Datatilsynets årsberetning 2003

DATATILSYNET

Datatilsynets årsberetning
2003

Udgiver: Datatilsynet
Design: Kontrast design
Tryk: TrykNet
Beretningen er sat med Meta
Oplag: 600
Oktober 2004
ISSN: 1601-5657
ISBN: 87-989860-1-5

Indhold

Til Folketinget

Hermed afgiver Datatilsynet sin årsberetning for 2003.

2003 var det 25. år med persondatabeskyttelse i Danmark, idet de første love om persondatabeskyttelse - lov om offentlige myndigheders registre og lov om private registre mv. - trådte i kraft den 1. januar 1979. Denne årsberetning er således den 25. i rækken. De første 21 blev udgivet af Registertilsynet, som blev afløst af Datatilsynet i forbindelse med ikrafttrædelsen af lov om behandling af personoplysninger (persondataloven) pr. 1. juli 2000.

Beretningen afgives i henhold til § 65 i persondataloven, hvorefter Datatilsynet afgiver en årlig beretning om sin virksomhed til Folketinget.

Beretningen indeholder en beskrivelse af Datatilsynets aktiviteter i 2003 og 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.

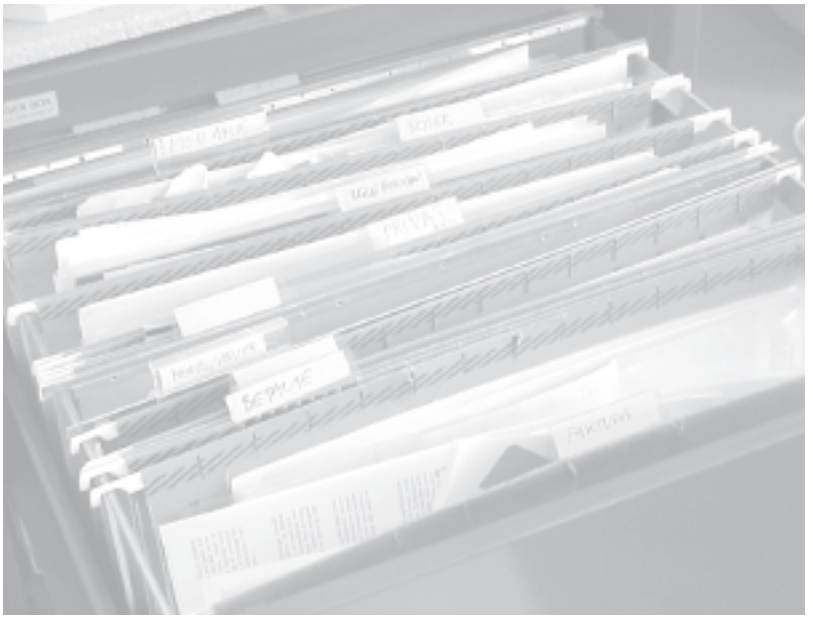
I afsnittet om tilsynsvirksomhed omtales de inspektioner (kontrolbesøg), som Datatilsynet har foretaget i årets løb.

Beretningen indeholder endelig også et afsnit om jubilæumskonferencen den 5. februar 2004 i anledning af de første 25 år med persondatabeskyttelse i Danmark.

København, september 2004

Asbjørn Jensen
Formand for Datarådet

Janni Christoffersen
Direktør



Datatilsynets virksomhed i 2003

Datatilsynets virksomhed i 2003

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 2003 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 mv.
- 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 mv.
- Sager på tilsynets eget initiativ, herunder inspektioner hos offentlige myndigheder samt hos en række private virksomheder og forskere
- Planlægning og afholdelse af jubilæumskonference
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsynsmyndigheder
- Deltagelse i arbejdsgrupper
- Registertilsyn for Grønland

Udtalelser om lovforslag mv.

Blandt opgaverne kan fremhæves, at Datatilsynet efter persondataloven skal høres over udkast til bekendtgørelser, cirkulærer o.l. generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger. Tilsynet bliver også hørt over lovforslag, direktivforslag og betænkninger mv. på dette område.

Datatilsynet oplever et stadigt stigende antal sager i denne kategori (109 registrerede nye sager i 2003 mod 66 i 2001 og 94 i 2002). 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.

Datatilsynets udtalelser over lovforslag mv. giver bl.a. Folketinget viden om, hvilke konsekvenser for databeskyttelsen et lovforslag har. Tilsynets høringssvar udgør således et bidrag til grundlaget for den politiske beslutningsproces. Efter Datatilsynets opfattelse er denne opgave vigtig, dels fordi tilsynet

er i besiddelse af ekspertviden om databeskyttelse, dels fordi tilsynet efter persondatalovens § 56 udøver sine funktioner i fuld uafhængighed. Datatilsynet anvender derfor stadigt flere af sine ressourcer på dette område.

Rådgivning og vejledning

Tilsynet yder desuden råd og vejledning til myndigheder og virksomheder. Det er tilsynets erfaring, at det ofte er en god ide, at tilsynet tages med på råd tidligt i et forløb, således at der tages højde for persondatalovens krav i det videre arbejde med et projekt. Herudover er der af og til også behov for dialog på senere stadier. At yde råd og vejledning er derfor også en central og prioriteret opgave for tilsynet. Hertil kommer, at tilsynet i forbindelse med en række initiativer til fremme af elektronisk borgerservice i det offentlige har påtaget sig opgaven som central godkendelsesinstans. Når andre myndigheder etablerer selvbetjeningssystemer på internet o.l., yder Datatilsynet således vejledning om, hvordan sikkerheden skal være for at beskytte oplysningerne.

Klagesagsbehandling

Herudover modtager Datatilsynet en del forespørgsler og klager fra registrerede personer. Tilsynet vejleder således de registrerede om deres rettigheder og om, hvad der i øvrigt gælder efter persondataloven.

I klagesagerne træffer Datatilsynet egentlige afgørelser om, hvorvidt en behandling er i overensstemmelse med loven. Det er selvsagt af afgørende betydning, at borgere, der er udsat for behandling af oplysninger i strid med loven, eller som f.eks. ikke får de oplysninger, de har krav på efter reglerne om de registreredes rettigheder, kan få Datatilsynets vurdering af forholdet. Datatilsynet har hidtil ikke i praksis oplevet problemer med at få den dataansvarlige myndighed eller virksomhed til at efterkomme tilsynets afgørelser.

Tilsynet har registreret en lille stigning i antallet af klager vedrørende offentlige myndigheder (fra ca. 140 til ca. 165), mens niveauet er uændret i forhold til de private dataansvarlige. Andelen af klager, som var berettigede, udgjorde ca. 40 % af de sager, som tilsynet afsluttede vedrørende private dataansvarlige, og ca. 18 % af de sager, som tilsynet afsluttede vedrørende offentlige myndigheder. De tilsvarende tal var i 2002 ca. 39 % og ca. 11 %.

Sager af egen drift

Ud over de sager, som rejses ved klager og forespørgsler, tager Datatilsynet også sager op på eget initiativ. Datatilsynet har i 2003 registreret 114 sager rejst på tilsynets eget initiativ, hvilket svarer til niveauet i 2001, mens der i 2002 blev registeret 202 sager. Dette tal omfatter såvel inspektioner, der omtales nærmere nedenfor, som andre "egen driftssager". Det forholdsvis høje antal sager i denne kategori i 2002 hang sammen med, at tilsynet i det år

gjorde en særlig indsats i forhold til myndigheder, som ikke havde efterlevet persondatalovens krav om anmeldelse til Datatilsynet.

I 2003 har Datatilsynet gennemført 71 inspektioner, heraf 41 hos offentlige myndigheder og 31 hos forskellige private virksomheder. Dette svarer til niveauet i 2001, mens der i 2002 blev gennemført i alt 116 inspektioner. Som følge af besparelser har Datatilsynet set sig nødsaget til at begrænse antallet af årlige inspektioner, og der må forventes en nedgang i antallet også i de kommende år, hvor tilsynets bevilling vil blive yderligere beskåret. I 2003 gennemførte Datatilsynet bl.a. en særlig inspektionsrunde i Lolland/Falster-området. Datatilsynets inspektioner er nærmere beskrevet i afsnittet om tilsynsvirksomhed.

Anmeldelser og tilladelser

Datatilsynet har også i 2003 behandlet mange anmeldelser og ansøgninger om tilladelser. Der er sket et fald i forhold til 2002 for så vidt angår anmeldelser for den offentlige forvaltning, hvilket er naturligt set i lyset af, at persondataloven nu har været i kraft nogle år, og myndighederne således i vidt omfang har fået anmeldelserne til Datatilsynet på plads.

Antallet af anmeldelser fra private dataansvarlige svarer stort set til antallet af anmeldelser i 2002. Dette hænger navnlig sammen med, at anmeldelsesordningen på forskningsområdet administreres således, at en privat forsker ikke kan foretage en generel anmeldelse af sine aktiviteter, men skal indsende anmeldelse til Datatilsynet, hver gang den pågældende påbegynder et nyt projekt. Antallet af nye sager om anmeldelse af private forsknings- og statistikprojekter er steget fra 938 i 2002 til 983 i 2003. Herudover sker der løbende ændringer i de anmeldelser, som allerede er modtaget. F.eks. når et projekt udvides, eller der kommer en ny databehandler ind i billedet, eller der er behov for at forlænge projektet ud over den oprindeligt forudsete periode. I 2003 har Datatilsynet modtaget ca. 900 ændringer til eksisterende anmeldelser af private forsknings- og statistikprojekter.

Anmeldelsesordningen er nærmere omtalt på Datatilsynets hjemmeside og i afsnittet "Anmeldelser fra myndigheder og virksomheder mv." i Datatilsynets årsberetning for 2001.

Tv-overvågning

I 2003 har Datatilsynet behandlet en del sager om tv-overvågning. Persondataloven sætter grænser for, hvor tv-overvågning må foretages, og hvordan det kan ske. I Datatilsynets praksis vedrørende tv-overvågning er billeder af både personale, kunder, elever og andre tilstedeværende blevet anset for at være personoplysninger omfattet af loven. I 2003 har Datatilsynet bl.a. udtalt, at princippet om god databehandlingsskik medfører, at der i forbindelse med tv-overvågning i kontroløjemed som den absolutte hovedregel skal gives forudgående information til de ansatte. Ved vurderingen af, om der kan ske fravigelse af denne hovedregel, må de hensyn, der kan begrunde fravigelse af op-

lysningspligt inddrages. Det vil sige, der skal være afgørende hensyn til private eller offentlige interesser.

Datatilsynet har også taget stilling til en række spørgsmål vedrørende offentlige myndigheders tv-overvågning med brug af digitalt udstyr. Datatilsynet finder bl.a., at en offentlig myndighed ikke bør tv-overvåge områder, hvor der er adgang for almindelig færdsel. Dette svarer til den hovedregel, der gælder for private virksomheder, butikker mv. En myndighed, der vil foretage tv-overvågning for at forebygge og afsløre kriminelle aktiviteter, skal først sende en anmeldelse til Datatilsynet, og Datatilsynets udtalelse skal foreligge, inden overvågningen går i gang. Datatilsynet opfordrer via sin hjemmeside alle myndigheder, som benytter digitalt udstyr i forbindelse med tv-overvågning, til at få anmeldelsen til Datatilsynet bragt i orden. Der henvises i øvrigt til afsnittet om sager om behandling af personoplysninger.

Herudover har Datatilsynet også i 2003 taget stilling til spørgsmål om offentliggørelse på internet. Dette gælder bl.a. oplysninger i form af billeder fra web-kameraer forsynet med zoom-funktion, oplysninger på debatsider på internet og oplysninger om grunde, der er omfattet af amtets kortlægning vedrørende forurening. Disse sager er nærmere omtalt i afsnittet om sager om behandling af personoplysninger.

