-631-0086)

I forlængelse af en udsendelse i Nordjyllands Radio rettede Datatilsynet henvendelse til en pub i forbindelse med pubbens ønske om at sende "live" video fra pubben over internettet.

Det fremgik af sagen, at pubben fandt, at "live" video på en hjemmeside er en nyskabende måde at markedsføre pubben på. Pubben havde derfor forfulgt ideen og spurgt adskillige kunder og samtlige ansatte om, hvad de ville synes om at se "live" video fra pubben. Alle syntes, at det kunne være spændende og sjovt. Pubben havde i øvrigt i længere tid vist digitale billeder af besøgende på pubben på dens hjemmeside.

Det var virksomhedens opfattelse, at "live" udsendelser fra pubben over internettet ikke var i strid med persondataloven og derfor ikke krænkende for besøgende.

Der blev i den forbindelse henvist til, at der ville blive skiltet omhyggeligt - der ville således blive sat et skilt op ved indgangen til pubben, om at man i et vist udsnit af baren blev filmet til internettet, at det kun var 3 meter af baren, der blev filmet, (baren er 15 meter lang) dvs., at man sagtens kunne vælge at sætte sig i områder, hvor man ikke blev filmet, at det ikke var teknisk muligt at gemme billederne fra kameraet, og der derfor ikke ville være et register over, hvem der var blevet filmet, at billederne ville blive brugt som en mini tv-udsendelse fra pubben - det var stemningsbilleder, der viste livet på pubben, og at pubbens kunder frivilligt valgte at besøge pubben - og selv kunne vælge, om de ville sidde i den del af baren, der blev filmet.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at det var tilsynets opfattelse, at billeder af *ansatte* på pubben må siges at indeholde personoplysninger, idet de pågældende som ansatte på pubben ville være umiddelbart genkendelige.

Billederne af *de besøgende* ville efter Datatilsynets opfattelse også kunne indeholde personoplysninger. Datatilsynet lagde til grund, at de besøgende i en række tilfælde ville kunne genkendes af de personer, der ser video-billederne via pubbens hjemmeside.

Det var desuden Datatilsynets opfattelse, at den omhandlede aktivitet udgjorde en "behandling" af personoplysninger, jf. lovens § 3, nr. 2.

Datatilsynet fandt ikke at have tilstrækkeligt grundlag for at antage, at indsamling og videregivelse af oplysninger via et kamera med henblik på markedsføring af en pub på internettet ikke levede op til kravet om et sagligt formål, jf. lovens § 5, stk. 2.

Da oplysninger omfattet af lovens §§ 7 og 8 (følsomme oplysninger) kun ville indgå i ganske sjældne situationer, fandt Datatilsynet, at aktiviteten skulle vurderes efter lovens § 6 om ikke-følsomme oplysninger. Datatilsynet tillagde det betydning, at det beroede på tilfældigheder, om der optrådte oplysninger, som kunne karakteriseres som følsomme, og at det ikke var tilsigtet at behandle sådanne oplysninger.

Det var Datatilsynets opfattelse, at interesseafvejningen i § 6, stk. 1, nr. 7, ikke faldt ud til fordel for pubbens offentliggørelse af "live" optagelser på internettet. Tilsynet lagde vægt på, at flere gæster ville kunne føle det ubehageligt, at man på internettet kunne se, at den pågældende befandt sig på en pub eller lignende, og at denne interesse oversteg pubbens interesse i at kunne markedsføre sig ved hjælp af "live" optagelser. Dette gjaldt, uanset at det kun var et begrænset område, optagelserne foregik på.

Efter Datatilsynets opfattelse ville behandlingen således kun kunne ske i henhold til persondatalovens § 6, stk. 1, nr. 1, hvorefter behandling af oplysninger må finde sted, hvis den registrerede har givet sit udtrykkelige samtykke.

Efter Datatilsynets opfattelse indebar den omstændighed, at der var foretaget skiltning ved indgangen til pubben *ikke*, at de besøgende ved at gå ind på pubben kunne siges at have givet udtrykkeligt samtykke til offentliggørelsen af videobillederne på internettet.

Efter Datatilsynets opfattelse ville et holdbart bevis for, at der foreligger samtykke, forudsætte, at der anvendes en procedure, der indebærer en skriftlig tilkendegivelse fra de registrerede f.eks. i forbindelse med en ordning med medlemskab eller lignende. Datatilsynet anbefalede således, at pubben indførte rutiner, der sikrede klubben skriftligt bevis for, at der var samtykke fra alle, der ville få deres billede sendt ud over internettet.

Det var endvidere Datatilsynets opfattelse, at der ikke måtte ske lagring af optagelserne, idet dette næppe ville være i overensstemmelse med det angivne formål med optagelserne eller i overensstemmelse med god databehandlingskik

Tilsynet anbefalede i øvrigt, at de videobilleder, der blev sendt, samtidig blev vist på en skærm i baren.

Det var endvidere Datatilsynets opfattelse, at der ikke måtte ske manipulation af billederne, jf. lovens § 5, stk. 4.

For så vidt angik offentliggørelsen af billeder på internettet henvises der til sagen om offentliggørelse af situationsbilleder på internettet, som er omtalt ovenfor.

Udtalt, at tv-overvågning under visse betingelser er omfattet af persondataloven. Vurderet overvågningen i forhold til lovens bestemmelser, herunder § 5 om sagligt formål og sletning, bestemmelserne i §§ 6-8 om hjemmel til behandlingen samt §§ 28-29 om information til de berørte (Datatilsynets j.nr. 2001-211-0027)

Tv-overvågning i supermarkedskæde

På baggrund af en henvendelse fra en fagforening rettede Datatilsynet henvendelse til en kæde af supermarkeder med spørgsmål om supermarkedernes tv-overvågning. Fagforeningen ønskede særligt Datatilsynets stillingtagen til, om den skiltning, der blev foretaget i butikkerne, levede op til kravene i persondatalovens § 28.

Supermarkedskæden oplyste, at der kun blev foretaget tv-overvågning på steder, hvor der var skiltet med det. Tv-overvågningen skete på offentligt tilgængelige steder som kundeservice, flaskemodtagelse, varemodtagelser, vareudlevering og i det hele taget i butikernes åbningstider, hvor både kunder og ansatte kan blive optaget. Tv-overvågningen skete også på andre lokaliteter, hvor personer ofte færdes eller arbejder, f.eks. på lagre og i butikken uden for arbejdstiden, hvor både ansatte i kæden samt ansatte i andre firmaer (f.eks. ansatte i rengøringsselskaber, pengetransportfirmaer, håndværkerfirmaer, vagtfirmaer og hos leverandører) kan blive optaget.

Formålet med tv-overvågningen og optagelserne var bl.a. at forebygge og opklare røverier, misbrug af dankort og andre uregelmæssigheder. Det var kun betroede medarbejdere fra butikkens ledelse og en medarbejder fra Intern Revision, der havde adgang til optagelserne. Konstaterede en medarbejder fra Intern Revision uregelmæssigheder, ville der blive afholdt et møde med tillidsrepræsentanten eller en betroet medarbejder og den ansatte. Optagelserne blev videregivet sammen med en anmeldelse til politiet. Øvrige optagelser blev slettet løbende, idet der blev kørt nye optagelser over de gamle.

Det blev i øvrigt oplyst, at cirka 30 procent af de nuværende kameraer var digitale, mens de øvrige kameraer var analoge. Fremover ville der dog kun blive indkøbt digitale kameraer.

Efter sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at digital tv-overvågning som udgangspunkt er omfattet af persondataloven, da der sker elektronisk behandling af oplysningerne.

Datatilsynet lagde til grund, at kædens tv-overvågning var forbundet med optagelse, og at optagelserne blev opbevaret systematisk. Persondataloven fandt således anvendelse, uanset om der var tale om digital eller analog behandling, jf. lovens § 1, stk. 1 og stk. 2.

For at en behandling kan være omfattet af persondataloven, er det også en betingelse, at behandlingen omfatter "personoplysninger". Det var Datatilsynets opfattelse, at billeder af *ansatte* må betragtes som personoplysninger, idet de pågældende, som er ansat i butikken, vil være umiddelbart genkendelige.

Billeder af *kunder og andre uvedkommende personer* ville efter Datatilsynets opfattelse også kunne indeholde personoplysninger. I lyset af den teknologiske udvikling, f.eks. elektronisk ansigtsgenkendelse, var der således efter tilsynets opfattelse meget, der talte for, at personbilleder efter omstændighederne i sig selv må betragtes som personoplysninger og dermed omfattet af loven.

Det var på dette grundlag Datatilsynets opfattelse, at tv-overvågningen omfattede personoplysninger om såvel ansatte som kunder. Datatilsynet tillagde det herved endvidere betydning, at tv-overvågningen skulle afdække persons handlinger i forhold til uregelmæssigheder, at der ville ske forevisning af optagelser for betroede medarbejdere fra butikkens ledelse og en medarbejder fra Intern Revision, samt at der eventuelt ville ske videregivelse af optagelser til politiet.

Datatilsynet fandt i øvrigt, at digital tv-overvågning selv *uden* optagelse udgør en behandling i persondatalovens forstand. Endvidere blev det understreget, at opbevaring af båndene ligeledes var en behandling i lovens forstand.

Ifølge persondatalovens § 5, stk. 2, 1. pkt., skal indsamling af oplysninger ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål.

Datatilsynet fandt, at den indsamling af oplysninger via tv-overvågning, som blev foretaget med henblik på at forebygge og opklare røverier, misbrug af dankort og andre uregelmæssigheder, havde et udtrykkeligt angivet og sagligt formål. Dette gjaldt overvågning af såvel kunder og andre uvedkommende som de ansatte.

Det følger af persondatalovens § 5, stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Datatilsynet fandt, at der som følge af § 5, stk. 5, skulle ske løbende sletning af optagelserne, og disse kun måtte opbevares i en vis kortere periode, som ikke burde overstige 30 dage.

For så vidt angik hjemmel til behandling fandt Datatilsynet, at da oplysninger omfattende af lovens §§ 7 og 8 (følsomme oplysninger) kun i ganske sjældne situationer ville indgå, skulle aktiviteten vurderes efter lovens § 6 om ikke-følsomme oplysninger. Datatilsynet tillagde det betydning, at det beroede på tilfældigheder, om der optrådte oplysninger, som kunne karakteriseres som følsomme, og at det ikke var tilsigtet at behandle sådanne oplysninger.

I tilfælde, hvor tv-overvågningen afslørede kriminelle aktiviteter, ville der dog blive behandlet oplysninger omfattende af lovens § 8 - se nedenfor.

Efter Datatilsynets opfattelse var der hjemmel i lovens § 6 stk. 1, nr. 7, til såvel den behandling, som var forbundet med selve tv-overvågningen, som den efterfølgende optagelse og opbevaring heraf. Datatilsynet lagde vægt på, at supermarkeds kæden havde en berettiget interesse i at forsøge at forhindre kriminalitet (tv-overvågningens præventive effekt) samt i at kunne opklare kriminalitet ved hjælp af optagelser af sådanne hændelser.

Afslører tv-overvågningen kriminelle aktiviteter, indebar det efter Datatilsynets opfattelse, at der behandles oplysninger omfattende af persondatalovens § 8. Det primære formål bag tv-overvågningen var endvidere at afsløre kriminelle handlinger.

Efter § 8, stk. 4, må private foretage behandling af bl.a. strafbare oplysninger, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede. Ifølge bemærkningerne til § 8, stk. 4, giver bestemmelsen - i overensstemmelse med Register-tilsynets praksis - mulighed for, at en virksomhed kan registrere oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse, f.eks. om butikstyveri, og eventuel senere afgivelse af vidneforklaring i retten. Oplysningerne skal dog destrueres snarest muligt, jf. § 5, stk. 5.

Efter § 8, stk. 6, jf. § 7, stk. 2, nr. 4, må behandling desuden ske, hvis behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Efter Datatilsynets opfattelse kunne behandlingen i de omhandlede tilfælde ske i henhold til persondatalovens § 8, stk. 4, samt § 8, stk. 6, jf. § 7, stk. 2, nr. 4. Datatilsynet lagde bl.a. vægt på, at kæden i forbindelse med et tyveri eller røveri kan have et erstatningskrav mod den registrerede.

Det var Datatilsynets opfattelse, at persondatalovens regler om oplysningspligt fandt anvendelse parallelt med skiltningsskrevet i lov om forbud mod tv-overvågning, når det gjaldt tv-overvågning af butiklokaler m.v., i det omfang tv-overvågningen var digital.

Datatilsynet vurderede spørgsmålet efter persondatalovens § 29 om oplysningspligt, hvor oplysninger ikke er indsamlet hos den registrerede. Tilsynet fandt med andre ord ikke, at oplysningerne fra tv-overvågningen kunne siges at være indsamlet hos den registrerede som nævnt i lovens § 28.

For så vidt angik tv-overvågningen af *kunder og lignende personer* var det tilsynets opfattelse, at kunderne allerede via skiltningen efter lov om forbud mod tv-overvågning var blevet informeret om, at der finder tv-overvågning sted. Det var Datatilsynets opfattelse, at yderligere underretning af de registrerede må kunne siges at være uforholdsmæssig vanskelig, jf. § 29, stk. 3. Tilsynet lagde vægt på, at det vil være praktisk umuligt og i hvert fald yderst ressourcekrævende at give hver enkelt kunde selv en standardmeddelelse indeholdende de påkrævede oplysninger efter § 29, stk. 1. Hertil kom, at en uddybende tekst indeholdende disse oplysninger i sammenhæng med skiltningen ikke nødvendigvis ville blive bemærket og læst af kunderne.

Modsat fandt tilsynet, at underretning af de *ansatte* i butikken ikke kunne siges at være uforholdsmæssig vanskelig efter § 29, stk. 3. Tilsynet lagde vægt på, at det ville være relativt enkelt at give hver enkelt ansat underretning om de i § 29, stk. 1, nævnte oplysninger. Dette gjaldt efter Datatilsynets opfattelse alle de personer, der fast udførte arbejde i lokalerne, uanset om ansættelseskontrakten var indgået med supermarkeds-kæden eller en anden virksomhed, f.eks. et rengøringsfirma. Kæden vil eventuelt kunne lade den virksomhed, som de pågældende er ansat i, give informationen, men det er supermarkeds-kædens ansvar, at den blev givet.

Datatilsynet fandt, at de ansatte og andre personer, der udførte arbejde i lokalerne, skulle have meddelelse om bl.a. *formålene* med den behandling, hvortil oplysningerne var bestemt, jf. § 29, stk. 1, nr. 2. I kravet om formålsangivelse ligger, at der skal gives den registrerede tilstrækkelig information til, at den pågældende bliver klar over, hvad der er baggrunden for, at der indsamles oplysninger om den pågældende. Hvis en del af formålet med tv-overvågning var at forebygge og opklare også *de ansattes* eventuelle kriminalitet mv., fandt Datatilsynet, at dette i så fald skulle fremgå af informationen.

Der vil endvidere skulle gives meddelelse om alle *yderligere oplysninger*, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser.

Det var Datatilsynets opfattelse, at det i forlængelse af angivelsen af overvågningens formål ville være naturligt, at meddelelsen indeholdt oplysning om, at optagelserne ville kunne blive videregivet til politiet, samt om i hvilke tilfælde dette ville kunne ske. Det var desuden tilsynets opfattelse, at der burde gives information om, i hvilke tilfælde optagelserne ville blive gennemgået af ledelsen og Intern Revision, f.eks. om dette fandt sted i form af stikprøvekontrol eller i forbindelse med mistanke om kriminelle aktiviteter eller lignende.

Det var endvidere tilsynets opfattelse, at der burde gives de ansatte meddelelse om, hvor længe oplysningerne blev opbevaret.

Tilsynet fandt endvidere, at oplysningspligten i § 29 måtte medføre, at de ansatte blev informeret om, i hvilke lokaler overvågningen foregik, mens der efter Datatilsynets opfattelse næppe kunne stilles krav om, at der blev givet information om, *hvornår* der skete tv-overvågning, hvis dette kun fandt sted i tilfælde af problemer i de enkelte butikker.

Supermarkedskæden har over for Datatilsynet oplyst, at man nu har indrettet sin tv-overvågning i overensstemmelse med tilsynets retningslinier.

Fagforeningen vendte på baggrund af Datatilsynets brev tilbage med en række supplerende spørgsmål. Fagforeningen ønskede således oplyst, om et skilt med ordlyden "Der foretages regelmæssig eller vedvarende tv- eller videoovervågning i butikken" var i strid med persondataloven sammenholdt med lov om forbud mod tv-overvågning.

Datatilsynet oplyste, at der næppe kan stilles krav om, at der gives information om, hvornår der sker tv-overvågning, hvis dette kun finder sted i tilfælde af problemer i de enkelte butikker. Datatilsynet vurderede således, at et sådant krav næppe kan indfortolkes i lovens § 29. Spørgsmålet havde efter tilsynet opfattelse også snarere karakter af at være arbejdsretligt fremfor databeskyttelsesretligt. Endvidere faldt det uden for Datatilsynets kompetence at udtale sig om lov om forbud mod tv-overvågning.

Det var endvidere fagforeningens opfattelse, at der ved tv-overvågning er tale om særlige omstændigheder, som begrunder en præcis information til de ansatte om, hvor kameraerne er sat op. Datatilsynet oplyste, at det ikke kan udledes af bestemmelsen i lovens § 29, at medarbejderne skal have oplysning om præcis, hvor de pågældende kameraer befinder sig i lokalet eller antallet af kameraer.

Efter fagforeningens opfattelse burde salgsassistenter, som kunne være kollegaer til den overvågede, ikke have adgang til båndene. Datatilsynet fandt ikke, at tilsynet kunne udtale sig om, hvilke stillingskategorier, der ville kunne få adgang til de pågældende oplysninger.

Videregivelse af oplysninger fra forskningsregistre

Fundet, at persondatalovens § 10, stk. 2, ikke kan suppleres med lovens samtykkeregler, idet bestemmelsen må antages udtømmende at have gjort op med mulighederne for videregivelse (Datatilsynets j.nr. 2002-216-0096)

Den Sociale Højskole i Århus havde rettet henvendelse til Datatilsynet vedrørende en registreret persons mulighed for efter persondataloven at give samtykke til, at oplysninger om den pågældende, der er indsamlet og behandlet til videnskabelige formål (projektoplysninger), gøres tilgængelige for en bredere kreds af personer. Skolen ønskede dispensation fra Datatilsynets standardvilkår, således at de studerendes rapporter kan offentliggøres og udlånes på skolens bibliotek.

Af det omhandlede standardvilkår følger, at en eventuel offentliggørelse af undersøgelsens resultater ikke må ske på en sådan måde, at det er muligt at identificere enkeltpersoner.

Det følger af persondatalovens § 10, stk. 1, at følsomme oplysninger som nævnt i § 7, stk. 1, og § 8 må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelsen.

Det følger af § 10, stk. 2, at der ikke senere må ske behandling af oplysninger, som er omfattet af stk. 1 til andre formål. Af bemærkningerne til denne bestemmelse fremgår bl.a., at der alene vil kunne ske efterfølgende behandling, herunder videregivelse, til private forskere eller offentlige myndigheder i det omfang, behandlingen sker med henblik på udførelsen af andre statistiske eller videnskabelige undersøgelser.

Endelig fremgår det af § 10, stk. 3, at der kun kan videregives oplysninger til tredjemand efter forudgående tilladelse fra tilsynsmyndigheden. Tilsynsmyndigheden kan stille nærmere vilkår.

Datatilsynet fandt, at persondatalovens § 10, stk. 2, ikke kan suppleres med samtykkereglerne i persondataloven, idet bestemmelsen må antages udtømmende at have gjort op med mulighederne for videregivelse.

Det var endvidere Datatilsynets vurdering, at en person i nogle tilfælde måske ville føle sig presset til at give samtykke til offentliggørelse, og det derfor var tvivlsomt, om der i realiteten ville være tale om et frivilligt samtykke. Da der kan være tale om følsomme oplysninger, vejer hensynet til de registrerede personer efter Datatilsynets opfattelse tungere end hensynet til de projektansvarliges interesse i at kunne offentliggøre deres rapporter i personhenførlig form.

Datatilsynet arbejder fortsat på - evt. i samarbejde med den Sociale Højskole - at finde en løsning, der muliggør udlån til andre elever på skolen. Dette vil dog forudsætte, at den efterfølgende behandling ligeledes alene sker til videnskabelige formål, og der skal indhentes forudgående tilladelse fra Datatilsynet til videregivelsen (udlånet) til andre elever. Hvis en sådan ordning etableres, vil den studerende, der låner en rapport, imidlertid være selvstændig ansvarlig i henhold til persondataloven for deres anvendelse og opbevaring af rapporten.

Udtalt, at det kræver samtykke at videregive oplysninger om en persons indkomst til andre husstandsmedlemmer i forbindelse med en ansøgning om boligstøtte, jf. § 6, stk. 1, nr. 1. Endvidere udtalt tvivl i forhold til etablering af en særhjemmel til fravigelse af dette krav. Endelig udtalt, at en ansøgers husstandsmedlem ikke kan antages at være bekendt med, at en sag om boligstøtte påbegyndes, hvorfor oplysningspligten ikke bør fraviges (Datatilsynets j.nr. 2002-321-0174)

Videregivelse i forbindelse med ansøgninger om boligstøtte

Socialministeriet anmodede om Datatilsynets vurdering i forbindelse med ministeriets planer om at gennemføre en digitalisering af den kommunale boligstøtteadministration.

Den digitale ordning skulle bygges op således, at en ansøger ville få oplysninger om alle husstandsmedlemmers indkomstforhold i forbindelse med indgivelse af en ansøgning, og at ansøgeren herefter skulle validere disse oplysninger. Den nuværende ordning fungerer således, at en ansøger selv skal tilvejebringe de oplysninger, der skal bruges i forbindelse med en ansøgningssag, og alle husstandsmedlemmer skal i den forbindelse underskrive ansøgningen.

Ministeriet ønskede en række spørgsmål afklaret; herunder om en videregivelse af oplysninger om husstandsmedlemmers økonomiske forhold til ansøgeren var muligt uden samtykke fra husstandsmedlemmet og hvis ikke, om man eventuelt kunne etablere en lovhjemmel, således at der ikke skulle indhentes samtykke. Datatilsynet blev tillige bedt om at vurdere, hvorvidt et husstandsmedlem kan antages at være bekendt med, at der rejses en ansøgningssag, således at oplysningspligten bortfalder.

Sagen blev behandlet i Datarådet, og Datatilsynets udtalelse havde følgende hovedindhold:

Økonomiske oplysninger er såkaldte almindelige ikke-følsomme oplysninger, som skal behandles i overensstemmelse med § 6 i persondataloven.

Behandling kan efter reglerne i § 6, stk. 1, bl.a. ske, hvis den registrerede har givet udtrykkeligt samtykke hertil, jf. § 6, stk. 1, nr. 1. Herudover kan oplysninger behandles i medfør af § 6, stk. 1, nr. 3, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, eller efter § 6, stk. 1, nr. 6, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave, som henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt. Endelig kan oplysninger behandles efter § 6, stk. 1, nr. 7, 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.

Ved vurderingen af den ønskede videregivelse lagde Datatilsynet til grund, at oplysningerne skulle videregives automatisk til ansøgeren i forbindelse med en ansøgningssags start, idet boligstøttesystemet - når ansøgeren logger på systemet - indhenter de relevante oplysninger fra forskellige offentlige registre og gør dem direkte tilgængelige for ansøgeren. Ansøgeren godkender derefter oplysningerne og sender dem til kommunen.

Da oplysningerne ved den digitale løsning efter planen skulle udleveres ved sagens start, forelå der efter Datatilsynets opfattelse ikke en situation, hvor en myndighed skulle begrunde en afgørelse i forbindelse med et afslag. Videregivelsen ved sagens start var dermed ikke nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, jf. § 6, stk. 1, nr. 3.

Socialministeriet havde over for Datatilsynet anført en række hensyn, der talte for en videregivelse af oplysningerne, herunder tæt økonomisk forhold mellem ægtefæller/samlevende, den forvaltningsretlige begrundelsespligt ved afslag samt den positive betydning, som boligstøtte har for en husstand.