Internationalt samarbejde

Datatilsynets deltagelse i internationalt samarbejde er fortsat et område, der vokser i 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 2003 har Datatilsynet desuden deltaget i den ny fælles tilsynsmyndighed i forhold til Eurojust. Aktiviteterne i de fælles tilsynsmyndigheder omtales nærmere i afsnittet om internationale sager.

I 2003 blev det 25. internationale møde for datatilsynsmyndighederne arrangeret af det australske datatilsyn og afholdt i Sydney, hvor der blev sat fokus på uafhængige tilsynsmyndigheders rolle og beskyttelse af personoplysninger i internationale sammenhænge. Ved samme lejlighed afholdt de europæiske databeskyttelseskommissærer et lukket møde, der bl.a. resulterede i udtalelser vedrørende overførsel af oplysninger om passagerer, RFID ("radio-frequency identification"), forbedring af kommunikation af praksis vedrørende databeskyttelse, automatisk software opdatering og databeskyttelse og internationale organisationer.

Andre opgaver

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.

Datatilsynets organisation

Datatilsynet består af et råd - Datarådet - og et sekretariat. Datatilsynet udøver sine funktioner i fuld uafhængighed, men har en finanslovsmæssig 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 2003

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.

Der har i 2003 været en forholdsvis stor udskiftning blandt de juridiske medarbejdere, bl.a. fordi flere fuldmægtige har forladt tilsynet på grund af et planlagt videre uddannelsesforløb.

Ansatte i sekretariatet

Pr. 31. december 2003

Direktør, cand. jur. Janni Christoffersen
Kontorchef, cand. jur. Lena Andersen
IT-chef, civilingeniør Ib Alfred Larsen
Konsulent, akademiingeniør Robert Hartmann Pedersen
IT-sikkerhedskonsulent Nils Rasmussen
Specialkonsulent, mag.art. Camilla Daasnes
Fuldmægtig, cand. jur. Bettina Agerskov (orlov)
Fuldmægtig, cand. jur. Maiken Christensen Breüner
Fuldmægtig, cand. jur. Kira Kolby Christensen (orlov)
Fuldmægtig, cand. jur. Lena Bjerregaard Danvøgg (orlov)
Fuldmægtig, cand. jur. Stine Dyhr
Fuldmægtig, cand. jur. Ditte Friis-Pedersen
Fuldmægtig, cand. jur. Anette Gramstrup
Fuldmægtig, cand. jur. Helene V. Grønfeldt
Fuldmægtig, cand. jur. Anders Ankerstjerne Hansen
Fuldmægtig, cand. jur. Lene Engedal Kragelund
Fuldmægtig, cand. jur. Camilla Sonne Kristensen
Fuldmægtig, cand. jur. Jakob Gøtze Pedersen
Fuldmægtig, cand. jur. Frederik Siegumfeldt
Fuldmægtig, cand. jur. Christian Wiese Svanberg
Fuldmægtig, cand. jur. Ane Holland Sørensen

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

Stud. jur. Marie Gjesing Fynsk (orlov)
Stud. jur. Rikke Lundby Jensen
Stud. jur. Karina Kok Jørgensen
Stud. jur. Malene Lybæk Møller
Stud. jur. Thomas Impgaard Sørensen (orlov)

Persondataloven

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.

Datatilsynets hjemmeside

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 2003 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 2003 var der i alt ca. 3.170 abonnenter på Datatilsynets hjemmeside mod 2.700 abonnenter i 2002.

Statistiske oplysninger

Oplysningerne i dette afsnit er baseret på registreringerne af nye sager i tilsynets journalsystem i 2003. 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. Dog kan det konstateres, at Datatilsynet i 2003 har modtaget ca. 900 ændringer til eksisterende anmeldelser af private forsknings- og statistikprojekter.

Datatilsynet registrerede 3.521 nye sager i perioden 1. januar 2003 til 31. december 2003. Disse sager fordeler sig som følger:

Datatilsynets egen administration mv.	223
Lovforberedende arbejde	109
Forespørgsler og klager vedrørende private	415
Forespørgsler og klager vedrørende offentlige myndigheder	495
Anmeldelser for den private sektor	1.227
Anmeldelser for den offentlige forvaltning	743
Sager på Datatilsynets eget initiativ	114
Sikkerhedsspørgsmål	26
Internationale sager	151
Kompetence i henhold til anden lovgivning	18

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

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 415 sager med forespørgsler og klager vedrørende private dataansvarlige.

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

Klager	ca. 29 %
Forespørgsler	ca. 71 %

Endvidere kan det oplyses, at i de afsluttede sager var ca. 40 % af klagerne berettigede, mens resten var uberettigede.

Sagerne var fordelt på følgende virksomhedstyper:

Almindelige virksomheder	65
Den finansielle sektor	36
Fagforeninger, a-kasser, pensionskasser mv.	15
Telesektoren	43
Foreninger og organisationer	34
Sundhedssektoren (medicinalvirksomheder, klinikker, læger mv.)	15
Kreditoplysningsbureauer	63
Advarselsregistre	15
Stillingsbesættende virksomheder	0
Ansøgninger om tilladelser	54
Diverse	74
Sager af generel karakter	1

Forespørgsler og klager vedrørende offentlige myndigheder

Datatilsynet registrerede i alt 495 sager med forespørgsler og klager vedrørende offentlige myndigheder.

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

Klager	ca. 33 %
Forespørgsler	ca. 67 %

I de afsluttede sager var ca. 18 % af klagerne berettigede, mens resten var uberettigede.

Sagerne var fordelt således:

Statslige myndigheder	269
Amtskommuner	21
Kommuner	103
Ansøgning om tilladelser	87
Diverse	14
Sager af generel karakter	1

Anmeldelser for den private sektor

Datatilsynet registrerede i alt 1.227 sager om anmeldelser. Fordelingen af sagerne var følgende:

Forskning og statistik	983
Privates behandling af oplysninger om rent private forhold	181
Advarselsregistre	3
Spærrelister	15
Kreditoplysningsbureauer	2
Stillingsbesættende virksomheder	17
Edb-servicebureauer	26
Diverse sager af generel karakter	0

Anmeldelser for den offentlige forvaltning

Datatilsynet registrerede i alt 743 sager om anmeldelser. Fordelingen af sagerne var følgende:

Fællesanmeldelser	1
Kommuner	261
Amtskommuner	121
Statslige myndigheder	183
Tilslutninger til fællesanmeldelser fra kommuner	158
Tilslutninger til fællesanmeldelser fra amtskommuner	2
Tilslutninger til fællesanmeldelser fra statslige myndigheder	17
Diverse/sager af generel karakter	0

Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 114 sager oprettet på tilsynets eget initiativ. Sagerne var fordelt på følgende sagstyper:

Inspektion og kontrol vedrørende private	32
Inspektion og kontrol vedrørende offentlige myndigheder	47
Sager rejst på grundlag af presseomtale o.l.	30
Diverse/sager af generel karakter	5

Sikkerhedsspørgsmål

Datatilsynet registrerede i alt 26 sager under kategorien sikkerhedsspørgsmål. Fordelingen af sagerne var følgende:

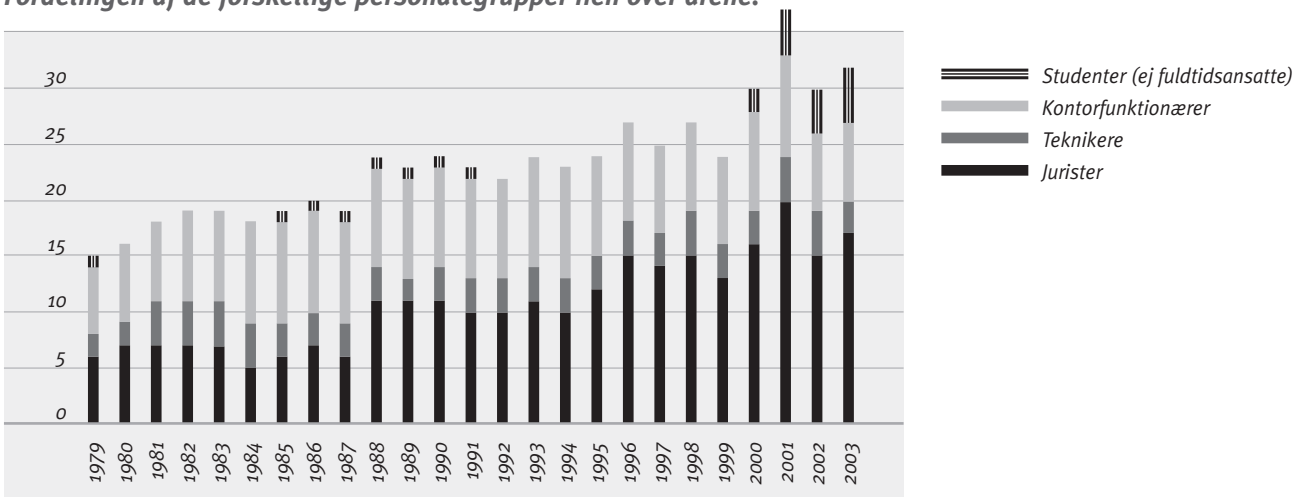
Sager vedrørende private	11
Sager vedrørende offentlige myndigheder	15

Internationale sager

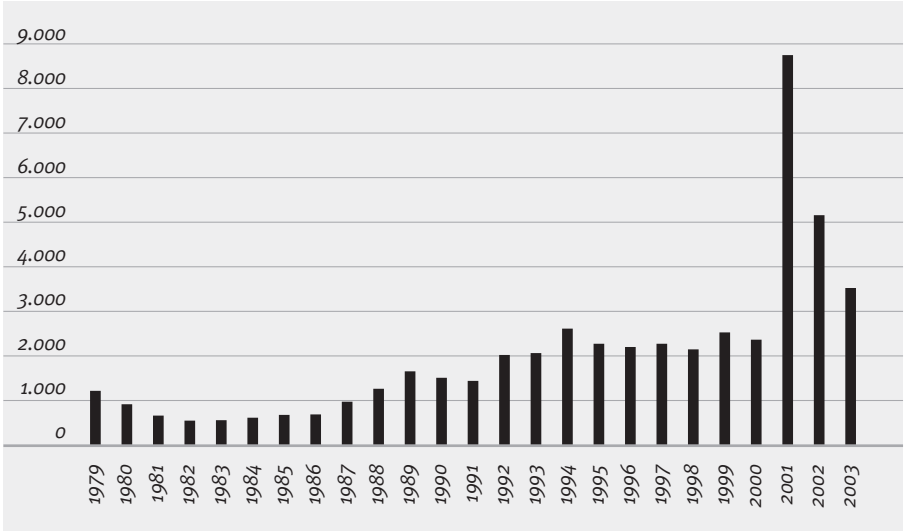
Datatilsynet registrerede i alt 151 internationale sager. Fordelingen af sagerne var følgende:

Forespørgsler fra udlandet om dansk lovgivning	56
Nordisk tilsynssamarbejde	5
Europarådet	1
EU	37
Konventioner	26
Datakommissærsamarbejdet	15
OECD	0
Diverse/sager af generel karakter	11

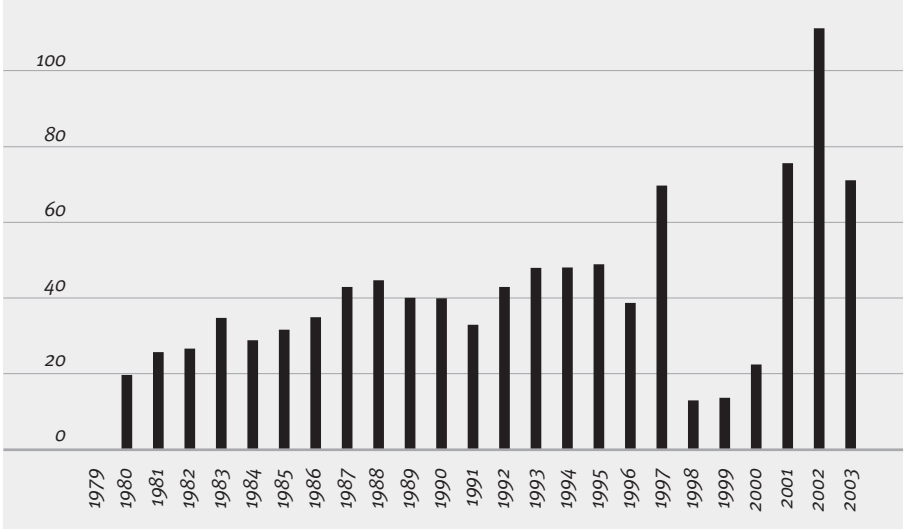
Fordelingen af de forskellige personalegrupper hen over årene.