Hertil kom myndighedernes interesse i at digitalisere boligstøttesagerne. Et krav om indhentelse af samtykke til videregivelse ville komplicere den digitale ansøgning, idet en procedure, der kan kræve flere digitale underskrifter, efter det af ministeriet oplyste i dag dårligt lader sig gennemføre i teknisk henseende.

Datatilsynet var enig i, at tildeling af boligstøtte kan have en positiv betydning for hele husstanden. Efter Datatilsynets opfattelse kunne dette hensyn imidlertid ikke begrunde den ønskede videregivelse i alle situationer, hvor

ansøgningen sker digitalt. Datatilsynet lagde i den forbindelse bl.a. vægt på misbrugsmulighederne ved ordningen.

En selvbetjeningsløsning med adgang til oplysninger om andre personer ville således efter Datatilsynets opfattelse indebære en risiko for, at en ansøger handler i strid med andre husstandsmedlemmers interesser - enten ved at søge om boligstøtte og derved gøre sig bekendt med indkomstoplysninger mod deres vilje eller ved at søge og modtage boligstøtte uden den øvrige husstands vidende.

Heller ikke det anførte om den økonomiske afhængighed mellem ægtefæller/samlevende kunne begrunde en generel videregivelsesadgang. Der kunne således efter Datatilsynets opfattelse være situationer, hvor der ikke er tætte økonomiske bånd mellem ægtefæller/samlevende. Der er således hensyn at tage til ægtefællen/samleveren.

Socialministeriet havde påpeget, at oplysninger ville kunne videregives til ansøgeren uden samtykke fra husstandens medlemmer i forbindelse med en begrundelse for afslag. Denne videregivelse skulle efter tilsynets opfattelse som ovenfor anført behandles separat fra den videregivelse, som Socialministeriet ønskede gennemført. Begrundelsen i forbindelse med et afslag gives, når en sag er færdigbehandlet. På det tidspunkt må kommunen antages at have opfyldt persondatalovens oplysningspligt (jf. nedenfor) i forhold til ægtefællen/samleveren, således at denne er bekendt med sagen og har haft mulighed for at gøre indsigelse, hvis vedkommende af særlige grunde ikke ønsker, at de økonomiske oplysninger videregives.

For så vidt angår myndighedens interesse i at digitalisere boligstøttesagerne på en enkel måde bemærkede Datatilsynet, at tilsynet selvfølgelig anerkendte denne interesse. Tilsynet måtte imidlertid afveje denne i forhold til persondatalovens krav - herunder nødvendighedskravet - i forhold til de hensyn til registrerede personer, som talte imod. Ved vurderingen af disse interesser tillagde Datatilsynet tillige oplysningernes karakter betydning. Oplysninger om en persons indtægtsforhold må anses for at være af fortrolig karakter og vil således normalt ikke kunne udleveres til private.

Det var endvidere Datatilsynets opfattelse, at den omstændighed, at en løsning er teknisk vanskelig eller kræver udvikling af nye teknikker, ikke i sig selv medførte, at betingelserne for behandling af oplysninger var opfyldt.

Det var på denne baggrund Datatilsynets opfattelse, at der ikke kunne ske videregivelse til ansøgeren efter § 6, stk. 1, nr. 6 eller 7, idet en sådan videregivelse ikke kunne anses for nødvendig, og idet den registreredes interesse i, at der ikke sker videregivelse, vejede tungere end ansøgerens interesse i at modtage oplysningerne.

Datatilsynet fandt således, at der skulle foreligge samtykke fra husstandsmedlemmerne, herunder ægtefællen/samleveren, inden oplysningerne om indkomst kunne videregives til ansøgeren, jf. persondatalovens § 6, stk. 1, nr. 1.

En hjemmelsbestemmelse ville give adgang til, at oplysninger om en ægtefælle/samlevers økonomiske forhold kunne videregives til ansøgeren uden samtykke fra den, som oplysningerne vedrører. Videregivelsen er muligvis nødvendig for digitaliseringen af administrationen, men ikke som sådan for behandlingen af ansøgningen om boligstøtte.

Etableringen af en hjemmel til at videregive oplysningerne uden samtykke fra husstandsmedlemmerne skulle ske i overensstemmelse med EU's databeskyttelsesdirektiv. Efter Datatilsynets opfattelse kunne det give anledning til tvivl, om en sådan fravigelse ville være forenelig med direktivet.

Spørgsmålet var i den forbindelse, om det kunne anses for nødvendigt, at der - uden samtykke - ville ske videregivelse af oplysningerne til ansøgeren i forbindelse med en sag om boligstøtte. Nødvendighedskravet indgår både i artikel 7, c) og e).

Derudover skulle der tages hensyn til direktivets artikel 6, efter hvilken oplysningerne skal behandles rimeligt og lovligt. Behandling skal ske til saglige formål samt være relevant og tilstrækkelig og ikke omfatte mere, end hvad der kræves til opfyldelse af formålet.

Det var som udgangspunkt Datatilsynets opfattelse, at alene hensynet til en hurtig gennemførelse af en digitalisering ikke burde medføre fravigelse af den beskyttelse, som registrerede personer nyder efter persondataloven. Ideelt set burde der efter Datatilsynets opfattelse i stedet arbejdes for at etablere en selvbetjeningsordning, hvor husstandsmedlemmer deltager i tilvejebringelsen af oplysninger i elektronisk form, eventuelt således at disse får mulighed for at give et digitalt samtykke.

Datatilsynet fandt derfor ikke umiddelbart at kunne anbefale, at der indførtes hjemmel i særlovgivningen, der på dette punkt fraveg persondataloven, men den endelige afgørelse vedrørende dette spørgsmål måtte bero på en vurdering af, hvor vægtige samfundsmæssige interesser der knytter sig til digitaliseringen af administrationen på dette område. Datatilsynet fandt ikke at burde udtale sig nærmere herom.

Socialministeriet bad Datatilsynet om at oplyse, i hvilke tilfælde der ville være oplysningspligt i forhold til et husstandsmedlem, når oplysningerne var indhentet uden samtykke, herunder om husstandsmedlemmet kan antages at være bekendt med indhentning og videregivelse, når der er tale om videregivelse til en ægtefælle/samlever.

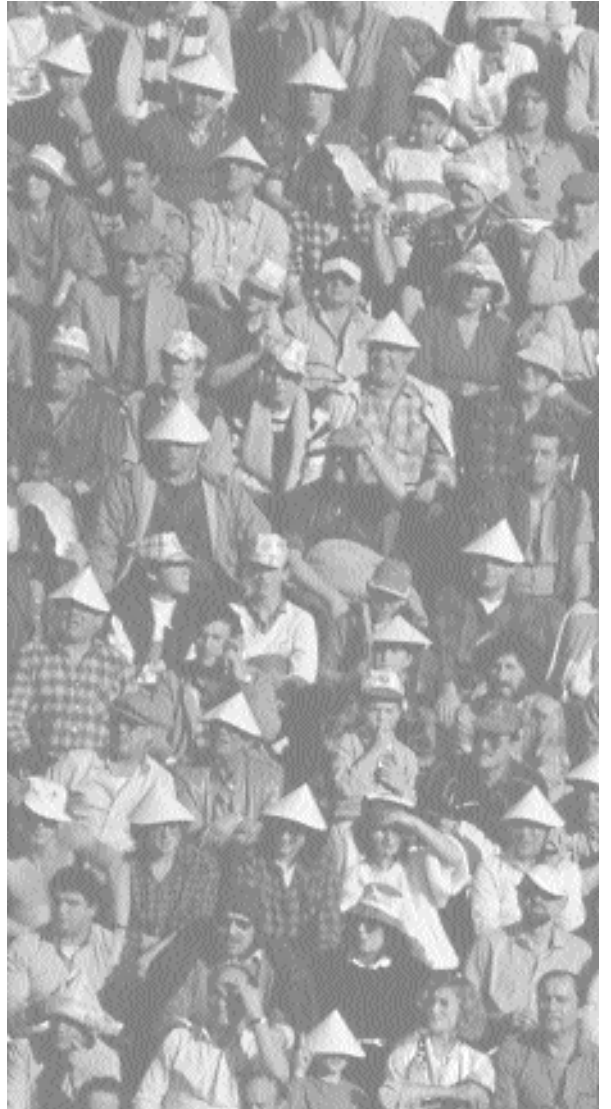
Det følger af § 29, stk. 2, at oplysningspligten ikke gælder, hvis den registrerede allerede er bekendt med oplysningerne opregnet i § 29, stk. 1, eller hvis registreringen eller videregivelsen er udtrykkeligt fastsat ved lov eller bestemmelser fastsat i henhold til lov.

Selv om der eksisterer en retsregel, der udtrykkeligt beskriver, hvilke oplysninger og hvilke behandlinger, herunder videregivelse, der sker i forbindelse med en sag om boligstøtte, vil det pågældende husstandsmedlem efter Datatilsynets opfattelse fortsat kunne være uvidende om eksistensen af en boligstøttesag.

Oplysninger, som afgives af en ansøger, behøver ikke nødvendigvis at være indsamlet hos husstandsmedlemmet selv, men kan være fremskaffet på anden vis - f.eks. ved at læse en selvangivelse eller lønseddel - uden at orientere det pågældende husstandsmedlem herom.

På dette grundlag og under hensyntagen til § 29's karakter af beskyttelsesregel var der efter Datatilsynets opfattelse ikke grundlag for at antage, at et husstandsmedlem generelt var bekendt med myndighedens indhentning/modtagelse af oplysninger fra LetLønsregistret eller fra den pågældende ægtefælle eller samlever.

Datatilsynet bemærkede afsluttende, at oplysningspligten efter Datatilsynets opfattelse ikke ville være et problem, hvis de personer, der indsamles/modtages oplysninger om, konkret er involverede i tilvejebringelsen af oplysningerne.



Internationalt arbejde

<i>Indledning</i>	<i>76</i>
<i>Europarådet</i>	<i>77</i>
<i>Den Europæiske Union</i>	<i>78</i>
<i>International konference for Datatilsynsmyndigheder</i>	<i>87</i>
<i>Nordisk samarbejde</i>	<i>88</i>

Internationalt arbejde

Indledning

Datatilsynet har siden 1. juli 2000 fortsat Registertilsynets opgaver på det internationale område og har - afledt af reglerne i persondataloven - fået visse udvidede beføjelser, som vedrører samarbejdet med tilsynene i de øvrige EU-medlemsstater, jf. lovens § 64.

Som nærmere beskrevet i tidligere årsberetninger, senest Datatilsynets Årsberetning for 2001, har der siden 1979 - men især fra 1989 - udviklet sig et omfattende regelsæt på databeskyttelsesområdet, som har fået stadig større betydning for Datatilsynets arbejde. På Datatilsynets hjemmeside er de regelsæt, som nærmere vil blive omtalt, tilgængelige via link under Internationalt.

Den væsentligste ældre konvention på området er Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, som trådte i kraft i 1985.

Forud herfor var i september 1980 fremkommet OECDs internationalt dækkende Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, som indeholder en række hovedprincipper for persondatabeskyttelse, og som har størst betydning for de lande, der ikke har ratificeret Europarådskonventionen.

Særligt afgørende har dog været udviklingen inden for EU med vedtagelse af direktiver gældende for det indre marked (søjle I-området), bl.a. det generelle databeskyttelsesdirektiv, men også - afledt af det stigende europæiske samarbejde mellem kontrollerende myndigheder i de enkelte EU-medlemsstater (politi, toldvæsen og asylmyndigheder) - vedtagelse af en række konventioner, som efterhånden er blevet inddraget under EU, og som er omfattet af Amsterdam-traktatens afsnit VI om politisamarbejde og retligt samarbejde i kriminalsager (søjle III-området). Disse konventioner indeholder specifikke regler om persondatabeskyttelse og om tilsyn med overholdelse af disse regler.

Både FNs Menneskerettighedskonvention og Den Europæiske Menneskerettighedskonvention indeholder bestemmelser, der omhandler respekten for privatlivets fred.