Antal sager



Antal inspektioner



Datatilsynets jubilæumskonference

Datatilsynets jubilæumskonference

25 år med persondatabeskyttelse

Danmark var et af de første lande i Europa, som lovgav omkring beskyttelse af personoplysninger, da lov om offentlige myndigheders registre og lov om private registre mv. trådte i kraft den 1. januar 1979.

Den 1. juli 2000 blev de to registerlove afløst af lov om behandling af personoplysninger, og vi kunne således den 1. januar 2004 fejre 25 år med lovgivning om beskyttelse af personoplysninger.

Datatilsynet markerede dette med en jubilæumskonference den 5. februar 2004 i Landstingssalen. Konferencen, der blev åbnet af justitsminister Lene Espersen, satte bl.a. fokus på en række aktuelle emner inden for persondatabeskyttelsen.

Der var meget stor interesse for deltagelse i arrangementet fra private virksomheder, offentlige myndigheder, politikere og borgere. Da der imidlertid kun var plads til ca. 150 deltagere, måtte Datatilsynet desværre afvise mange interesserede.

Konferencen var bygget op med en række kortere indlæg med efterfølgende besvarelse af spørgsmål under hovedoverskrifterne status, overvågning i forskellige perspektiver og fremtidens udfordringer. Endvidere var der indlagt to sessioner, hvor der – under ledelse af ordstyrer Connie Hedegaard – blev debatteret ivrigt med deltagelse både fra salen og fra et panel bestående af oplægsholderne og Datatilsynets direktør Janni Christoffersen.

Datatilsynet takker alle, der bidrog til gennemførslen af en vellykket konference. En særlig tak til Grete og Sigurd Pedersens Fond for økonomisk støtte til arrangementet, som gjorde denne markering af jubilæet mulig.

Programmet for jubilæumskonferencen og en række af indlæggene gengives i det følgende.

Datatilsynets jubilæumskonference - 25 år med persondatabeskyttelse

torsdag den 5. februar 2004 i Landstingssalen, Christiansborg

09.00	*Velkomst*	ved direktør Janni Christoffersen, Datatilsynet
09.05	*Åbning*	ved justitsminister Lene Espersen
09.15	*Databeskyttelse – hvorfor og hvordan?*	ved formanden for Datarådet, højesteretsdommer Hugo Wendler Pedersen
09.35	*Service, effektivitet, kontrol og privatliv*	ved kommunaldirektør Estrid Oxlund, Holstebro Kommune
09.55	*Persondataloven – en barrierefor sygdoms- og sundhedsforskning nationalt oginternationalt?*	ved medlem af Datarådet, overlæge, afdelingschef Hans Henrik Storm, Forebyggelse & Dokumentation, Kræftens Bekæmpelse
10.15	*Kaffepause*	
10.45	*Persondatabeskyttelse i en international virksomhed*	ved General Counsel Christian Hartvig, Grundfos Management A/S
11.10	*Spiller persondataloven en hovedrolle eller en birolle i forhold til borgerens databeskyttelse?*	ved medlem af Datarådet, professor, dr.jur. Peter Blume, Retsvidenskabeligt Institut B, Københavns Universitet
11.30	*Debat med panelet*	Formiddagens foredragsholdere
12.00	*Frokostpause*	
13.00	*Overvågning – en politisk synsvinkel*	ved formanden for Folketingets Retsudvalg Anne Baastrup
13.15	*Privatlivet – et offentligt rum?*	ved direktør Johan Peter Paludan, Instituttet for Fremtidsforskning
13.30	*Overvågning i et arbejdsgiver-perspektiv*	ved juridisk direktør Kim Munch Lendal, Dansk Handel og Service
13.45	*Overvågning i et arbejdstager-perspektiv*	ved advokat Martin Gräs Lind, Schebye & Jacobsen
14.00	*Debat med panelet*	Eftermiddagens foredragsholdere
14.30	*Kaffepause*	
15.00	*Persondatabeskyttelse i et fremtidsperspektiv*	ved professor, dr. jur. Jon Bing, Institutt for rettsinformatikk, Universitetet i Oslo
15.25	*Den mobile identitet*	ved udviklingsdirektør Preben Mejer, TDC
15.50	*Afrunding*	ved direktør Janni Christoffersen, Datatilsynet

Dagens ordstyrer: Connie Hedegaard

De enkelte indlæg er gengivet med tilladelse fra oplægsholderne.

25 år med persondatabeskyttelse

Ved justitsminister Lene Espersen

1. Jeg vil gerne takke Datatilsynet for invitationen, der giver mig lejlighed til at indlede dagens konference.

Datatilsynet skal i den forbindelse også have særlig tak for at have taget initiativ til afholdelsen af denne jubilæumskonference - 25 år med persondatabeskyttelse. Hermed får vi mulighed for at markere, at vi nu i 25 år har haft lovgivning i Danmark om beskyttelse af personoplysninger. Og jeg kan se af det program, der er fastsat for konferencen, at der lagt op til nogle interessante timer, hvor deltagerne kan komme ind på et bredt spektrum af emner, der knytter sig til databeskyttelse.

2. 25 år er jo ingen alder. Men når det gælder lovgivning om persondatabeskyttelse, hører vi faktisk til blandt de ældre.

Danmark var et af de første lande i Europa, som lovgav om beskyttelse af personoplysninger. Det skete med vedtagelsen af lov om offentlige myndigheders registre og lov om private registre, der trådte i kraft 1. januar 1979.

Tilblivelsen af de 2 love var undervejs et stykke tid. Allerede i 1970 havde Justitsministeriet nedsat et udvalg benævnt "Registerudvalget". På baggrund af udvalgets betænkninger blev forslaget til de 2 registerlove fremsat i Folketinget og dernæst i 1977 vedtaget. Dermed var registerlovgivningen i Danmark en realitet.

3. Siden udgjorde de 2 love den retlige ramme for persondatabeskyttelsen – og dermed også grundlaget for den kontrol, der blev udøvet af Registertilsynet, som det dengang hed.

Vigtigt er det således at fremhæve, at lovgivningen om databeskyttelse og Registertilsynet – nu Datatilsynet - er lige gamle. Vores lovgivning om databeskyttelse har med andre ord i alle 25 år været underlagt en administrativ kontrol, der udøves uafhængigt af de politiske organer.

Det er selvfølgelig også værd at hæfte sig ved, at man tilbage i 1970´erne ikke talte om en persondatalov – men om en *register*lov. Fokus var således rettet mod systematiske fortegnelser og lignende, der kunne karakteriseres som et register. Det var her, at man først og fremmest så et behov for regler i lovgivningen, der bl.a. beskyttede enkeltindividets interesser.

4. I de forløbne år er fokus blevet bredt langt mere ud. I takt med den teknologiske udvikling har det klassiske registerbegreb ikke længere den samme betydning som omdrejningspunkt, når det gælder behovet for persondatabeskyttelse.

Denne udvikling viste sig navnlig, da de 2 registerlove i 2000 blev afløst – ikke af en ny registerlov, men af en ny samlet lov om behandling af personoplysninger, i daglig tale persondataloven. Og samtidig skiftede Registertilsynet helt naturligt navn til Datatilsynet.

Dette var en markering af, at behovet for persondatabeskyttelse i dagens moderne samfund har et langt bredere anvendelsesområde – og ikke blot er mere snævert knyttet til egentlige, traditionelle registre med personoplysninger.

Samtidig er persondataloven resultatet af en udvikling i retning af stigende internationalisering på området. Vores persondatalov er som bekendt i meget betydeligt omfang en implementering af reglerne i EU-direktivet fra 1995 om persondatabeskyttelse. Med vedtagelsen af dette direktiv blev det således tydeligt, at EU for alvor har betydning også på dette felt.

Formålet med databeskyttelsesdirektivet var – i hvert fald i mere snæver forstand – at fastsætte regler, der vedrører realisering af den fri bevægelighed mellem medlemslandene. Men direktivet har herigennem også mere generelt fået indflydelse på udformningen af reglerne om persondatabeskyttelse i vores lovgivning.

I den forbindelse er det efter min mening også værd at nævne, at direktivet – og i det hele taget den øgede internationale fokus på databeskyttelse – kan have medvirket til, at spørgsmålet om databeskyttelse er blevet sat på dagsordenen i en lang række lande – også i lande, hvor der ikke i forvejen var særlige traditioner på dette område.

5. Som sagt implementerede Danmark databeskyttelsesdirektivet med vedtagelsen af persondataloven i 2000. Forud var der en omfattende og langvarig proces i Folketinget. Jeg var i øvrigt selv med i denne proces. Så jeg kan bekræfte – hvad andre sikkert har sagt før mig – at det var kompliceret stof at skulle sætte sig ind i forslaget til den nye persondatalov.

Formålet med denne lov var jo ikke blot at implementere EU-direktivet i dansk ret. Et væsentligt formål med loven var også mere generelt at gennemføre en ny og tidssvarende lovgivning om behandling af personoplysninger i forhold til den tidligere gældende registerlovgivning.

I den forbindelse var det naturligvis afgørende at sikre et højt beskyttelsesniveau i forhold til den enkelte borger. Samtidig skulle loven skabe en fleksibel

ordning, som kunne danne rammerne for en hensigtsmæssig udnyttelse af den stadig større mulighed for at gøre personoplysninger til genstand for elektronisk behandling. Alt sammen afstedkommet af den teknologiske udvikling, som ingen vel havde kunne forestillet sig – og slet ikke tilbage i 1979, da den første registerlovgivning trådte i kraft.

6. Persondataloven har nu samlet de generelle regler om behandling af personoplysninger hos offentlige myndigheder og i den private sektor i én lov. En lov, der har betydning for utrolig mange af de aktiviteter, der foregår – både i det private og hos offentlige myndigheder. Og hvor det er en af Datatilsynets opgaver at formidle lovens regler videre ud i det praktiske liv, hvor det vel er de færreste, som er i stand til ved en gennemlæsning af persondataloven at opnå et fuldstændigt overblik over rettigheder og pligter på dette område.

7. Både for så vidt angår den offentlige og den private sektor foregår behandlingen af personoplysninger i dag i meget vidt omfang i elektronisk form. Papirsager, som vi kendte dem i gamle dage, hvor håndteringen af oplysninger foregik manuelt, bliver mindre og mindre udbredt.