Af generel betydning er det også, at artikel 8 i EU-Charteret om grundlæggende rettigheder - underskrevet i december 2000 - indeholder en bestemmelse, som særligt vedrører persondatabeskyttelse. Også heri er retten til databeskyttelse anerkendt som en grundlæggende menneskeret.

Artikel 8 har følgende ordlyd (EF-tidende 18.12.2000 C 364/01):

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende.
2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører ham/hende, og til berigtigelse heraf.
3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.

En engelsk oversættelse af lov om behandling af personoplysninger er tilgængelig på Datatilsynets hjemmeside www.datatilsynet.dk.

Nedenfor gives en kort beskrivelse af det formelle grundlag for tilsynets aktiviteter på det internationale område suppleret med oplysninger om de væsentligste sager, som tilsynet har beskæftiget sig med i 2002. Desuden omtales også det mere uformelle, internationale samarbejde, som har udviklet sig gennem årene.

Konventionens navn: Den europæiske konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (COE 108).

Ikrafttræden: Den 1. februar 1990 i Danmark.

Den rådgivende Komité (Consultative Committee T-PD), som er nedsat i henhold til konventionens artikel 18, har i 2002 bl.a. beskæftiget sig med spørgsmålet om overførsel af oplysninger til tredjelande og en analyse af konventionsteksten i lyset af de seneste tendenser på databeskyttelsesområdet.

Den rådgivende Komité vedtog i 2000 et forslag til tillægsprotokoltekst til konventionen, som vedrører oprettelse af databeskyttelsesmyndigheder og forholdet til tredjelande. Tillægsprotokollen blev i 2001 vedtaget af Ministerkomiteen og efterfølgende fremlagt til underskrivelse. I slutningen af 2002 har 21 lande underskrevet tillægsprotokollen.

Ministerkomiteen har i øvrigt den 15. juni 1999 på grundlag af T-PDs forberedelse vedtaget en ændring af konventionen, som gør det muligt for De europæiske Fællesskaber at tiltræde konventionen. Ændringen træder først i kraft,

Europarådet

når alle parter til COE 108 har accepteret ændringen. Alle medlemslandene har endnu ikke accepteret, og De Europæiske Fællesskaber har derfor endnu ikke tiltrådt konventionen.

Databeskyttelsesekspertgruppen (CJ-PD) har i 2002 færdigbehandlet retningslinier for anvendelsen af videoovervågning. Dette er sket på baggrund af en ekspertrapport, der er blevet offentliggjort på Europarådets hjemmeside indeholdende et forslag til "Guiding Principles for the protection of individuals with regard to the collection and processing of personal data by means of video surveillance."

CJ-PD har i 2002 bl.a. også arbejdet med den tredje evaluering af rekommandation nr. R (87) 15 regulating the use of personal data in the police sector.

CJ-PD bliver ofte anmodet om at være andre ekspertgrupper i Europarådet behjælpelig med at vurdere, hvorledes reglerne om persondatabeskyttelse bør anvendes. I 2002 drejede det sig bl.a. om arbejdet med et udkast til rekommandation "on the interoperability of information systems in the justice sector".

På grund af manglende økonomiske ressourcer har Europarådet i nogen tid måttet foretage indskrænkninger i mødeaktiviteterne for både T-PD og CJ-PD, således at der kun har kunnet afholdes plenarmøder en gang årligt. Dette har haft væsentlig indflydelse på den effektivitet, hvormed der har kunnet arbejdes. På denne baggrund har både T-PD og CJ-PD i 2002 drøftet mulighederne for omstrukturering af de to organers arbejdsform og ændringer i beslutningskompetence. Arbejdet hermed vil blive fortsat.

De officielle tekster kan findes på Europarådets hjemmeside via link fra Datatilsynets hjemmeside.

Den Europæiske Union

Europol-konventionen

Konventionens navn: Konventionen af 26. juli 1995 om oprettelse af en europæisk politienhed (Europol-konventionen).

Ikrafttræden: I Danmark blev gennemførelsen af konventionen vedtaget ved lov nr. 415 af 10. juni 1997. Ifølge lovens § 6 fastsætter justitsministeren tidspunktet for lovens ikrafttræden. Ved bekendtgørelse nr. 508 af 23. juni 1999 er det fastsat, at loven træder i kraft den 1. juli 1999.

Formål: Gennem oprettelse af en europæisk politienhed med en national enhed i hver EU-medlemsstat at forbedre effektiviteten hos medlemsstaternes kompetente myndigheder og disses samarbejde om forebyggelse og bekæmpelse

pelse af bl.a. terrorisme, ulovlig narkotikahandel og andre former for grov international kriminalitet.

Arbejdsopgaver: I henhold til konventionen skal der føres tilsyn med den europæiske politienhed Europol, som fysisk er placeret i Haag, og hvis virksomhed formelt påbegyndtes 1. juli 1999. Dette tilsyn varetages af Den fælles Kontrolinstans, og hertil knytter sig Det fælles Klageudvalg, jf. artikel 24, som skal behandle konkrete klager. Datatilsynet er repræsenteret ved 2 medlemmer i Den fælles Kontrolinstans, hvoraf 1 medlem er indtrådt i Det Fælles Klageudvalg. Ved Retsakt nr. 1/99, udstedt den 22. april 1999 (1999/C 149/01) og offentliggjort i De Europæiske Fællesskabers Tidende den 28. maj 1999 har Den fælles Kontrolinstans efter godkendelse i EU-Rådet fastsat sin forretningsorden, som trådte i kraft den 30. april 1999.

Den fælles Kontrolinstans har i 2002 afholdt 6 møder, hvor man bl.a. har behandlet spørgsmål, som vedrører oprettelse af analysedatabaser, se konventionens artikel 10 og artikel 12, og relationerne til Europol.

Af særlige spørgsmål, der har været drøftet i årets løb, skal især nævnes spørgsmålet om indgåelse af en aftale mellem USA og Europol om udveksling af oplysninger. Endvidere har tilsynsmyndigheden afgivet en udtalelse vedrørende et forslag til ændring af Europol-konventionen.

Det Fælles Klageudvalg har i år 2002 afholdt en række møder, hvor man bl.a. har behandlet to klagesager fra fysiske personer. De pågældende personer har klaget over, at de ikke har kunnet få oplyst, hvorvidt Europol har registreret oplysninger om dem.

Klageudvalget har ved redaktionens slutning afgjort en sag. Klageudvalget udtalte i den forbindelse, at man ikke fandt grundlag for at kritisere Europols afgørelse, hvorefter den pågældende person ikke kunne få oplyst, hvorvidt Europol behandler oplysninger om vedkommende eller ej.

Registertilsynet - nu Datatilsynet - er udpeget som national kontrolinstans efter konventionens artikel 23. Europol er forbundet med en national forbindelsesenhed, som oprettes eller udpeges efter artikel 4, jf. gennemførelseslovens § 3. Denne nationale forbindelsesenhed er i Danmark etableret i Rigspolitechefens regi.

Schengen-konventionen (Schengen-samarbejdet)

Konventionens navn: Konvention om gennemførelse af Schengen-aftalen af 14. juni 1985 mellem regeringerne for staterne i Den økonomiske union Be-

nelux, forbundsrepublikken Tyskland og den Franske Republik om gradvis ophævelse af kontrollen med de fælles grænser (Schengen-konventionen).

Formål: Schengen-regelgrundlaget fastlægger to overordnede formål: Dels at etablere fri personbevægelighed over de indre grænser, dels at styrke indsatsen mod international kriminalitet og illegal indvandring. Formålene skal bl.a. opfyldes ved hjælp af udveksling af oplysninger og erfaringer til brug for de enkelte landes bekæmpelse af kriminalitet.

Baggrunden for Schengen-konventionen var Schengen-aftalen om gradvis ophævelse af kontrollen ved de fælles grænser, der blev indgået den 14. juni 1985 mellem Frankrig, Tyskland, Holland, Luxembourg og Belgien. De samme 5 oprindelige aftalelande underskrev den 19. juni 1990 en konvention om gennemførelse af Schengen-aftalen (Schengen-konventionen). Konventionen blev senere i første omgang tiltrådt af Italien, Spanien, Portugal, Grækenland og Østrig.

Schengen-konventionen blev taget i anvendelse i Frankrig, Tyskland, Belgien, Holland, Luxembourg, Portugal samt Spanien den 26. marts 1995 og efterfølgende i Italien, Østrig og Grækenland. Den 19. december 1996 undertegnede Danmark, Finland og Sverige tiltrædelsesaftaler i forhold til Schengen-konventionen, ligesom der samme dag blev indgået en samarbejdsaftale med Norge og Island.

Ikrafttræden: Folketinget bemyndigede ved lov nr. 418 af 10. juni 1997 om Danmarks tiltrædelse af Schengen-konventionen regeringen til at ratificere tiltrædelsesaftalen på Danmarks vegne, og ratifikationen fandt sted den 23. september 1997. Loven blev delvis sat i kraft (§ 1, jf. § 4, stk. 1), men således at Justitsministeriet blev bemyndiget til at fastsætte ikrafttrædelsestidspunktet for lovens øvrige bestemmelser. I medfør af lovens § 4, stk. 2, traf justitsministeren ved bekendtgørelse nr. 1366 af 20. december 2000 bestemmelse om, at lovens regler om Schengen-informationssystemet trådte i kraft den 1. januar 2001, og at lovens øvrige bestemmelser trådte i kraft den 25. marts 2001.

Arbejdsopgaver: I henhold til konventionens artikel 115 er der nedsat en fælles tilsynsmyndighed, der bl.a. skal føre tilsyn med Schengen-informationssystemets tekniske støttefunktion (C.SIS), som fysisk er placeret i Strasbourg. Repræsentanter for tilsynene i de 3 nordiske EU-medlemsstater samt Island og Norge har siden foråret 1997 haft mulighed for at deltage i Den fælles Tilsynsmyndigheds møder. Efter Danmarks indtræden i Schengen-samarbejdet har Danmark deltaget i møderne som medlem.

Der er i 2002 afholdt 5 møder. Den fælles Tilsynsmyndighed har i januar 2002 afgivet sin 5. aktivitetsrapport for perioden marts 2000 til december

2001. Rapporten er tilgængelig på Datatilsynets hjemmeside. Tilsynsmyndigheden har i år 2002 behandlet forslag til udviklingen af et nyt Schengen-informationssystem (SIS II) og har i øvrigt afgivet en udtalelse vedrørende slettefrister.

Hvert halvår gennemføres i et af Schengen landene en evaluering af det pågældende lands gennemførelse af Schengen konventionen. Evalueringen foretages af en række ekspertgrupper, som nedsættes ad hoc for at undersøge forskellige områder, herunder databeskyttelse. I september 2002 blev der foretaget en samlet evaluering af Holland, Belgien og Luxembourg. Som følge af det danske formandskab varetog det danske Datatilsyn rollen som leder af den internationale ekspertgruppe på 8 medlemmer, der undersøgte databeskyttelsen i Benelux-landene.

På databeskyttelsesområdet var der kun mindre bemærkninger, som ikke gav anledning til rekommandationer i de overordnede konklusioner i den samlede evalueringsrapport.

Registertilsynet - nu Datatilsynet - er udpeget som tilsynsmyndighed efter konventionens artikel 114 og 128, jf. gennemførelseslovens § 2, stk. 3, hvilket bl.a. indebærer, at der skal føres tilsyn med den nationale del af SIS-systemet (N.SIS), som er en kopi af C.SIS. I Danmark er den nationale del af SIS-systemet oprettet i Rigspolitichefens regi.

Toldinformations-systemet

Konventionens navn: Konvention udarbejdet på grundlag af artikel K.3. i traktaten om Den Europæiske Union om brug af informationsteknologi på toldområdet.

Formål: At danne grundlag for oprettelse af "Toldinformationssystemet (CIS)", som skal bidrage til forebyggelse, efterforskning og retsforfølgning af alvorlige overtrædelser af de nationale love ved gennem en hurtig udbredelse af oplysninger at øge effektiviteten i samarbejds- og kontrolprocedurerne hos toldadministrationerne i medlemsstaterne.

Ikrafttræden: Konventionen blev undertegnet den 26. juli 1995. CIS-konventionen er dog ikke trådt i kraft for alle de undertegnede EU-medlemslande, men er midlertidigt bragt i anvendelse mellem de otte lande, der på nuværende tidspunkt har ratificeret konventionen, herunder Danmark, fra den 1. november 2000.

Arbejdsopgaver: I henhold til konventionens artikel 17 skal medlemsstaterne udpege en national tilsynsmyndighed med ansvar for beskyttelse af per-

sonoplysninger. Registertilsynet (nu Datatilsynet) er af Skatteministeriet blevet anmodet om at påtage sig opgaven som national tilsynsmyndighed, og tilsynet har givet ministeriet tilsagn om at ville varetage denne opgave.

Der skal oprettes en fælles tilsynsmyndighed, jf. artikel 18, bestående af 2 repræsentanter fra hver af medlemsstaterne, udpeget blandt medlemsstaternes uafhængige tilsynsmyndigheder. Denne myndighed skal føre tilsyn med en central database, som skal oprettes i EU-regi i Bruxelles, med terminaladgang for samtlige medlemsstaters myndigheder.

I 2002 blev der afholdt flere møder i den fælles tilsynsmyndighed, hvor man bl.a. har vedtaget en endelig forretningsorden. Det egentlige arbejde i myndigheden er endnu ikke startet. Det forventes dog, at informationssystemet tages i brug i løbet af 2003.

CIS-toldinformationssystemet skal udgøre en del af en fælles edb-database, hvori der også indgår oplysninger, som er omfattet af Rådets Forordning (EF) nr. 515/97 af 13. marts 1997 om gensidig bistand mellem medlemsstaternes administrative myndigheder og om samarbejde mellem disse og Kommissionen med henblik på at sikre den rette anvendelse af told- og landbrugsbestemmelserne. Det må forventes, at tilsynet med den forordningsregulerede del af systemet (søjle I) skal henlægges til den uafhængige kontrolinstans, der er omhandlet i EU-traktatens artikel 286, når denne er blevet oprettet, se pkt. 4.2.7. Indtil da skal tilsynet føres af EU-Parlamentets Ombudsmand, jf. artikel 37 stk. 4.

Sekretariatet for de fælles tilsynsmyndigheder

EU-Rådet har den 17. okt. 2000 (2000/641/RIA) under henvisning til artikel 30 og artikel 34, stk. 2, litra c), i traktaten om Den Europæiske Union truffet afgørelse om oprettelse af et sekretariat for de fælles tilsyns/kontrolmyndigheder vedrørende databeskyttelse, der er oprettet i henhold til konventionen om oprettelse af en europæisk politienhed (Europol-konventionen), konventionen om brug af informationsteknologi på toldområdet og konventionen om gennemførelse af Schengen-aftalen om gradvis ophævelse af kontrollen ved de fælles grænser (Schengen-konventionen), se EF-Tidende 2000, nr. L 271 af 24. oktober 2000, s. 1-3.

Afgørelsen trådte i kraft dagen efter vedtagelsen, men således at den kan anvendes fra 1. september 2001.

Ved afgørelsen har de fælles tilsynsmyndigheder fået mulighed for at fungere mere effektivt, og samtidig kan omkostningerne nedbringes. Det er udtrykkeligt fastslået, at databeskyttelsessekretariatet skal være uafhængigt, idet det

ved udførelsen af sine opgaver kun er bundet af instrukser fra de fælles tilsynsmyndigheder. Af praktiske grunde er databeskyttelsessekretariatets administration dog tæt knyttet til Generalsekretariatet for Rådet.

I overensstemmelse med Rådets afgørelse begyndte sekretariatet sit virke i september 2001. Sekretariatet ledes af en jurist med stor erfaring inden for databeskyttelse. Det kan konstateres, at etableringen af sekretariat har medført en positiv udvikling i forbindelse med sekretariatsbistanden til de fælles tilsynsmyndigheder.

Napoli II-konventionen

Konventionens navn: Konvention udarbejdet på grundlag af artikel K.3. i traktaten om Den Europæiske Union om gensidig bistand og samarbejde mellem toldmyndighederne (Napoli II).

Formål: At styrke EU-toldmyndighedernes samarbejde vedrørende vareoverførsler over såvel medlemslandenes indre grænser som over grænser fra tredjelande med ulovlige varer (narkotika, våben og børnepornografi m.v.) samt ulovlig handel med højtbeskattede varer.

Ikrafttræden: Konventionen blev undertegnet den 18. december 1997. Napoli II-konventionen erstatter konventionen af 7. september 1967 om gensidig bistand mellem EU-landenes toldforvaltninger (Napoli I-konventionen), der blev tiltrådt af Danmark i forbindelse med indtrædelsen i EF i 1973. Napoli I-konventionen ophæves ved ikrafttrædelsen af Napoli II-konventionen.

Arbejdsopgaver: Ifølge Napoli II-konventionens artikel 25, litra i), træffer hver enkelt medlemsstat passende foranstaltninger for ved hjælp af effektiv kontrol at sikre, at denne artikel overholdes. Artikel 25 indeholder en række regler om databeskyttelse. Den enkelte medlemsstat kan overdrage disse kontrolopgaver til den nationale tilsynsmyndighed, der er omhandlet i artikel 17 i CIS-konventionen.

Registertilsynet afgav i 1999 en udtalelse til Skatteministeriet om et udkast til forslag til lov om gennemførelse af konventionen om gensidig bistand og samarbejde mellem toldmyndighederne (Napoli II) og om gennemførelse af protokol om præjudiciel fortolkning ved De Europæiske Fællesskabers Domstol af Konventionen om brug af informationsteknologi på toldområdet (CIS-konventionen).

Tilsynet udtalte, at såfremt de i artikel 25 nævnte kontrolopgaver skulle henlægges til tilsynet, burde dette fremgå direkte af loven.

I lov nr. 482 af 7. juni 2001 om Danmarks tiltrædelse af konventionen om gensidig bistand og samarbejde mellem toldmyndighederne (Napoli II-konventionen), vedtaget den 15. maj 2001, er Datatilsynet derfor nu indsat som tilsynsmyndighed efter konventionens artikel 25, jf. lovens § 4, stk. 2. Lovens § 1, stk.1, § 2, stk.1, og § 3 træder i kraft dagen efter bekendtgørelse i Lovtidende. Skatteministeren fastsætter tidspunktet for ikrafttrædelse af lovens øvrige bestemmelser.

Eurodac-systemet

Forordningens navn: EU-Rådets forordning (EF) nr. 2725/2000 om oprettelse af "Eurodac" til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af Dublin-konventionen (EF-Tidende Nr. L 316 af 15/12/2000 s. 1), vedtaget af EU-Rådet den 11. december 2000.

Forordningen trådte i kraft den 15. december 2000 på dagen for offentliggørelse i EF-Tidende.

Som følge af det danske forbehold vedrørende retlige og indre anliggender deltog Danmark ikke i vedtagelsen af forordningen, som ikke er bindende for og ikke finder anvendelse i Danmark. Danmark har imidlertid anmodet om at blive tilknyttet Eurodacsystemet på mellemstatsligt grundlag, men deltager ikke aktuelt i Eurodacsystemet.

Formålet med Eurodacforordningen er at fastlægge regler for oprettelse af en elektronisk database af fingeraftryk af asylansøgere og visse andre personer for at lette anvendelsen af Dublinkonventionen, som indeholder bestemmelser til fastsættelse af, hvilken medlemsstat der er ansvarlig for behandling af en asylansøgning. EU-medlemsstaterne kan gennem databasen udveksle fingeraftryk af en asylansøger med henblik på at afklare, om denne tidligere har søgt asyl i en anden medlemsstat.

Af særlig interesse kan nævnes, at det i forordningen er bestemt, at der midlertidigt skal oprettes en uafhængig fælles tilsynsmyndighed, som skal kontrollere den centrale enheds behandling af personoplysninger, indtil den uafhængige kontrolinstans, der er omhandlet i EU-traktatens artikel 286, er blevet oprettet, se herom nedenfor.

Det følger af Eurodacforordningens artikel 19, stk. 1, at hver medlemsstat drager omsorg for, at den eller de nationale tilsynsmyndigheder, der udpeges i henhold til artikel 28, stk. 1, i direktiv 95/46/EF, i fuld uafhængighed og i overensstemmelse med det pågældende medlemsstats nationale ret overvåger, at den pågældende medlemsstats behandling af personoplysninger i

overensstemmelse med Eurodacforordningen, herunder videregivelsen af oplysninger til den centrale enhed, foregår på lovlig vis.

Datatilsynet forventer at blive udpeget som national tilsynsmyndighed i forhold til behandlingen af de oplysninger, der er videregivet og modtaget efter Eurodacforordningen.

Det generelle databeskyttelsesdirektiv

Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger er det vigtigste internationale regelsæt for Danmark inden for databeskyttelsesområdet. Direktivet trådte i kraft den 24. oktober 1998 og er med persondatalovens ikrafttræden den 1. juli 2000 gennemført i Danmark.

Arbejdsopgave: Direktivet giver Europa-Kommissionen forskellige beføjelser efter en særlig komitéprocedure, jf. artikel 31, bl.a. vedrørende forholdet til tredjelande, det vil sige lande uden for EU. I henhold til direktivets artikel 29 er der nedsat en "gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger", den såkaldte "Artikel 29-gruppe". Gruppen er rådgivende og uafhængig og består af repræsentanter for den eller de tilsynsmyndigheder, som hver medlemsstat har udpeget, og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne, samt af en repræsentant for Kommissionen. Kommissionen (GD for det Indre Marked) er sekretariat for gruppen.

Artikel 29-gruppen har i 2002 afholdt 5 to-dagsmøder. Datatilsynet har deltaget i en underarbejdsgruppe "Internet Task Force", som særligt arbejder med beskyttelse af personoplysninger i forbindelse med anvendelse af internet og anden ny teknik. Datatilsynet har også deltaget i en underarbejdsgruppe vedrørende WP 56, se nedenfor. Der har endvidere været afholdt en konference om direktivets implementering fra den 30. september 2002 til den 1. oktober 2002 med deltagelse af repræsentanter fra Datatilsynet.

Artikel 29-gruppen har også i 2002 vedtaget en række henstillinger, udtalelser m.v.

Der er således i 2002 vedtaget dokumenter om følgende:

- Arbejdsdokument om overvågning af elektronisk kommunikation på arbejdspladsen (WP 55)

- Arbejdsdokument om den internationale anvendelse af Fællesskabets databeskyttelseslovgivning ved behandling af personoplysninger på Internet, som foretages af websteder, der er etableret uden for Fællesskabet (WP 56)
- Udtalelse nr. 1/2002 om CEN/ISSS-rapporten om standardisering af beskyttelsen af privatlivets fred i Europa (WP 57)
- Udtalelse nr. 2/2002 om anvendelsen af unikke identifikationskoder i teleterminaludstyr: tilfældet IPv6 (WP 58)
- Arbejdsdokument om Artikel 29-gruppens første retningslinier vedrørende online-autentificeringstjenester (WP 60)
- Udtalelse nr. 3/2002 om databeskyttelsesbestemmelserne i Kommissionens forslag til direktiv om harmonisering af medlemsstaternes love og administrativt fastsatte bestemmelser om forbrugerkredit (WP 61)
- Arbejdsdokument om anvendelsen af safe harbor-aftalen i praksis (WP 62)
- Udtalelse nr. 4/2002 om databeskyttelsesniveauet i Argentina (WP 63)
- Udtalelse nr. 5/2002 om de europæiske databeskyttelsesmyndigheders erklæring på den internationale konference i Cardiff (9.-11. september 2002) om obligatorisk og systematisk lagring af teletrafikdata (WP 64)
- Arbejdsdokument om "Black lists" (WP 65)
- Udtalelse nr. 6/2002 om transmission af passageroplysninger samt andre oplysninger fra luftfartsselskaber til USA (WP 66)

Artikel 29-gruppens dokumenter er tilgængelige på Kommissionens hjemmeside, hvortil der er adgang via link fra Datatilsynets hjemmeside. Tilsynets hjemmeside indeholder yderligere information om arbejdsgruppen og dens dokumenter.