Den teknologiske udvikling har uden tvivl gjort mange ting lettere i forbindelse med behandlingen og udvekslingen af personoplysninger.

Samtidig gør den stadig større mulighed for elektronisk udveksling – og dermed udbredelse - af personoplysninger, at det oftere og oftere kan være nødvendigt for f.eks. en privat virksomhed at forholde sig til konkrete og praktiske spørgsmål om databeskyttelse.

8. Man kan så stille det generelle spørgsmål: Hvad er det, der skal være vores overordnede retningslinier, når vi også fremover diskuterer databeskyttelse?

For mig er det i den forbindelse afgørende, at vi lader hensynet til privatlivets fred og den enkeltes integritet veje meget tungt. Enhver person har nogle grundlæggende rettigheder, der skal respekteres. Der kan ikke være ubegrænset adgang til at behandle oplysninger om en person – særligt ikke, hvis der er tale om følsomme oplysninger.

På den anden side er der hensynet til at sikre, at samfundet kan fungere effektivt. Der er et nødvendigt behov for, at offentlige myndigheder såvel som private kan foretage udveksling og behandling af personoplysninger, herunder til tider også følsomme oplysninger.

Også det indre marked og den stigende internationalisering hviler på en forudsætning om udveksling af oplysninger. Den fri bevægelighed for varer, per-

soner, tjenesteydelser og kapital forudsætter således, at personoplysninger kan cirkulere fra én medlemsstat til en anden. Og den økonomiske og sociale integration, der er en følge af hele den øgede globalisering, indebærer en stadig strøm af personoplysninger på tværs af landegrænserne.

Det er altså disse to grundlæggende hensyn, der står over for hinanden – på den ene side hensynet til den enkeltes integritet og på den anden side hensynet til det moderne samfunds behov for at kunne behandle og udveksle personoplysninger.

For at sikre, at begge disse hensyn tilgodeses på en hensigtsmæssig måde, er det afgørende at finde den rette balance mellem de to hovedhensyn. Det er alle vist enige om. Derimod kan der naturligvis være delte meninger om, hvor denne balance så ligger.

9. Efter min opfattelse er persondataloven et godt billede på, hvordan man kan skabe balance mellem de to hensyn. Jeg mener generelt, at vi med persondataloven har opnået en god balance mellem på den ene side hensynet til at sikre borgerne privatliv og integritet og på den anden side hensynet til i et moderne samfund at kunne udveksle en række personoplysninger inden for bl.a. den offentlige administration og det private erhvervsliv.

Som jeg antydede før, vil mange sikkert i den forbindelse være enige om, at persondataloven kan være temmelig kompliceret med mange og lange paragraffer. Her tror jeg, at man må sige, at dette vel delvist skal forklares med, at man netop har villet foretage en meget omhyggelig afvejning af de forskellige hensyn, jeg var inde på.

10. Databeskyttelsesområdet er et område, der vil blive ved med at være i stadig udvikling. Tænk i den forbindelse blot på, at der i 1995, da man vedtog EU-direktivet, nok ikke var mange, der kunne forudse, hvilken rivende udvikling der ville ske på dette område. Og i de små 4 år, vi har haft persondataloven, er der sandelig også sket meget. Tænk f.eks. på indførelsen af e-dag i det offentlige og på den fortsatte udvikling af det såkaldte papirløse samfund.

Så der er al mulig grund til med denne 25 års jubilæums konference ikke alene at se tilbage, men i mindst lige så høj grad at drøfte de udfordringer, som nutiden og fremtiden kan byde på. Og jeg kan da også af programmet se, at bl.a. persondatabeskyttelse i et fremtidsperspektiv er blandt de temaer, der vil indgå i dagens oplæg og diskussioner.

11. Jeg vil gerne slutte af med endnu en gang at takke Datatilsynet for invitationen og for det gode initiativ, som jeg synes, at denne konference er. Jeg håber, at dagen vil byde på en masse gode meningsudvekslinger, og at alle

vil få et stort udbytte af konferencen. Når jeg kigger på programmet, emnerne for oplæggene og de pågældende oplægsholdere, er jeg i hvert fald ikke i tvivl om, at der er lagt op til en spændende dag for deltagerne.

Databeskyttelse - hvorfor og hvordan?

Ved formanden for Datarådet, højesteretsdommer Hugo Wendler Pedersen

1. Indledning

Jeg har kaldt mit foredrag "Databeskyttelse - hvorfor og hvordan?"

Jeg vil forsøge at indkredse, hvilke hensyn der kan begrunde en beskyttelse af data.

Dernæst vil jeg i hovedtræk se på, hvorledes databeskyttelsen er udmøntet her i landet. Dels ved at se på, hvorledes databeskyttelseshensynet vægtes i forhold til andre konkurrerende hensyn. Dels ved at se på, hvordan databeskyttelsen praktisk gennemføres og håndhæves. Jeg vil ved denne gennemgang i alt væsentligt holde mig inden for de rammer, der afstikkes af den danske persondatalov fra 2000.

2. Hensynene bag databeskyttelse

Det naturlige udgangspunkt, når man vil forsøge at fastlægge hensynene bag databeskyttelse, må være at se på persondataloven. Denne lov indeholder imidlertid ikke en formålsbestemmelse, der angiver de bærende hensyn bag loven. Heller ikke forarbejderne til dataloven angiver mere præcist de overordnede beskyttelseshensyn bag loven.

Loven regulerer - bortset fra nogle få bestemmelser uden betydning i denne sammenhæng - behandling af personoplysninger. Herved forstås ifølge § 3, nr. 1: Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Lovens sigte er således at beskytte behandling af oplysninger om mennesker af kød og blod - ikke om bygninger, ting, dyr eller virksomheder (juridiske personer).

En belysning af formålene bag databeskyttelse får man, hvis man ser på Europaparlamentet og Rådets direktiv 95/46/EF af 24.10.1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Loven er baseret på dette direktiv. Loven bygger derudover i hovedsagen på de to tidligere registerlove: Lov nr. 293 af 8. juni 1978 om private registre og lov nr. 294 af 8. juni 1978 om offentlige myndigheders registre.

EF-direktivet har i artikel 1 en formålsbestemmelse, der siger:
"Medlemsstaterne sikrer i overensstemmelse med dette direktiv beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med personoplysninger."

I betragtning 10 til direktivet siges:
"Medlemsstaternes lovgivning om behandling af personoplysninger skal sikre overholdelsen af de grundlæggende rettigheder og frihedsrettigheder, navnlig den ret til privatlivets fred, der er fastslået i artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder ...".

I den europæiske menneskerettighedskonventions art. 8, stk. 1, siges:
"Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance."

I udkastet til Den Europæiske Unions Charter om Grundlæggende Rettigheder findes i artikel 8 følgende bestemmelse om beskyttelse af personoplysninger:
"Enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende. 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. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol."

Også forarbejderne til de tidligere registerlove indeholder bidrag til belysning af formålene bag databeskyttelse. I betænkning nr. 767/1976 om offentlige registre omtaler udvalgsbetænkningen den berømte amerikanske tidsskriftartikel fra 1890 om "The right to privacy", hvor det, der beskyttes, er en persons "interest in not having his affairs known to others or his likeness exhibited to the public", eller i kortere form "the right to be let alone". Udvalget forsøger selv at angive, hvad der menes med personlig integritet eller privatlivets fred. En væsentlig bestanddel heraf er ifølge udvalget:
"En retsbeskyttet adgang til at leve uden kontrol, indblanding eller overvågning på alle områder, hvor en sådan indblanding ikke er uskadelig eller pånøder sig af samfundsmæssige grunde."

Et aspekt af denne "interest in not having his affairs known to others" eller "right to be let alone" er personens ret til selv at bestemme over personlig information om ham. Undertiden har man talt om, at den enkelte person har ejendomsret til personlige informationer om ham selv. Synspunktet om den enkeltes selvbestemmelsesret vedrørende personlige oplysninger om ham selv har som konsekvens, at andre som udgangspunkt kun kan råde over personlige oplysninger om ham, hvis han giver samtykke hertil. Dette synspunkt har fået en betydelig gennemslagskraft i dataloven, der på en række

områder tillægger samtykke betydning. Ifølge § 3, nr. 8, forstås ved samtykke:
"enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling."

Der findes en omfattende litteratur, der forsøger nærmere at indkredse hensynene bag databeskyttelse. Den vil jeg ikke komme ind på i denne sammenhæng. Jeg vil alene nævne, at professor, dr.jur. Peter Blume, der er en af vores førende eksperter på databeskyttelsesområdet, senest i bogen: Databeskyttelsesret (Jurist- og økonomforbundet. 2000), s. 29, giver følgende definition af privatlivsbeskyttelsen af personlig data:
"Individet har ret til et privat informatorisk område, der tillader en sådan grad af kontrol og indflydelse, at individet kan deltage i den samfundsmæssige kommunikation og samtidig har en egen individualitet og fred i forhold til andre individer, offentlige myndigheder og private virksomheder."

Sammenfattende kan man vel sige, at det ikke er muligt helt præcist at angive hensynene bag persondatabeskyttelsen. Formålet er imidlertid at sikre den del af den enkeltes privatliv, der vedrører oplysninger om hans person, som han ønsker, at andre ikke skal have kendskab til. Beskyttelsen bygger på en antagelse om, at alle har en privat- eller intimsfære, som de ikke ønsker at andre invaderer. Beskyttelsen angår det, man har kaldt det informationelle privatliv.

Det er imidlertid klart, at hensynet til det informationelle privatliv må afbalanceres i forhold til en lang række konkurrerende hensyn og menneskelige behov.

Som man har sagt, har individet i dagens samfund ikke mulighed for eller ønsker om at få sit informationelle privatliv tilgodeset ved at blive "let alone" på en øde ø. Vi er alle borgere i et samfund, der har behov for informationer om os. Og vi har alle i vores daglige menneskelige samkvem behov for informationer om andre.

Det er der ikke noget nyt i.

Vores tidsregning starter faktisk med en begivenhed i forbindelse med dataregistrering. Der står i Lukas-Evangeliet kap. 2, vers 1:
"Men det skete i de Dage, at der udgik en Befaling fra Kejser Augustus, at al Verden skulle skrives i Mandtal".

Jeg vil i det følgende skitsere, hvorledes afvejningen mellem det informationelle privatliv og de konkurrerende hensyn er sket i persondataloven.

3. Persondataloven

3.1 Persondatabeskyttelsens tre hovedformer: Materielle regler, processuelle regler, datatilsyn

Persondataloven arbejder med et behandlingsbegreb, der er meget omfattende. Ifølge lovens § 3 forstås ved behandling:
"Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for."

En række konkurrerende hensyn har ført til, at visse former for behandling af personlige oplysninger helt er undtaget fra persondataloven.

3.1.1 Persondatabehandling, der ikke er omfattet af persondataloven

- Loven gælder ikke for behandlinger, der udføres for politiets og forsvarets efterretningstjenester (PET og FE).

PETs formål er "at overvåge, forebygge og modvirke handlinger, som må antages at rumme en fare for rigets selvstændighed og sikkerhed og den lovlige samfundsorden".

FEs opgave er "at indsamle, bearbejde og formidle informationer om forhold i udlandet af betydning for Danmarks sikkerhed, herunder for danske enheder mv. i udlandet."

Hensynene til disse overordnede demokratiske værdier er tillagt en sådan vægt, at persondatalovens regler ikke gælder.

De to tjenester er dog underlagt en række interne regler om behandling af personoplysninger.

Ved regeringserklæringen af 30. september 1968 blev det besluttet "at registrering af danske statsborgere ikke længere må finde sted alene på grundlag af lovlig politisk virksomhed."