Databeskyttelse internt i EU-/EF-institutionerne

Forordningens navn: Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger. Forordningen blev vedtaget den 18. december 2000 og har sit grundlag i traktaten om Det Europæiske Fællesskab, idet der i artikel 286 er optaget en bestemmelse om beskyttelse af personoplysninger, således at der skal gælde databeskyttelsesregler for institutionerne og organer, som er oprettet ved eller på grundlag af denne traktat (EF-Tidende Nr. L 8 af 12/1/2001, s. 1).

Ikrafttræden: Ifølge artikel 51 træder forordningen i kraft på tyvendedagen efter offentliggørelsen den 12. januar 2001 i EF-Tidende.

Formålet: Hensigten med forordningen er, at regler svarende til det generelle databeskyttelsesdirektiv og til direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren skal gælde

for fællesskabets institutioner og organer i lighed med de nationale gennemførselsbestemmelser for medlemsstaterne. Forordningen indeholder tillige bestemmelser om oprettelse af en uafhængig kontrolmyndighed.

Kontrolinstansen kaldes "Den europæiske tilsynsførende for databeskyttelse" og har til opgave at overvåge og sikre overholdelsen af de bestemmelser i forordningen og i enhver anden fællesskabsretsakt, der vedrører beskyttelsen af fysiske personers grundlæggende rettigheder, se artikel 41. Der tillægges den tilsynsførende en række hverv og beføjelser, som nærmere er beskrevet i artikel 46 og artikel 47. Det fremgår bl.a., at den tilsynsførende har til opgave at samarbejde med de nationale tilsynsmyndigheder i EU-medlemsstaterne.

EU-datakommisærernes arbejde

Alle EU's medlemsstater har nu lovgivning om persondatabeskyttelse.

Der er i årsberetning 1996 side 18-20 redegjort for det siden 1995 formaliserede samarbejde mellem EU-datatilsynene, der dog i nogen grad har ændret indhold, efter at der afholdes regelmæssige møder i Artikel 29-gruppen.

Samarbejdet foregår fortsat i form af afholdelse af en årlig konference samt et møde, som afholdes i forbindelse med den årlige internationale konference.

I 2002 blev den årlige EU-datatilsynskonference afholdt i Bonn, arrangeret af det tyske tilsyn (Der Bundesbeauftragte für den Datenschutz). På konferencen drøftedes en række spørgsmål af fælles interesse, bl.a. erfaringer efter 11. september 2001, certificering, biometrisk identifikation og e-government.

Det 24. årlige internationale møde for datatilsynsmyndighederne blev i september 2002 afholdt i Cardiff, arrangeret af datatilsynsmyndighederne i Det Forenede Kongerige, Irland, Isle of Man, Jersey og Guernsey. På konferencen beskæftigede man sig med en række emner af fælles interesse, herunder bl.a. e-government, uafhængige tilsynsmyndigheders rolle og e-handel.

I forbindelse med det 24. årlige internationale møde afholdt de europæiske databeskyttelseskommisærer et lukket møde. I den anledning afgav de europæiske databeskyttelseskommisærer en udtalelse med følgende overskrift: "Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data". I udtalelsen udtryktes bekymring angående obligatorisk systematisk opbevaring af trafikdata vedrørende alle

International konference for datatilsynsmyndigheder m.v.

former for telekommunikation i et år eller mere for at give bl.a. politiet mulighed for at få adgang til oplysningerne.

En international arbejdsgruppe - International Working Group on Data Protection in Telecommunication - blev etableret i 1983 på initiativ af tilsynsmyndighederne (Data Protection Commissioners) fra en række lande, herunder Danmark, i forbindelse med den internationale konference.

Sekretariatsfunktionen har siden gruppens etablering været varetaget af Berlins Datatilsyn (Berliner Beauftragter für Datenschutz und Informationsfreiheit). Arbejdsgruppen har beskæftiget sig med databeskyttelsesmæssige anliggender inden for telekommunikation i bred forstand, i de senere år i vid udstrækning vedrørende internettet.

Berlin-gruppen afholder normalt møde to gange om året. Efter ønske fra et eller flere af medlemmerne eller fra den europæiske eller internationale konference behandles en række emner. Resultatet af behandlingen af et emne vil ofte blive udtrykt i en fælles holdning (et "Working Paper"). Disse "Working Papers" kan anvendes i det videre konkrete arbejde med lovgivning eller fastlæggelse af praksis, som behandles internationalt eller nationalt.

Gruppens "Working Papers" og øvrige dokumenter er tilgængelige på tysk eller engelsk på Berlins Datatilsyns hjemmeside (<http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm>). Gruppen og dens dokumenter beskrives nærmere på Datatilsynets hjemmeside under menupunktet Internationalt.

Nordisk samarbejde

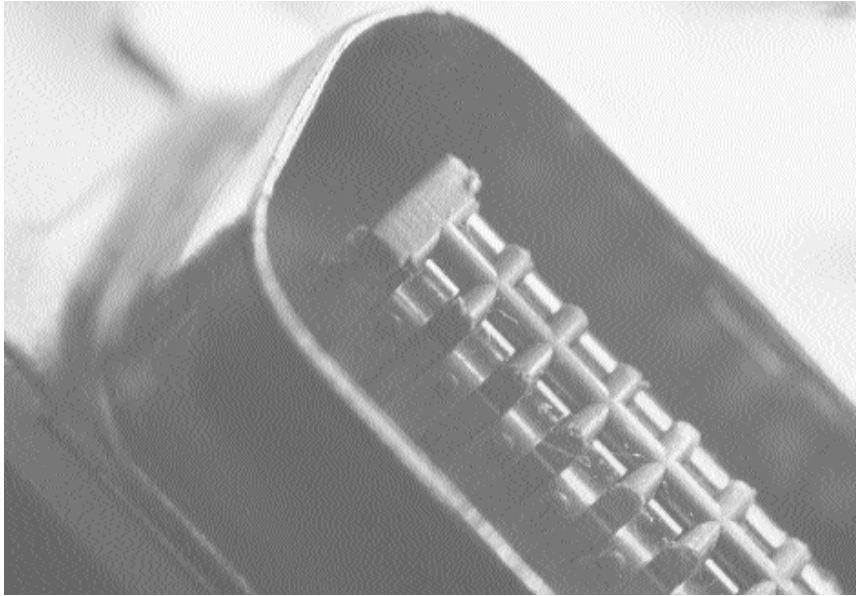
Det nordiske samarbejde mellem datatilsynsmyndighederne i Danmark, Finland, Island, Norge og Sverige er blevet fortsat, og i 2002 stod det svenske datatilsyn for afholdelse af det fællesnordiske datachefmøde.

På mødet udvekslede deltagerne oplysninger om såvel generelle som konkrete afgørelser. Bl.a. diskuterede deltagerne særlige spørgsmål i tilknytning til behandling af personoplysninger på arbejdsmarkedet og i skoler, i genetiske databaser og Safe Harbor-ordningen.

Nordisk Teknikermøde 2002

Datatilsynet var i september måned vært for Nordisk Teknikermøde. Mødet afholdes årligt og afvikles over to dage. I årets møde deltog teknikere samt sikkerheds- og inspektionsmedarbejdere fra datatilsynsmyndighederne i Finland, Norge, Sverige og Danmark. Blandt de behandlede emner var praktisk og konkret sikkerhed, elektronisk borgerbetjening, erfaringer omkring tilrette-

læggelse og gennemførelse af inspektioner, registrering og rapportering af observationer ved inspektioner, fremme af arbejde med branchevise adfærdsnormer inden for informationssikkerhed samt en række konkrete udfordringer af teknisk art, som tilsynsmyndighederne forventes at blive stillet overfor i de kommende år. Der var foruden kredsen af teknikere fra de nordiske tilsynsmyndigheder inviteret to eksterne foredragsholdere til at give indlæg om nye måder, hvorpå man kan sikre privatlivets fred samt om systematisk test af efterlevelse af persondatalovens regler.



Sikkerhedsspørgsmål

Persondatalovens krav om datasikkerhed 92

OCES certifikater 93

Sikkerhedsspørgsmål

Persondatalovens krav om datasikkerhed

I medfør af § 41, stk. 5, i lov om behandling af personoplysninger har justitsministeren fastsat nærmere regler om de i lovens § 41, stk. 3, anførte sikkerhedsforanstaltninger ved bekendtgørelse nr. 528 af 15. juli 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Bekendtgørelsen er siden ændret ved bekendtgørelse nr. 201 af 22. marts 2001. Sikkerhedsbekendtgørelsen findes bl.a. på www.datatilsynet.dk.

Datatilsynet har udarbejdet vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juli 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Vejledningen findes bl.a. på Datatilsynets hjemmeside.

Såvel bekendtgørelsen som vejledningen retter sig mod behandling af personoplysninger, som foretages for den offentlige forvaltning. For oplysninger, som behandles i den private sektor, gælder umiddelbart § 41, stk. 3, i persondataloven.

I flere konkrete sager har Datatilsynet ved vurdering af de sikkerhedsforanstaltninger, som har været truffet af private dataansvarlige, taget udgangspunkt i de anvisninger, som fremgår af sikkerhedsbekendtgørelsen og sikkerhedsvejledningen.

Konklusionen har været, at de beskrevne sikkerhedskrav bør følges, både når den dataansvarlige er en offentlig myndighed, og når der er tale om en privat virksomhed m.v. Det er således Datatilsynets opfattelse, at persondatalovens § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i private virksomheder m.v. som i den offentlige forvaltning.

Eksempelvis gælder dette ved transmission af personoplysninger over det åbne internet. Efter Datatilsynets opfattelse bør der ved transmission af oplysninger om *personnumre* over det åbne internet som minimum foretages kryptering. Der bør også foretages kryptering, hvis andre oplysninger, som må betragtes som fortrolige (f.eks. oplysninger om økonomiske forhold o.l.), transmitteres.

Hvis der er tale om *følsomme oplysninger* omfattet af persondatalovens § 7 og § 8 (f.eks. oplysninger om fagforeningsmæssige tilhørsforhold, helbredsforhold eller strafbare forhold), skal der som minimum anvendes en stærk kryptering, baseret på en anerkendt algoritme.

Udtalt, at såkaldte OCES certifikater generelt vil kunne benyttes ved borgerens indsendelse af oplysninger til myndigheder. For så vidt angår selvbetjeningsløsninger med en facilitet til forudfyldte blanketter udtalt, at persondatalovens krav ville være opfyldt, hvis der anvendes digital signatur med et OCES certifikat (Datatilsynets j.nr. 2002-321-0142)

Datatilsynet har udtalt, at det såkaldte OCES certifikat (Offentligt Certifikat til Elektronisk Service) i relation til databeskyttelsesmæssige krav i persondataloven må anses for tilstrækkeligt sikkert.

På baggrund af en henvendelse fra Ministeriet for Videnskab, Teknologi og Udvikling (MVTU) har Datatilsynet med udgangspunkt i det udkast til politik for OCES certifikatet som MVTU havde sendt i høring den 15. januar 2002, vurderet, at OCES certifikatet - i relation til persondataloven - generelt vil kunne benyttes ved borgerens indsendelse af oplysninger til myndighederne. Tilsynet vurderede endvidere, at OCES certifikatet vil kunne anvendes ved myndighedernes fremsendelse af oplysninger til den registrerede enten i form af forudfyldte skemaer, blanketter m.v. eller ved indsigtssøgninger.

Efter Datatilsynets opfattelse er det ved implementeringen af digitale selvbetjeningsløsninger ved hjælp af digitale signaturer et ufravigeligt krav, at der skal ske sikring af fortroligheden ved anvendelse af kryptering.

Datatilsynet udtalte, at man kan skelne mellem to situationer:

1. Borgeren *indsender* oplysninger til myndigheden (f.eks. i form af skemaer eller blanketter m.v.).
2. Myndigheden giver *adgang* til oplysningerne - enten i form af f.eks. indsigt (egenaccess) til borgeren eller ved delvist forudfyldte blanketter.

Borgeren indsender oplysninger til myndigheden (f.eks. i form af skemaer eller blanketter m.v.)

Datatilsynet henviste til persondatalovens § 41, stk. 3, og sikkerhedsbekendtgørelsens § 14 og udtalte, at der i forbindelse med selvbetjeningsløsninger samlet set skal være den fornødne sikkerhed for, at personoplysninger ikke kommer uvedkommende i hænde, og at personoplysninger ikke forringes eller tilintetgøres.