I 1964 nedsatte regeringen det såkaldte "Wamberg-udvalg" – opkaldt efter udvalgets første formand – der har til opgave at føre tilsyn og kontrol med PETs registrering og videregivelse af oplysninger. FE blev i 1978 underlagt "Wamberg-udvalgets" arbejdsområde.

I 1988 blev der ved lov oprettet et særligt parlamentarisk udvalg med det formål at have indseende med PET og FE.

- Loven gælder ikke, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonvention artikel 10.

Ifølge art. 10 har enhver ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker uden indblanding fra offentlig myndighed og uden hensyn til landegrænser.

Denne ret anses for en så central frihedsrettighed i et demokratisk samfund, at hensynet til det informationelle privatliv må vige. Retten til ytringsfrihed er naturligvis heller ikke ubegrænset, men grænserne trækkes af anden lovgivning end persondataloven. I det indbyrdes forhold mellem borgerne først og fremmest af straffelovens kapitel om freds- og æreskrænkelser, navnlig racismebestemmelsen i straffelovens § 266 b og injuriebestemmelsen i § 267.

- Loven gælder – bortset fra nogle få bestemmelser uden betydning i denne sammenhæng – ikke for behandling af oplysninger, som udelukkende finder sted i journalistisk øjemed eller udelukkende sker med henblik på kunstnerisk eller litterær virksomhed.

Retten til journalistisk og kunstnerisk ytringsfrihed anses for en så central rettighed, at hensynet til det informationelle privatliv må vige. Grænserne for ytringsfriheden sættes igen navnlig af straffelovens bestemmelser om freds- og ærekrænkelser.

- Loven gælder ikke for behandling af personoplysninger, der er omfattet af lov om massemediers informationsdatabaser.

Loven om massemediers informationsdatabaser (lov nr. 430 af 1. juni 1994) skelner mellem redaktionelle informationsbaser og offentligt tilgængelige informationsdatabaser.

En redaktionel informationsbase er en informationsdatabase, der kun er tilgængelig for massemediets journalister og redaktionsmedarbejdere. Der er ikke i loven fastsat nogen begrænsninger i de personoplysninger, der kan behandles i en sådan informationsdatabase.

Retten til informationsfriheden for massemedier (foretagender, der udgiver tekster, billeder og lydprogrammer, der periodisk udbredes til offentligheden, såfremt de har karakter af en nyhedsformidling, der kan ligestilles med en formidling, der er omfattet af nr. 1 eller nr. 2 (medieansvarslovens § 1), dvs. navnlig indenlandske periodiske skrifter og lyd- og billedprogrammer fra Danmarks radio mv.) anses for en så central frihedsret, at hensynet til det informationelle privatliv må vige.

- Loven gælder ikke for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter.

Betragtningen bag denne bestemmelse, der findes i EF-direktivet, er vel navnlig, at sådanne aktiviteter er relativt harmløse, og at en håndhævelse af lovens regler over for sådanne aktiviteter vil være praktisk umulig.

Med aktiviteter af rent privat karakter tænkes f.eks. på privat korrespondance og føring af adressefortegnelser over familie, venner, bekendte osv.

- På det offentlige område gælder loven kun for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Al anden ikke-elektronisk systematisk behandling på det offentlige område er undtaget fra lovens område. Det hænger sammen med, at reguleringen af behandling af personoplysninger i den almindelige sagsbehandling sker i forvaltningsloven og offentlighedsloven.

- Persondataloven er en lov, der kan fraviges ved andre love.

Det kan ske på to forskellige måder.

Det fremgår direkte af persondataloven, at dens regler fraviges, hvis regler i anden lovgivning giver den registrerede en bedre retsstilling.

Men anden lovgivning kan også give den registrerede en dårligere retsstilling.

Grænserne herfor sættes af EF-direktivet.

Peter Blume vil senere i dag komme ind på nogle af disse spørgsmål.

3.1.2 De materielle regler

3.1.2.1 De databeskyttelsesretlige grundprincipper

Navnlig persondatalovens § 5 indeholder nogle grundprincipper, der skal overholdes i forbindelse med al databehandling omfattet af loven.

- Efter lovens § 5, stk. 1, skal oplysninger behandles i overensstemmelse med god databehandlingsskik.

Det konkrete indhold af denne standard må som andre standarder, f.eks. om god markedsføringsskik, fastlægges i praksis.

I kravet om god databehandlingsskik ligger i hvert fald, at en behandling udover at være lovlig også skal være rimelig og hensynsfuld. Behandlingen skal

ske såvel efter lovens bogstav som ånd. Hermed gives tillige et bidrag til fortolkningen af lovens øvrige bestemmelser. Bestemmelsen giver Datatilsynet en mulighed for at gribe regulerende ind over for databehandling, der ikke lever op til kravet om god databehandlingsskik.

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

Denne bestemmelse indeholder princippet om formålsbestemthed (finalitéprincippet).

For det første skal der i forbindelse med indsamlingen angives et formål, som er tilstrækkeligt veldefineret og velafgrænset til at skabe åbenhed og klarhed om behandlingen.

For det andet må de oplysninger, som er indsamlet, ikke frit genbruges eller videregives.

- Efter lovens § 5, stk. 3, skal oplysninger, som behandles, 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.

Hermed udtrykkes et relevans- eller proportionalitetsprincip.

Dette princip vender sig navnlig mod dataophobning og overskudsinformation.

- Efter lovens § 5, stk. 4, skal der foretages den fornødne ajourføring af oplysninger. Det skal sikres, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes.

Her udtrykkes princippet om datakvalitet, der skal sikre, at behandlede oplysninger er korrekte.

- Efter lovens § 5, stk. 5, må indsamlede oplysninger ikke opbevares længere end nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Hermed udtrykkes princippet om tidsbegrænsning, der navnlig er vendt mod dataophobning.

Efter lovens § 41 må kun dataansvarlige og andre, der er berettiget hertil, få kendskab til behandlede oplysninger.

Denne bestemmelse udtrykker princippet om behandlingssikkerhed, der forpligter den dataansvarlige til at sikre, at kun autoriserede personer får adgang til personoplysninger, og at behandlingen sker i overensstemmelse med formålet.

Man skelner mellem fysisk sikkerhed, hvorefter oplysningerne skal være placeret i lokaliteter, der ikke er frit tilgængelige og sikret mod brand o.lign.

Systemteknisk sikkerhed, der skal sikre mod indtrængning i systemerne.

Organisatorisk sikkerhed, der skal sikre, at den dataansvarliges personale omgår personoplysningerne med den fornødne fortrolighed.

For oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

3.1.2.2 Behandlingsbetingelser efter oplysningstyper

Lovens §§ 6 - 8 indeholder nogle centrale regler om betingelserne for behandling af personoplysninger. Betingelserne er fastsat under hensyn til de generelle integritetskrænkelsesrisici, der er forbundet med at behandle en oplysningstype. Desto større risiko for integritetskrænkelse, desto strengere betingelser for behandling.

Samtidig angiver disse bestemmelser forudsætningsvis, at personoplysninger kun må behandles, hvis der er lovhjemmel hertil.

§ 6 indeholder behandlingsbetingelserne for almindelige, ikke-følsomme oplysninger, dvs. alle andre oplysninger end om rent private forhold.

Her er behandlingsbetingelserne lempelige.

Det offentlige kan således eksempelvis behandle almindelige, ikke-følsomme oplysninger, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse.

En privat kan eksempelvis behandle oplysninger, hvis det er nødvendigt for at forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

§ 7 indeholder behandlingsbetingelserne for de særlige følsomme eller sensitive personoplysninger, dvs. oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

Udgangspunktet her er, at der gælder et forbud mod behandling af sådanne personoplysninger, og at behandling kun undtagelsesvis kan ske.

§ 8 indeholder behandlingsbetingelserne for de såkaldte semifølsomme personoplysninger, dvs. strafbare forhold, væsentlige sociale problemer og andre rent private forhold.

Behandlingsbetingelserne er her strengere end efter § 6 men lempeligere end efter § 7.

3.1.3 De processuelle regler

3.1.3.1 Reglerne om oplysningspligt over for den registrerede

Lovens §§ 28 og 29 indeholder regler om, at der ved indsamling af oplysninger skal gives nogle nærmere angivne oplysninger til den registrerede, således at den registrerede informeres om indsamlingen.

3.1.3.2 Reglerne om anmeldelse af behandlinger, der foretages for den offentlige forvaltning og for en privat dataansvarlig

I kapitel 12 og 13 findes nogle regler om anmeldelse til Datatilsynet. Udgangspunktet er, at anmeldelse skal ske til Datatilsynet, inden en behandling iværksættes. Anmeldelsen er offentlig tilgængelig. Formålet er først og fremmest at sikre gennemskuelighed og kontrol.

3.1.3.3 Den registreredes indsigtsret

Lovens §§ 31 - 34 indeholder bestemmelser om den registreredes indsigtsret.

Udgangspunktet er, at den registrerede skal have meddelelse om:

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

3.1.3.4 Den registreredes øvrige rettigheder

Efter lovens § 35 kan den registrerede til enhver tid gøre indsigelse mod, at oplysninger om ham gøres til genstand for behandling. Hvis indsigelsen er berettiget må behandlingen ikke længere omfatte de omhandlede oplysninger.

Efter lovens § 36 kan en forbruger fremsætte indsigelse mod, at en virksomhed videregiver oplysninger om den pågældende til en anden virksomhed med henblik på markedsføring.

Efter lovens § 37 skal den dataansvarlige berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lovgivningen, såfremt en registreret person fremsætter anmodning herom. Er oplysningerne videregivet til tredjemand, skal denne som udgangspunkt underrettes.

Efter § 38 kan den registrerede tilbagekalde et samtykke.

Efter § 40 kan den registrerede klage til en tilsynsmyndighed over behandling af oplysninger vedrørende den pågældende.

3.1.4 Datatilsynet

Det er almindeligt anerkendt, at det ikke er tilstrækkeligt at basere databeskyttelsesretten på en håndhævelse gennem det almindelige domstolssystem, men at håndhævelsen må ske gennem en særlig offentlig tilsynsmyndighed. Som følge af databeskyttelsesrettens brug af brede retsstandarder er der behov for et sagkyndigt håndhævelsesorgan, hvis reglerne skal håndhæves. Ifølge EF-direktivets art. 28 forpligter medlemsstaterne sig til at oprette en offentlig tilsynsmyndighed. I udkastet til Den Europæiske Unions Charter Om Grundlæggende Rettigheder art. 8 skal overholdelsen af reglerne om beskyttelse af personoplysninger være underlagt en uafhængig myndigheds kontrol.

I Danmark er den offentlige tilsynsmyndighed Datatilsynet. Datatilsynet er ligesom det tidligere Registertilsyn organiseret som én myndighed, der består af henholdsvis et sekretariat og et råd (Datarådet).

Sekretariatet, der varetager Datatilsynets daglige forretninger, er sammensat således, at det besidder såvel juridisk som edb-teknisk sagkundskab.

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

Rådet træffer først og fremmest afgørelse i sager af principiel karakter. Derudover behandler rådet bl.a. sager af betydelig almindelig interesse eller med betydelige følger for en offentlig myndighed eller privat virksomhed eller borger. Sekretariatet behandler de øvrige sager.

4. Sammenfatning

Retten til egne data er en informationel frihedsrettighed. Hensynet til det informationelle privatliv må imidlertid afbalanceres i forhold til en lang række andre rettigheder og menneskelige behov. Jeg har forsøgt at give et øjebliksbillede af, hvorledes det sker i Danmark i dag.