Ifølge persondataloven § 5, stk. 4, skal den dataansvarlige tilrettelægge behandlingen af oplysninger således, at der foretages ajourføring af oplysningerne, og skal endvidere foretage den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger.

Datatilsynet udtalte i den forbindelse, at persondatalovens § 5, stk. 4, skulle indgå i overvejelserne om, hvorvidt en elektronisk selvbetjeningsløsning, der giver mulighed for indsendelse af oplysninger, opfyldte kravene i persondataloven.

Datatilsynet vurderede herefter, at OCES certifikatet generelt ville kunne benyttes ved borgerens indsendelse af oplysninger til myndighederne. Datatilsynet var således af den opfattelse, at løsningen, som var baseret på brug af folkeregisteradressen ved identitetskontrol i forbindelse med certifikatudstedelse, måtte anses for at være tilstrækkelig sikker i relation til de databeskyttelsesmæssige krav.

Myndigheden giver adgang til oplysningerne - enten i form af f.eks. indsigt (egenaccess) til borgeren eller ved delvist forudfyldte blanketter

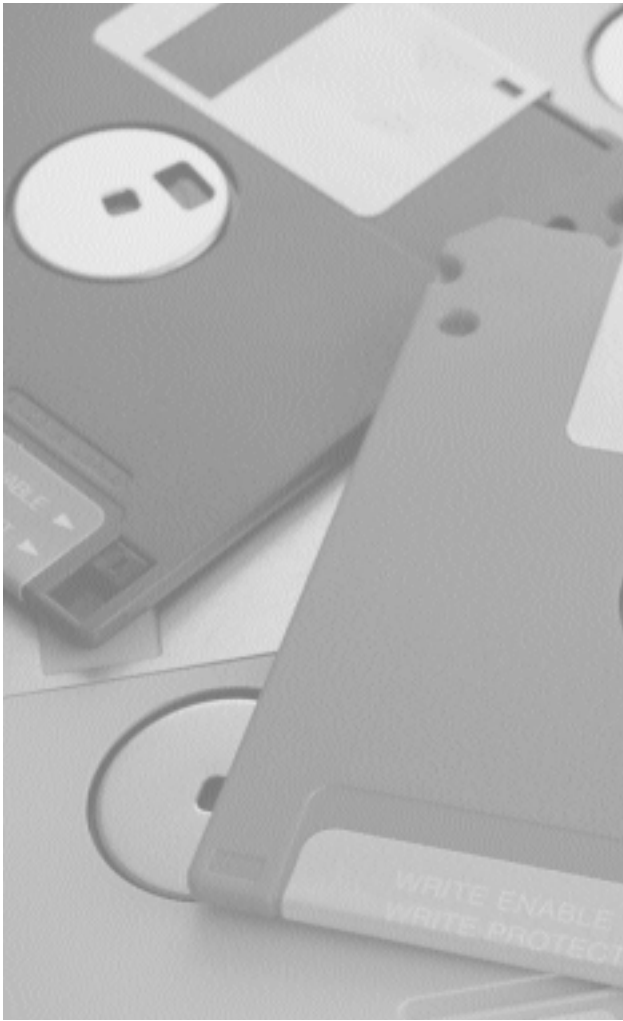
Af persondatalovens § 41, stk. 3, fremgår bl.a., at der skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Datatilsynet udtalte, at den dataansvarlige - og en eventuel databehandler - skal sikre sig, at den, der meddeles oplysninger til, er rette person, således at oplysninger om den registrerede ikke kommer til uvedkommendes kendskab m.v. Der må således efter tilsynets opfattelse kun udleveres oplysninger, når vedkommende har legitimeret sig behørigt, eller når der på anden måde er skabt sikkerhed for, at den der f.eks. fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører.

Ved udstedelse af OCES certifikatet kontrollerer udstederen underskriverens (f.eks. en borger) adresse i CPR-registeret, og den nødvendige pinkode sendes efterfølgende til underskriverens folkeregisteradresse.

Det var herefter Datatilsynets vurdering, at etablering af selvbetjeningsløsninger med en facilitet med forudfyldte blanketter kan opfylde persondatalovens krav, hvis der benyttes digital signatur med et OCES certifikat.

Datatilsynet har siden taget stilling til yderligere spørgsmål i relation til OCES certifikater. Se nærmere på www.datatilsynet.dk under "Værd at vide" - elektronisk borgerservice.



Tilsynsvirksomhed

<i>Generelt om Datatilsynets inspektioner</i>	98
<i>Gennemførelse af inspektioner</i>	99
<i>Formidling af resultater af inspektioner</i>	99
<i>Datatilsynets observationer ved inspektioner i 2002</i>	100
<i>Oversigt over udførte inspektioner i 2002</i>	104

Tilsynsvirksomhed

Generelt om Datatilsynets inspektioner

Datatilsynet fører tilsyn med enhver behandling, der omfattes af persondataloven, bortset fra behandlinger der foretages for domstolene. I forbindelse hermed påser Datatilsynet af egen drift eller efter klage fra en registreret, at en behandling finder sted i overensstemmelse med lovgivningen og de bestemmelser, der er udstedt i medfør af loven. Som led i denne tilsynsvirksomhed kan Datatilsynet tage sager op af egen drift, hvis tilsynet finder anledning dertil.

Datatilsynet kan efter persondatalovens § 62, stk. 1, kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

I forhold til behandlinger, som foretages for den offentlige forvaltning, har Datatilsynets personale efter lovens § 62, stk. 2, til enhver tid adgang til alle lokaler, hvorfra behandlingen administreres eller kan benyttes, samt til lokaler, hvor oplysninger eller de tekniske hjælpemidler opbevares eller anvendes. Tilsynet skal forevise behørig legitimation, men der kræves ikke retskendelse.

Det fremgår af persondatalovens forarbejder, at det er forudsat, at tilsynet har mulighed for selv at gøre sig bekendt med oplysningerne efter at have fået adgang til lokaler, hvorfra der er adgang til disse.

Datatilsynets har mulighed for at gennemføre uanmeldte inspektioner. I praksis varsles inspektionerne oftest nogle uger i forvejen, da det er vigtigt, at de relevante medarbejdere hos den dataansvarlige kan være til stede. Datatilsynet opfatter ikke kun inspektionerne som en kontrolforanstaltning, men lægger også stor vægt på at komme i dialog med de dataansvarlige. Tilsynets repræsentanter informerer og vejleder om lovens regler og Datatilsynets praksis.

Hvis Datatilsynet i forbindelse med en inspektion eller på anden vis må konstatere, at en myndighed har overtrådt persondataloven, og der er tale om overtrædelser af en vis alvor, udtaler tilsynet kritik over for myndigheden. Er der tale om en kommune eller et amt, kan der blive tale om et brev (indberetning) til kommunalbestyrelsen eller amtsrådet. For så vidt angår statslige myndigheder kan det komme på tale at orientere en overordnet myndighed eller den pågældende minister.

Datatilsynets inspektionskompetence i forhold til private virksomheder er i lovens § 62, stk. 3 og 4, begrænset til de typer af behandlinger, der er omfattet af tilladelseskravet i lovens § 50 samt til edb-servicevirksomheder

omfattet af anmeldelsespligten i lovens § 53. Se eventuelt Datatilsynets årsberetning for 2001 side 78 i afsnittet "Inspektioner hos private virksomheder".

Over for private virksomheder m.v. har tilsynet mulighed for at give påbud og forbud med henblik på overholdelse af loven og kan i yderste konsekvens skride til politianmeldelse.

Datatilsynet har i sin årsberetning for 2001 på siderne 77-80 beskrevet forløbet af inspektioner hos offentlige myndigheder, i private virksomheder og af private forskningsprojekter nærmere.

Der henvises i øvrigt til Datatilsynets hjemmeside, hvor der bl.a. ligger en vejledende dagsorden for inspektioner hos offentlige myndigheder.

Datatilsynet har i 2002 planlagt og gennemført flere inspektioner end i noget tidligere år. Det var derfor relevant at finde nye former for afholdelse af mange inspektioner, således at inspektionerne også geografisk kom til at omfatte hele landet. Tilsynet kunne konstatere, at to geografiske områder - Nordjylland og Sønderjylland - i forhold til landet som helhed havde haft et relativt lavt antal inspektioner siden først registerlovenes og senere persondatalovens ikrafttræden. Der blev derfor iværksat en målrettet indsats i disse to regioner.

Indsatsen har bestået i, at tilsynet hvert af de to steder har haft udstationeret seks medarbejdere i en uge. I løbet af disse to uger blev der i alt i de to regioner gennemført 58 inspektioner ved kommuner, amter, politimestre og andre statsinstitutioner samt hos private forskere og virksomheder.

Det er tilsynets indtryk, at man ved i en periode at koncentrere sig om veldefinerede områder – her geografiske – opnår stor opmærksomhed omkring persondatalovens regler, tilsynets opgaver og datasikkerhed generelt.

Datatilsynet har traditionelt formidlet resultaterne af sine inspektioner ved i årsberetningen og på sin hjemmeside at nævne, hvor inspektioner har været gennemført, og ved at offentliggøre den eventuelle kritik, som tilsynet har udtalt.

Som et forsøg blev resultaterne af 28 inspektioner, der blev gennemført i Nordjylland i foråret 2002, offentliggjort ved tildeling af karakterer på en skala fra 1 til 3. Karaktererne blev tildelt på baggrund af, hvad tilsynet kunne

Gennemførelse af inspektioner

Formidling af resultater af inspektioner

konstatere ved sine kontrolbesøg samt i nogle situationer i den efterfølgende dialog med de berørte parter.

Karaktererne blev givet som udtryk for følgende:

1. Inspektionen gav ikke anledning til bemærkninger eller alene bemærkninger af bagatelagtig karakter
2. Inspektionen gav anledning til visse bemærkninger af mindre alvorlig karakter
3. Inspektionen gav anledning til alvorlig kritik

En sådan inddeling vil i sagens natur være skønsmæssig, og den kan alene bygge på de oplysninger, som Datatilsynet har tilvejebragt gennem besøgene og den efterfølgende dialog. Det kan således ikke ud fra karakteren alene konkluderes, hvorvidt en given dataansvarlig har overholdt persondataloven.

Forsøget med karaktertildeling medførte en del omtale af og interesse for inspektionerne, men rejste samtidig spørgsmål om, hvilke forhold der førte til tildelingen af navnlig karakteren 2. Erfaringerne med denne måde at formidle inspektionsresultaterne på indgår i de løbende overvejelser om Datatilsynets informationsvirksomhed.

Datatilsynets observationer ved inspektioner i 2002

I det følgende beskrives i store træk de observationer, som Datatilsynet har gjort i forbindelse med inspektionerne i 2002. Der er ikke foretaget en egentlig statistisk bearbejdning af inspektionsresultaterne, men beskrivelsen er egnet til at illustrere de generelle tendenser, som tilsynet har oplevet dem på inspektionerne.

Anmeldelser

Det overordnede indtryk efter inspektionerne afholdt i 2002 er, at de dataansvarlige med ganske få undtagelser er opmærksomme på pligten til at anmelde behandlinger af personoplysninger til Datatilsynet, og at de dataansvarlige i det store hele har foretaget anmeldelse af de anmeldelsespligtige behandlinger, de foretager. Der ses dog af og til eksempler på manglende eller for sent foretagne anmeldelser. Som et eksempel på en behandling, der typisk overses, kan nævnes offentlige myndigheders kontrol af medarbejderes brug af e-post og internet.

Datatilsynet gennemførte i starten af 2002 en kampagne, hvor man rettede henvendelse til kommuner, der kun havde foretaget meget få eller slet ingen anmeldelser. Dette resulterede i, at Datatilsynet modtog et antal anmeldelser, hvoraf en stor del var tilslutninger til fællesanmeldelser.