Databeskyttelsesretten er under stadig udvikling både nationalt og internationalt. Det er vigtigt løbende at drøfte, hvorledes denne frihedsret skal vægtes i forhold til en række konkurrerende hensyn, og hvilken betydning der skal gives databeskyttelsesretten.

Jeg håber, at vi her ved Datatilsynets jubilæumskonference kan få en drøftelse af dette vigtige spørgsmål og sammen vil få en udbytterig dag.

Persondataloven - en barriere for sygdoms- og sundhedsforskning nationalt og internationalt?

Ved medlem af Datarådet, overlæge Hans Henrik Storm

Vi har nu levet med regulering af brug og adgang til vores personlige data i 25 år, først gennem registerloven og nu persondataloven. Da den individ- og befolkningsbaserede forskning er foregået i hele perioden og faktisk er øget, er det umiddelbart let at svare på spørgsmålet i overskriften. Hvis der er skabt barrierer, så er de til at overvinde i Danmark, og i øvrigt i hele det nordiske område. Arbejdet med at overføre det europæiske direktiv for beskyttelse af persondata til dansk lov må nok betegnes som en succeshistorie. Den danske lov varetager både individets, samfundets og forskerens interesser. Problemerne ligger måske snarere i samarbejdet med andre lande og dermed den fri bevægelighed af data, som jo var anledningen til Direktivet.

Sygdoms- og sundhedsforskning har i årevis været underlagt frivillig regulering. På baggrund af de nazistiske overgreb blev Nürnberg kodex, der sikrer patienters og forsøgspersoners helt basale rettigheder, og at forskning foregår lovligt med en høj etik, moral og selvbestemmelse, etableret. World Medical Association har siden opdateret og erstattet kodex med de såkaldte Helsinki deklarationer, og senest har epidemiologerne specificeret, hvad de mener, der skal gælde for befolkningsbaseret forskning.

Problemet er at finde den rette balance mellem privatlivets fred og de gevinster, der er ved forskning. Risikoen for, at ens data bliver misbrugt, må opvejes mod de gevinster, forskningen kan tilføre samfundet, det enkelte menneske og hele menneskeheden. Og balancen rykker sig hele tiden. Etik og forskning er nært forbundet. Forskningen skal have sin frihed, men ingen forskning uden etik sagde Erling Tiedeman som formand for Etisk Råd. Han sagde også uden etik ingen forskning begrundet i Aristoteles definition, at

etik handler om det gode liv. Forskningen bidrager til, hvad der kan fremme det gode liv, og er dermed en del af dets grundlag.

For at forstå de problemer, der kan opstå for forskningen ved vores persondatalov, må vi se på de forskellige typer af sundhedsforskning, der berører os som personer. Den kliniske forskning, f.eks. forsøg med medicin eller anden behandling, interview og prøvetagning, kræver informeret samtykke fra den enkelte og overvåges både af det videnskabsetiske komitesystem, Datatilsynet og forvaltningen af lov om patientrettigheder. Den befolkningsbaserede forskning – epidemiologien – inddrager større befolkningsgrupper eller hele befolkningen. Ofte foretages den ved brug af eksisterende registre uden direkte patientkontakt. Den type forskning reguleres dels gennem bevillinger og peer review af protokoller dels af Datatilsynet, og hvis f.eks. informationer hentes fra hospitalsjournaler tillige af lov om patientrettigheder. De biologiske databanker er også persondata og kan finde anvendelse både i den kliniske og den epidemiologiske forskning, men tillægger en ekstra dimension af muligheder for at karakterisere os som personer. Både de generelle aspekter ved forskningen og de specielle, der relaterer sig til de tre ovennævnte scenarier, diskuteres her.

Informeret samtykke er det principielle og bærende element for persondatabeskyttelse. Selvbestemmelse og viden om, hvad der foregår med mine data, er en selvfølgelig grundregel. Men lige så meget som det er en ret til at vide, må det være en ret til ikke at gøre det, eller til at overlade kontrollen til nogen, man har tillid til, vil agere fornuftigt og varetage såvel ens egne interesser, som de interesser, det samfund man har valgt at være medlem af, har. Den mulighed eksisterer i vores persondatalov og reguleres yderligere i lov om patientrettigheder. Kort sagt, jeg behøver ikke at vide, hvilke sammenhænge mine data indgår i, jeg afsløres ikke som person i resultaterne, og jeg kan nøjes med at høste de frugter, der springer af forskningen. Jeg skal heller ikke tage stilling til sager, jeg ikke har forudsætning for at tage stilling til.

Forskerne har også fordel af, at en del af forskningen kan foregå uden samtykke. Man har større sikkerhed for, at de data, man har, er repræsentative uden bias – de skævheder, der kan komme gennem selekteret bortfald. Vi får både generaliserbare og solide konklusioner, der har størst mulig statistisk styrke. Komplethed af data er vigtig – ikke mindst da selv de enkelte sygdomme, som f.eks. kræft er sjældne, og kun få ekstra tilfælde er med til at bestemme, om der er en øget risiko i forhold til, hvad der ses normalt i befolkningen. Dertil kommer, at registerforskning i princippet bruger samtlige personers data – og dermed skulle alle meddele samtykke, hvilket er en fysisk umulighed.

Et par eksempler: En vurdering af overlevelse efter en kræftsygdom kræver, at vi kender den enkelte patients skæbne, behandling mv. Resultaterne deri-

mod offentliggøres grupperet ofte for hele Danmark samlet. Forskeren har alle individuelle forløb, men det interessante er det samlede billede ikke den enkelte person. Et andet eksempel er udnyttelsen af forskellige registre med historiske data. Er der risiko for stråleinduceret brystkræft, når vi begynder screening med røntgenundersøgelsen mammografi, og hvor stor er den? Vi tog et register med 46.000 tuberkulosepatienter, som blev gennemlyst hyppigt med røntgenstråler, og identificerede ved datakobling 1.500 personer, der senere udviklede kræftsygdom. Af dem havde 125 brystkræft. Vi kunne finde journaler på 89 og sammenlignede data med 390 tuberkulosepatienter uden kræft, men med samme alder og køn som de kræftsyge på tidspunktet for deres tuberkulose. For hver enkelt patient kunne vi fra journalnotater udregne den stråledosis, deres bryst havde fået. Resultatet viste ingen sammenhæng mellem stråledosis og brystkræft. Dvs. at stråledosis svarende til et helt livs mammografi ikke ville give en målbar forøgelse af brystkræftrisikoen. Resultatet baserer sig på enkeltpersoners data, men det er det samlede billede, der betyder noget.

Det, vi forsøger at forhindre, er "snagen" – unødig eksponering af vores privatliv. Flere har forsøgt at løse problemet teknisk, men her må man vurdere, hvad det er, man vil opnå. Tyskerne har med vanlig grundighed designet et kompliceret system for dataoparbejdning i f.eks. cancerregistre, som reelt indebærer, at koblingen mellem personidentifikation og medicinsk information tabes indenfor en 3 måneders periode. I betragtning af, at vi stadig retter observerede fejl i vores registre 20-30 år efter første inddatering, er et sådant set-up, om end principielt funktionsdueligt, bekymrende. Når den tyske forsker kommer med data om personer, han vil analysere for mulig sygdom, skal han have tillid til, at hele 3 instanser behandler data fejlfrit efter envejs anonymisering, så de anonymiserede data med både sygdomsinformation og udsættelse for mulige kræftfremkaldende agens kan analyseres med korrekt resultat. Yderligere indebærer systemet, at "den kriminelle forsker" ved ulovligt at koble tilbage til sine originaldata har mulighed for at bryde koden – så den tekniske løsning garanterer os ikke anonymitet. Systemet gælder ikke for klinisk arbejdende læger, så det er yderst begrænset, hvad man opnår i tillæg til en fornuftig lovgivning som i Danmark.

Databeskyttelsesdirektivet 95/46/EF skal sikre, at vi frit kan dele data inden for EU. Det er nu principielt muligt, men det har taget en del tid for landene at få etableret følgelovgivning og få den implementeret. Som det kan ses på http://europa.eu.int/comm/internal_market/privacy/index_en.htm, så mangler Frankrig fortsat at få vedtaget den nødvendige lovgivning, og Irland kom først med midt i 2003. Danmark var sammen med Luxembourg, Tyskland, Frankrig og Irland blandt de lande, Kommissionen ville retsforfølge for sendrægtighed. Det er klart, at manglende lovgivning og forskelle i tolkning og dermed følgelovgivningen er en barriere mod det helt nødvendige samarbejde på tværs af grænser, når det gælder forskning. Men når det er sagt, så er

persondataloven ingen barriere for forskningen. Den har derimod været nyttig. Forskerne har været tvunget til at skærpe formålsbeskrivelserne og forbedre databehandlingen. Arkiveringen er forbedret og gjort mulig på lang sigt. Biobanker kan nu udnyttes lovligt under de samme regler med lidt tillæg som andre persondata.

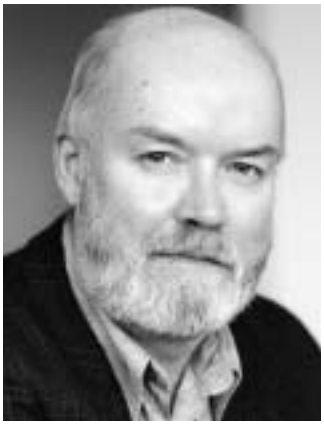
Men alt udvikler sig, og debatten om vores personlige data og beskyttelsen vil fortsætte. Der er stadig meget at tage stilling til som f.eks. den mulige krænkelse af privatlivet, når vi indlægges på et sygehus. En artikel i New England Journal of Medicine viste, at ca. 150 personer havde set en anden patients journal under indlæggelse.

Den nye genetiske forskning – Dolly syndromet – har på ny stimuleret debatten om vores arkiverede data, og både forskningen og debatten har været eksplosiv. Island har gennem "salget" af offentlige databaser til et privat firma, der kortlægger halvdelen af befolkningens gener i jagten på sygdomme og mulige moderne behandlinger, bragt diskussionen af brug af biologiske og andre arkiverede persondata ud til befolkningen. Og den debat er velkommen og nødvendig. Hvilken betydning det vil få, at mange har benyttet muligheden for, at deres data ikke indgår i forskningen, er svært at sige i dag. Men normalt er befolkninger positivt stemt over for forskning, som betragtes som samfundsnyttig. En canadisk undersøgelse viste, at 95 % havde fuld tillid, og kun en mindre del, de samme, som krævede total kontrol med miljø- og erhvervsmæssige udsættelser, krævede samtidig fuld fortrolighed og ingen invasion i privatlivets fred.

Jeg vil påstå, at vi ikke har et problem med forskningen, og Datatilsynet har da heller ikke i sin tid som Registertilsyn og Datatilsyn fundet alvorligt kritisable forhold hos forskerne. I den samme periode har der været uheldige sager fra dele af samfundet, der er undtaget fra Direktivets bestemmelser og persondataloven, hvilket burde bekymre. Forskerne har vænnet sig til kontrollen og åbenheden med, hvad de foretager sig. Anmeldelser af privat forskning er stigende, og alene i de sidste 3 år er der anmeldt svarende til halvdelen af, hvad der blev anmeldt på 12 år før den ny persondatalov. 90 % er lægevidenskabelig forskning, og 770 anmeldelser indebærer brug af biologiske data.

Persondataloven og administrationen af den i Danmark fungerer sammen med forskningen under hensyntagen til etik, fortrolighed og datasikkerhed. Borgerne har generelt tillid til Datatilsynet og andre myndigheder, til forskerne og forskningsinstitutionerne. Ikke mindst nyder vi godt af at være i et retssamfund.