Opfyldelse af logningskrav

Et problem, som tilsynet jævnligt er stødt på i 2002, er offentlige myndigheds manglende opfyldelse af sikkerhedsbekendtgørelsens regler om logning af brug af personoplysninger eller sletning af oplysningerne efter en vis kortere periode. Formålet med disse regler er at forebygge og have mulighed for at kontrollere autoriserede brugeres eventuelle misbrug af adgangen til personoplysninger. Kravet om logning gælder for elektronisk databehandling af personoplysninger, i det omfang behandlingen er omfattet af kravet om anmeldelse til Datatilsynet. Det vil groft sagt sige, når der indgår fortrolige eller følsomme oplysninger.

Der er set en række eksempler på opbygning af egentlige småsystemer uden logningsfaciliteter til behandling af personoplysninger og på manglende sletning af tekstbehandlingsdokumenter o.l., som indeholder fortrolige eller følsomme personoplysninger.

Tilsynet anmoder rutinemæssigt ved inspektioner om kontrolopslag i systemer, hvor der kræves logning for herved at kontrollere, om systemerne logger i overensstemmelse med reglerne herom.

Datatilsynet vil i løbet af 2003 i større omfang end hidtil forud for inspektioner anmode dataansvarlige eller databehandlere om logudskrifter. Stikprøver blandt transaktionerne fra disse logudskrifter vil blive gennemgået under inspektionerne.

Oplysningspligt, indsigtsret og samkøring i kontroløjemed

De fleste offentlige myndigheder er opmærksomme på reglerne på disse områder. Tilsynet har dog i en række tilfælde anbefalet en gennemgang af instrukser og forretningsgange samt af fortrykte tekster på blanketter m.v.

Mange kommuner har formelt fastsat en procedure for behandling af indsigtsbegæringer (egen-access), hvorefter disse koordineres fra centralt hold. En del har foldere, som informerer borgerne om deres rettigheder.

Billeder på internet

Det er meget forskelligt, i hvilket omfang dataansvarlige offentliggør billeder af personer på internettet. På det kommunale område er det især skoler, som ønsker at vise deres aktiviteter på internettet. Nogle - men ikke alle - kommuner har været opmærksomme på de regler, der gælder om samtykke, og har enten kun offentliggjort billeder, som kunne offentliggøres uden samtykke - eller de har sørget for at have samtykke fra personer, der optrådte på de offentliggjorte billeder.

Datatilsynet lempede i slutningen af 2002 praksis for krav om samtykke fra personer, som optræder på billeder, der offentliggøres på internettet. Tilsynet skelner mellem situationsbilleder og portrætbilleder. Situationsbilleder defineres som billeder, hvor en aktivitet eller en situation er det egentlige formål med billedet. Det kunne f.eks. være legende børn i en skolegård eller besøgende i en zoologisk have. Modsætningen hertil er portrætbilleder, hvor formålet er at afbilde en eller flere bestemte personer.

Udgangspunktet er, at situationsbilleder kan offentliggøres uden samtykke. Offentliggørelse skal dog ske under skyldig hensyntagen til karakteren af billedet, herunder den sammenhæng, hvori billedet optræder og formålet med offentliggørelsen. Det afgørende kriterium er, at den afbildede ikke med rimelighed må kunne føle sig udstillet, udnyttet eller krænket. Billederne skal således være harmløse.

Elektronisk borgerbetjening

Tilsynet har ved sine inspektioner set og påtalt enkelte eksempler på, at myndigheder transmitterede fortrolige personoplysninger over internettet - uden at have iagttaget persondatalovens krav om beskyttelse af oplysningerne med passende sikkerhedsforanstaltninger.

Datatilsynet har i praksis krævet, at der foretages kryptering ved transmission af fortrolige oplysninger og CPR-nummer over internettet. Ved transmission af følsomme oplysninger (omfattet af persondatalovens §§ 7 - 8) kræver tilsynet, at der foretages stærk kryptering ved anvendelse af en anerkendt krypteringsalgoritme. Datatilsynet finder ikke, at disse krav kan fraviges ved den registreredes samtykke.

Hjemmearbejdspladser og mobilt udstyr

Hjemmearbejdspladser og mobilt computerudstyr bliver anvendt i stigende omfang. Der er ofte i praksis etableret løsninger i forhold til sikring af kommunikation og begrænsning af adgang til data. Der ses dog eksempler på, at dataansvarlige myndigheder ikke som krævet i sikkerhedsbekendtgørelsen formelt har udformet særlige retningslinier på området. Sådanne retningslinier bør bl.a. omfatte emner som sikring af kommunikationen mellem hjemmearbejdspladsen og myndighedens systemer, sikring af data, der opbevares på hjemmearbejdspladsen, vedligeholdelse af antivirusprogrammel, regler for anden brug af hjemmearbejdspladsen end medarbejderens egen arbejdsmæssige brug samt regler om udskrivning, opbevaring og tilintetgørelse af udskrifter indeholdende personoplysninger. De sikkerhedsmæssige problemområder, som skal vurderes i forbindelse med pc-arbejdspladser uden for den dataansvarliges lokaliteter, er nærmere beskrevet i Datatilsynets vejledning til sikkerhedsbekendtgørelsen.

Trådløse netværk

Trådløse netværk er forbundet med en række sikkerhedsrisici afhængig af den benyttede standard og den specifikke konfiguration. Der kan således være en vis risiko for, at uvedkommende kan få adgang til personoplysninger, som transmitteres på det trådløse netværk. Ved anvendelse af trådløse netværk bør der derfor træffes særlige foranstaltninger med henblik på at sikre datas fortrolighed og integritet samt brugeres autenticitet på samme niveau som på et lukket kablet netværk. Det skal endvidere sikres, at eventuelle uvedkommende, som skulle få adgang til det trådløse netværk, ikke derved kan aflytte kommunikationen og opsnappe brugeridentifikationer og dertil hørende fortrolige adgangskoder, som anvendes i forbindelse med autoriserede brugeres adgang til personoplysninger.

Anvendelsen af og interessen for trådløse netværk er stigende. Det er dog ikke tilsynets indtryk, at trådløse netværk endnu er særlig udbredt hos offentlige myndigheder. Enkelte overvejer at anskaffe trådløse netværk f.eks. til undervisnings- og mødeformål.

Uddybende sikkerhedsregler

De dataansvarlige følger i langt de fleste tilfælde god praksis i forhold til it-sikkerhed. Tilsynet har dog i flere tilfælde konstateret manglende, mangelfulde eller forældede uddybende sikkerhedsregler hos offentlige myndigheder. Der er set eksempler på, at emner, for hvilke der i henhold til sikkerhedsbekendtgørelsen skal fastsættes interne regler, helt er forbigået, og at interne uddybende regler ikke har været tilstrækkelig detaljerede. Formålet med de uddybende sikkerhedsregler er at beskrive, hvordan myndigheden i praksis lever op til sikkerhedsbekendtgørelsens krav. De uddybende sikkerhedsregler skal således beskrive eller referere til beskrivelser af ansvarsforhold, etablerede sikkerhedsforanstaltninger, arbejds gange osv.

Besigtigelse af fysisk sikkerhed

I tilsynets inspektioner indgår oftest en besigtigelse af publikumsområder, serverrum og arkiver, hvor der behandles eller opbevares personoplysninger. I publikumsområder ses der i en del tilfælde printere og fax-maskiner, som er opstillet på en måde, der gør det let for uvedkommende at læse eller tilegne sig udskrifter med personoplysninger.

Der er ofte ved sådanne maskiner opstillet en papirkurv, og der er set nogle få eksempler på, at frit tilgængelige og åbne papirkurve har indeholdt kasserede udskrifter med følsomme personoplysninger, som uvedkommende meget let har kunnet fjerne.

Oversigt over udførte inspektioner i 2002

På nedenstående oversigt er der indsat markeringer "i" ved de inspektioner, som har givet Datatilsynet anledning til at underrette kommunalbestyrelsen/ amrådet eller en overordnet myndighed om Datatilsynets konstateringer.

Får så vidt angår årets politiinspektioner bemærkes, at der som opfølgning er sendt en samlet orientering til Rigspolitechefen. Markeringen ud for de enkelte politiembeder er således ikke nødvendigvis udtryk for, at persondatalovens regler ikke har været fulgt.

Staten

- AF regionskontor Nordjylland
- Beredskabsstyrelsen
- i Den sociale Sikringsstyrelse
- Flygtningenævnets sekretariat
- i Jernbanetilsynet
- Københavns Overpræsidium
- i Københavns Politi, Station C
- Københavns Universitet
- Nordjyllands Statsamt
- i Politimesteren i Esbjerg
- i Politimesteren i Fredericia
- i Politimesteren i Frederikshavn
- i Politimesteren i Gråsten
- i Politimesteren i Haderslev
- i Politimesteren i Helsingør
- i Politimesteren i Hjørring
- i Politimesteren i Horsens
- i Politimesteren i Kolding
- i Politimesteren i Middelfart
- i Politimesteren i Ribe
- Politimesteren i Ringsted
- i Politimesteren i Sønderborg
- i Politimesteren i Tønder
- i Politimesteren i Aalborg
- Rigspolitechefen (Afdeling A)
- Statsadvokaten for København
- i Statsfængslet i Horsens
- SU-Styrelsen
- AAU (Aalborg Universitet)

Kommuner og amter:

- Augustenborg
- Ballerup
- Bov
- i Brovst
- Brøndby
- Brønderslev
- Brørup
- Dragør
- Dronninglund
- i Fjerritslev
- Frederiksborg Amts Misbrugscenter
- Frederikshavn
- Greve
- i Gråsten
- Gundsø
- i Haderslev
- Hals
- Hedensted
- Hirtshals
- Hjørring
- Højer
- i Høje-Taastrup
- Juelsminde
- Københavns Kommune, Familie- og arbejdsmarkedsforvaltningen
- Københavns Kommune, Sundhedsforvaltningen
- Københavns Kommune, Økonomiforvaltningen
- i Køge
- i Lejre
- Løkken-Vrå
- Nordjyllands Amt
- Roskilde
- i Rødding
- i Sejlflod
- Sydals
- i Sønderborg
- i Sønderjyllands Amt
- Tønder
- Vallø
- i Aabenraa
- Ålborg

Offentlige sygehuse

H:S - Amager Hospital (generelt)
H:S - Bispebjerg Hospital (generelt)
H:S - Rigshospitalet - "Traumecenteret Rigshospitalet"
Hillerød Sygehus (generelt)
Køge Sygehus
Roskilde Sygehus
Sønderborg Sygehus

Private forskere

Adm. Overlæge Morten Bagge Hansen, Glostrup
Asbjørn Mohr Drewes, Aalborg Sygehus Syd
Elisabeth Carlsen, Rigshospitalet (to projekter)
Gunnar Lauge Nielsen, Aalborg Sygehus Nord
Henrik Lajer, Rigshospitalet (to projekter)
Karsten Haderup, Aalborg Psykiatriske Sygehus
Kjeld Reinert, Aalborg Psykiatriske Sygehus
Klinisk ass. Jessica Carlsson, København Ø
Lars Westergaard, Rigshospitalet -
Mette Holm, Rigshospitalet (to projekter)
Mie Aarup, prakt. læge
Overlæge Ebbe Lindegaard Madsen, Sønderborg
Overlæge Per Lykke Gregersen, Sønderborg
Overlæge Peter Lund Petersen, Sønderborg
Overlæge, dr.med Mogens Fenger,
Klinisk Biokemisk Afdeling, Hvidovre Hospital - "MONI-BANK"
Overlæge, dr.med Mogens Fenger,
Klinisk Biokemisk Afdeling, Hvidovre Hospital - "ENDOBANK"
Proj.kons. Gert Allan Nielsen, København Ø
Reimar Wernich Thomsen, Aalborg Sygehus Nord
Rikke Landholdt, Aalborg Sygehus
Stud.Scient. Bioc. Thomas Larsen, Frederiksberg
Ulrik Tage-Jensen, Aalborg Sygehus Syd (to projekter)

Øvrige private

Amager Kort
Dandy
Dankort A/S
Danris/Fremtiden (Ruds Vedby)
Dansk Forening for International Motorkøretøjsforsikring
Dansk Røde Kors Asylafdeling
DSB/Jysk Kontrolcenter
Forbrugsforeningen
Købmandstandens Oplysningbureau A/S
Redens Kvindekollegium
Rødovre Centrum Konto
Sonofon (personalearkiv)
STOP I/S
Zürich Forsikring