Spiller personoplysningsloven en hovedrolle eller en birolle i forhold til borgernes databeskyttelse?[1]



Ved medlem af Datarådet, professor, dr.jur. Peter Blume

Et jubilæum er normalt en festlig dag, hvor jubilaren modtager lykønskninger. Det er ikke intentionen med det følgende at kaste malurt i bægeret eller at ødelægge den gode stemning, men dog at angive nogle lidt kritiske synsvinkler på, hvad det er for en lov(givning), som bliver fejret i dag. Hvad er det egentlig, den vil, og hvorledes bliver målet nået? Og i denne forbindelse hvad er Datatilsynets rolle.

1. Formålet

For den person, der første gang læser persondataloven, er et indledende naturligt spørgsmål, hvad mon denne lovs formål egentlig er? Det gives der ikke umiddelbart noget svar på, idet loven straks i § 1 går i gang med at fastlægge sit anvendelsesområde. Der er ikke nogen formålsbestemmelse. Den pågældende må derfor søge andre steder, og før man tager den besværlige vej ind i lovens forarbejder, er et naturligt sted direktiv 95/46 EF, der jo implementeres i loven, og her kan man i artikel 1 blive lidt klogere. Der synes her at være to formål, dels at der skal være fri dataoverførsel inden for EU, dels at borgernes grundlæggende rettigheder, specielt privatlivets fred, skal ydes beskyttelse. Ifølge EF-Domstolen er den frie dataoverførsel det centrale, hvilket skyldes, at direktivets traktatmæssige grundlag er det indre marked. Dette står der dog ikke noget om i loven, og man skal endda være lidt kvik for overhovedet ud fra lovteksten at finde ud af, at der er denne fri overførsel. Det andet mål, privatlivets fred, er for de fleste det mest nærliggende.

I lovens forarbejder[2] møder man en skuffelse. Der står ikke meget ud over, at loven skal sikre et fortsat højt beskyttelsesniveau, hvorved der blankt henvises til registerlovene, og endvidere skal udgøre en fleksibel ordning for en hensigtsmæssig udnyttelse af elektroniske persondata. Privatlivets fred er ikke omtalt, men som nævnt er det for mange nok nærliggende, at dette er formålet.

I de andre nordiske lande er der formålsbestemmelser i personoplysningsloven, som loven med et bedre udtryk end vores kaldes i disse lande, og den svenske kommer nok tæt på, hvad der kunne være skrevet i den danske lov. Det hedder i § 1, at "syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter". Beskyttelsen af borgernes integritet, sikring af privatlivet og værn mod misbrug af personlige oplysninger er alt i alt de formål, som de fleste forbinder med persondataloven. Det står altså ikke nogen steder, men det er en udbredt opfattelse.

Dette er jo ædle formål, men er det rent faktisk lovens formål, eller er det kun en lille del eller måske slet ikke nogen del af sandheden. Er man måske snarere tættere på, hvis formålet netop er den nævnte fleksible ordning og at

[1] *Manuskript som grundlag for indlæg ved jubilæumskonference 5. februar 2004.*

[2] *FT 1999-2000 A p.3990.*

opstille rammer, således at persondata bliver benyttet på en ordentlig måde. Er det måske mere rigtigt at opfatte loven som primært processuel, således at den skal sikre en civilisering af persondatabehandlingen. Også ganske ædelt, men dog ikke helt så ædelt. Efter min opfattelse er der her tale om en mere præcis beskrivelse af lovens formål, der danner en naturlig ramme for en drøftelse af, hvorledes lovens forhold til den øvrige lovgivning er. Det er dette forhold, som fortæller noget om, hvor stor en rolle loven faktisk spiller. Dele af dette forhold giver således kun mening, såfremt persondatalovens formål forstås på denne noget mere jordnære facon.

Der foreligger på dette område to problemstillinger, der må holdes ude fra hinanden. Den første vedrører forholdet til love med databeskyttelsesretlige regler, altså regler som har samme emne som loven. Den anden vedrører forholdet til love og andre retskilder med bestemmelser, der ikke har et databeskyttelsesretligt sigte.

2. Lovvalg

Jeg starter med den første og på sin vis letteste problemstilling, som vedrører lovvalg. Udgangspunktet er, at persondataloven som en almindelig lov ikke har større vægt end andre love. Direktivet fastlægger et bindende udgangspunkt, men direktivet behøver ikke kun at blive implementeret i én lov. Er direktivet respekteret afhænger valget mellem flere lovbestemmelser af almindelig juridisk metode, medmindre der fastsættes en styrende lovvalgsregel.

Efter § 2, stk. 1, går lovbestemmelser, som giver den registrerede en bedre retsstilling, forud for lovens regler. Det er ikke helt klart, hvorfor vi har denne regel, fordi den ville gælde alligevel, og specielt fordi den ikke skal forstås så bastant, som den er skrevet, og fordi den ikke bliver overholdt fuldt ud. Det er et velkendt offentligretligt princip, at er flere regler anvendelige, skal man vælge den, der giver det gunstigste resultat for borgeren. Det svære er at afgøre, hvad der er mest gunstigt, og når forarbejderne som et eksempel fremhæver patientretsstillingslovens videregivelsesregler som bedre end lovens, afhænger dette i mangt og meget af, hvilke øjne der læser de to love. Det er heller ikke udelukket, at en mindre god regel kan gå forud, bare dette har været lovgivers intention og ikke strider imod direktivet. Dette fremgår af forarbejderne til bestemmelsen og følger i øvrigt af elementær forfatningsret; det ene Folketing kan ikke binde det næste. Endelig har man formuleret forarbejderne således, at visse af forvaltningslovens regler, der giver en bedre retsstilling, alligevel ikke skal gå forud[3]. Lovens tilsyneladende klare regel giver reelt kun i beskedent omfang en retningspil for, hvorledes lovvalget skal træffes, og på mange måder er der tale om en overflødig regel.

I praksis er lovvalget ikke altid let, og det er ikke altid klart, hvorledes persondatalovens generelle bestemmelser og de specielle lovregler hænger sam-

3 Om det komplicerede forhold til forvaltningsloven se Jon Andersen, Juristen 2003 p.281-95.

men. Det må her fremhæves, at der findes ganske mange af disse regler på vidt forskellige områder. Til illustration kan nævnes bestemmelser i betalingsmiddelloven, lov om finansiel virksomhed, tinglysningsloven, lov om massemediers databaser, patientretsstillingsloven og arkivloven. Fra europæisk side har man ofte karakteriseret amerikansk lovgivning som et kludetæppe, men vi er faktisk også ret gode til at væve. Den sektororienterede lovgivning reducerer persondatalovens selvstændige område, men dette er dog ikke det mest tankevækkende ved den historie, som jeg prøver at fortælle i dag.

3. Anden ret

Af langt større praktisk og principiel interesse er det mere upåagtede spørgsmål om lovens forhold til den almindelige lovgivning, som ikke umiddelbart har en databeskyttelsesretlig karakter, og som jeg i det følgende har valgt at kalde anden ret. Denne problemstilling angår, om databeskyttelsen kun bestemmes af de databeskyttelsesretlige regler, eller om noget uden for dette univers også har betydning. Denne problemstilling har betydning både for forståelsen af persondatalovens formål og i forhold til mange borgeres barnetro på, hvad denne lov egentlig magter, og dermed også hvad Datatilsynet kan udrette.

Læser man loven igennem, kan man føle lidt uro, fordi der mange steder er referencer til noget, der ligger uden for loven. Det kan virke som om, at mange af lovens regler har en uselvstændig tilværelse og kun får deres mening, når de udfyldes med den anden ret. Det skal jeg nu illustrere, hvorefter jeg bagefter vil omtale nogle af de mulige konsekvenser, der er forbundet med denne retstilstand.

Anden ret spiller en rolle på forskellig måde, idet der dels kan være tale om, at der i persondatalovens regler er indsat en direkte reference hertil, eller at en sådan sammenhæng er underforstået. Rollen spilles primært ved udfyldningen af de almindelige principper for behandling, som er fastlagt i lovens § 5, samt i forhold til betingelser for behandling, der er listet primært i lovens §§ 6-8. Der er indledningsvis grund til at fremhæve, at det særligt er for behandling foretaget for den offentlige forvaltning, at anden ret spiller en rolle, men eksempler herpå findes dog også i relation til den private sektor.

En række af principperne i § 5 angår, hvorvidt oplysninger må opbevares, og hvor længe dette i givet fald må ske. Kort fortalt må der ikke opbevares oplysninger, der enten ikke har sammenhæng med indsamlingsformålet eller er urigtige, og opbevaring forudsætter, at formålet ikke er blevet uaktuelt. Når en sådan situation forekommer, skal oplysningerne enten korrigeres eller slettes, idet der dog også er en mulighed for, at de kan overføres til Statens Arkiver. Tegner disse regler nu et dækkende billede af den retlige virkelighed? I den private sektor må spørgsmålet formentlig besvares bekræftende, idet der

ikke er andre regler eller retlig tradition, som i almindelighed peger i modsat retning. I forhold til den offentlige forvaltning er situationen en anden, selvom man i og for sig ikke i den forvaltningsretlige lovgivning kan finde bestemmelser, der vedrører denne problemstilling. Det er dog en indarbejdet og fast tradition, at så snart oplysninger er registreret hos forvaltningen, slettes de ikke igen, uanset om de måtte være forkerte eller forældede. Dette er en stærk tradition, der ikke lader sig påvirke af persondataloven. Det kunne nu indvendes, at mange oplysninger fortsat i dag findes i manuelle sagsmapper, der ikke er omfattet af loven, men iagttagelsen vedrører den del af forvaltningen, der er omfattet, og denne vil som bekendt blive større i takt med, at forvaltningen bliver digital. Der foreligger således en konfrontationskurs, og selvom det måske kan være lidt svært at forstå, er det ikke sandsynligt, at persondatalovens principper vil stå med sejrens palmer til sidst.

I en række andre tilfælde fremgår det direkte af persondatalovens bestemmelser, at regler andetsteds skal tillægges betydning. Mest tydeligt fremstår denne sammenhæng i behandlingsbetingelserne, hvorfra jeg nu nævner nogle eksempler, idet der startes i § 6, stk. 1, der angår behandling af almindelige oplysninger. Det kan først anmærkes, at der ved anvendelsen af denne regel i forhold til forvaltningen skelnes mellem to typer almindelige oplysninger, hvilket ikke fremgår af bestemmelsen, men med lidt kløgt kan læses ud af reglerne om anmeldelse i § 44. En særlig kategori er således oplysninger, der er fortrolige, altså undergivet tavshedspligt. Her er behandlingsadgangen uden samtykke mere snæver, og ved praktiseringen af reglerne må Datatilsynet dermed kunne afgøre, om en oplysning har denne karakter, hvilket forudsætter forvaltningsretlig kundskab. Ofte let, men undertiden ganske vanskeligt.

Bevæger vi os herefter ind i § 6, stk. 1, støder vi på 7 alternerende behandlingsgrundlag. Jeg nævner blot den, der findes i nr. 6, hvorefter behandling kan ske, såfremt dette er nødvendigt af hensyn til offentlig myndighedsudøvelse. I forarbejderne udlægges dette således, at omfattet er forvaltningens afgørelsessager og i et eller andet ikke helt præcist defineret omfang tillige faktisk forvaltningsvirksomhed. Afgørende i denne sammenhæng er, at den egentlige normering af behandlingsadgangen sker i forvaltningsretten, altså et andet sted. Af interesse er ligeledes, at opstår der en sag, må Datatilsynet på ny have forvaltningsretlig kundskab for at afgøre, dels om der i det konkrete tilfælde er tale om myndighedsudøvelse, dels om behandling er nødvendig for udføre denne, hvilket kan være endnu vanskeligere.

Der kunne nævnes andre eksempler, men det er mere illustrativt at bevæge sig over i § 7, der vedrører behandling af de følsomme oplysninger, og som for mange udgør den egentlige kerne i den databeskyttelsesretlige regulering. Det er her, at vi møder privatlivets fred. Denne bestemmelse starter jo flot med et behandlingsforbud, men herefter kommer alle undtagelserne, som i

praksis har den største interesse. En række af disse undtagelser henviser til anden ret. Blandt de generelle undtagelser, der er listet i stk. 2, gælder det for nr. 4, der uden den pågældendes samtykke tillader behandling, såfremt denne er nødvendig for, at "et retskrav kan fastlægges, gøres gældende eller forsvares". Denne regel, hvis kodeord er "retskrav", forekommer ganske uskyldig, men indebærer i realiteten en meget vidtgående behandlingshjemmel, der ganske ofte er aktuel i praksis. Afgørende her er dog, at det for bestemmelsens anvendelse er centralt at fastslå, om der foreligger et retskrav. Dette hjælper loven ikke med, idet svaret herpå må søges i anden ret og her først og fremmest i den almindelige lovgivning, der således får afgørende betydning for behandlingsomfanget.

Et eksempel fra tilsynets praksis[4] illustrerer dette. Der er i den sociale lovgivning fastsat regler, hvorefter borgerne har ret til at få behandling imod alkoholmisbrug. Det lyder jo meget fornuftigt, men enhver ret afspejler sig også i et retskrav, og i den konkrete sag betød dette, at selvom Datarådet foretrak, at der blev indhentet et samtykke, kunne der uden et sådant ikke blot behandles følsomme oplysninger om den pågældende, men tillige også om visse af dennes pårørende, da det blev hævdet, at de sidstnævnte oplysninger var nødvendige for, at misbrugsbehandlingen kunne lykkes. Dette er måske i orden, men har næppe stået Folketinget klart, da disse regler blev gennemført. Ovre i § 6, stk. 1, har vi i nr. 3 en parallel regel, hvor der tales om retlig forpligtelse, og der er i almindelighed ikke nogen tvivl om, at der i den almindelige lovgivning er et væld af forpligtelser og retskrav med bl.a. den konsekvens, at persondataloven får et uselvstændigt præg.

Andre konsekvenser kommer jeg til om lidt, men først tilbage til § 7. Blandt de følsomme oplysninger finder vi for mange noget overraskende oplysninger om fagforeningsmæssigt tilhørsforhold. For denne oplysningstype findes der en særlig undtagelse i stk. 3, hvorefter behandling kan ske, såfremt dette er nødvendigt i forhold til en arbejdsretlig forpligtelse eller rettighed. Svaret på, om behandling kan ske, skal således søges i arbejdsretten. Der er grund til her at bemærke, at der er tale om et særegent retligt system, som det ikke altid er lige let for udenforstående at gennemskue.

Endelig kan der være grund til at nævne bestemmelsen i § 7, stk. 5, hvorefter følsomme oplysninger kan behandles til sundhedsformål, såfremt de pågældende har tavshedspligt. Bestemmelsen er for så vidt angår videregivelse[5] fraveget ved patientretsstillingsloven, men når den anvendes, må der tages stilling til, om der er tavshedspligt, og om et sundhedsformål foreligger; på ny spørgsmål, der er betinget af anden ret.

Også visse af lovens rettighedsregler er forbundet med anden lovgivning. Her skal blot som det mest klare eksempel nævnes § 32, stk. 2, hvorefter der ikke er indsigtsret i oplysninger, der efter offentlighedslovens bestemmelser er

4 Datatilsynets Beretning 2001 p. 37-38.

5 Hermed menes videregivelse i patientretsstillingslovens forstand.

kategoriseret som interne. Det er forvaltningsretten, der er bestemmende for retsstillingen.

Sammenfattende kan det konstateres, at persondataloven på en række punkter må karakteriseres som uselvstændig, og at det dermed er nødvendigt at medtænke den almindelige lovgivning, når man skal besvare spørgsmålet om, hvorledes beskyttelsesniveauet egentlig er i gældende dansk ret. Alene på grundlag af persondataloven er det ikke muligt at besvare et spørgsmål om, hvorvidt databeskyttelsesniveauet er bedre i 2004, end det var i 1979.

4. Tilsynets rolle

Jeg vil herefter påpege en række konsekvenser, der er forbundet med denne retstilstand, idet disse konsekvenser også har betydning, når man kigger fremad mod de næste 25 år. Dansk som europæisk databeskyttelsesret er baseret på, at der findes et uafhængigt datatilsyn, der fungerer som en garant for at databeskyttelsen bliver realiseret. Domstolene findes selvsagt, men i alle lande bruges de meget sjældent på dette område. De tidligere gjorte iagttagelser demonstrerer, at det er en særdeles krævende opgave at være datatilsyn. Det er ikke tilstrækkeligt at have oparbejdet ekspertise i persondatalovens mysterier, men det er ligeledes nødvendigt at kunne tage stilling til vanskelige fortolkningsspørgsmål i relation til den øvrige lovgivning samt i uskreven ret som f.eks. arbejdsret. Det siger sig selv, at en sådan egen selvstændig ekspertise ikke kan foreligge, og at tilsynet derfor i nogen udstrækning må basere sig på andres opfattelse. Dette er selvsagt ikke et træk, der er unikt for Datatilsynet, men det har dog den kritiske undertone, at der kan være situationer, hvor den dataansvarliges opfattelse af den relevante ret bliver udslagsgivende.

Større principiel interesse er knyttet til lovgivningsprocessen. Det følger af persondatalovens § 57 og især bestemmelsens forarbejder, at Datatilsynet skal høres i forbindelse med lovforslag, der indeholder databeskyttelsesretlige bestemmelser. En naturlig afgrænsning af denne høringsforpligtelse er, at den omfatter bestemmelser, for hvilke et lovvalg efter § 2, stk. 1, er aktuelt. Med andre ord de regler, der direkte er databeskyttelsesretlige. Det er jo i henseende til sådanne bestemmelser, at Datatilsynet råder over en særlig ekspertise, og det er ligeledes her, at det må vurderes, om de påtænkte regler er i overensstemmelse med direktivet. Det er et almindeligt indtryk, at denne høringsforpligtelse bliver overholdt om end ofte med uacceptabelt korte høringsfrister. Formålet med høringen er udover at sikre, at de EU-retlige forpligtelser overholdes, at fremme lovkvaliteten ved bl.a. at bidrage til Folketingets beslutningsgrundlag. Selvom høringsfristerne beklageligvis undertiden modvirker denne intention, fungerer ordningen alt i alt godt, men det er altså kun et mindre udsnit af lovgivningen, hvorom der høres, selvom enkelte myndigheder også fremsender lovudkast, der falder uden for den nævnte ramme.

I almindelighed høres der ikke om de lovudkast, der falder ind under det, som her er betegnet anden ret. Dette er ikke nogen fejl, fordi der ikke er nogen pligt hertil. Konsekvensen er dog, at bestemmelser, der har betydning for udfyldningen af persondatalovens regler, ikke på dette stadium bliver vurderet under det databeskyttelsesretlige perspektiv. Folketinget gives dermed ikke nogen mulighed for at vurdere, om denne facet skal tillægges nogen betydning, eller om der blot er tale om en bivirkning, som ikke bør tillægges vægt. Dette er principielt uheldigt, men spørgsmålet er, om situationen kunne være anderledes. To forhold taler for, at der ikke findes et egentligt alternativ.

For det første ville en ordning, hvorefter Datatilsynet skulle høres vedrørende stort set alle lovfor-slag medføre en betydelig anstrengelse af Datatilsynets allerede anstrengte ressourcer. I dag foretager tilsynet således ikke en realitetsbehandling af de forslag, der fejlagtigt forelægges. Med den foreliggende bevillingsmæssige ramme vil en sådan ordning ikke være realistisk, og der er desværre ikke udsigt til at rammen bliver større.

For det andet og principielt mere væsentligt må det erkendes, at det ofte er meget vanskeligt at afdække disse afledte virkninger, eftersom dette forudsætter en betydelig fortrolighed med det pågældende lovgivningsområde. I det hele taget vil det i en del tilfælde være vanskeligt at forudse de databehandlingstilfælde, der senere opstår. Dette vil dog i nogle situationer være muligt for det ansvarlige ministerium, og her bør det være en forpligtelse at gøre opmærksom på disse afledte virkninger. Det er således værd at overveje om de oplysningsforpligtelser, der er indbygget i lovgivningsprocessen, bør udvides på dette punkt.

5. Uoverskuelighed

En yderligere konsekvens af samspillet mellem de egentlige databeskyttelsesretlige regler og anden ret er, at der ikke er nogen, som fuldt ud kan overskue dansk ret og dermed udrede landets databeskyttelsesniveau. I Sverige, der jo er kendt for sin tradition for grundighed, igangsættes, så vidt jeg har forstået, her i foråret et udredningsarbejde netop med henblik på at fremskaffe dette samlede overblik. Hvorvidt noget tilsvarende er ønskeligt hos os kan diskuteres, men under alle omstændigheder kan det opleves som utilfredsstillende ikke at kunne angive, i hvilket omfang persondata behandles her i landet.

Dette savn føles måske særlig stærkt ved et jubilæum, hvor det er naturligt at se på, hvorledes det er gået på databeskyttelsesområdet og at angive en form for state of the nation erklæring. Det må konstateres, at der ikke kan gives noget fuldgyldigt svar på, om lovgivningen har været en succes. Med den forståelse af lovens formål, som jeg nævnte i starten, er det dog nærlig-

gende at udtale, at det trods alt er en succeshistorie, vi markerer i dag. Persondatabehandlingen er mere civiliseret, end den ville være uden loven. Persondataloven spiller hovedrollen nogle gange, men dog andre gange blot en birolle. Malurten i bægeret er især, at den anden rets voldsomme omfang har betydet, at persondatabehandlingens omfang i dag er betydelig større end i 1979. Succesen er således betinget, og der er fortsat meget at gøre for sikringen af borgernes integritet og informationelle privatliv.

Den mobile identitet - tanker om fremtiden ved registerlovens jubilæum

Ved udviklingsdirektør Preben Mejer

Tak for invitationen til at komme her i dag og være med til at markere jubilæet.

Titlen på mit indlæg blev til for 3 måneder siden og skulle være udgangspunktet for en præsentation af mine tanker i forbindelse med registerlovens 25 år jubilæum. I mellemtiden har jeg nu rent faktisk gjort mig nogle tanker om fremtiden, og i den forbindelse er foredragets titel beklageligvis blevet en anelse uprækis.

Naturligvis må tanker om fremtiden og registerloven handle om identiteter – dels de identiteter, der får adgang til persondata, dels de identiteter, der gemmer sig under disse persondata. Talen må også handle om mobilitet, fordi den digitale verden er blevet mobil. Endelig må snakken dreje sig om alle former for håndtering af personoplysninger – om hvordan persondata genereres, udveksles, distribueres, opsamles, opbevares, videregives og sammenstilles – i den verden af pervasive computing – IT i alting – som vi er på vej imod.

Dét vil mine ord handle om.

I januar blev præsidenten for Hells Angels fængslet mistænkt for skattefusk i millionklassen. Præsidentens fald skyldtes et samarbejde mellem en række myndigheder – de sociale, de kommunale og statslige skattemyndigheder og politiet. Samarbejdet bestod i en samkøring af en række registre. Registre med oplysninger om præsidenten. Isoleret og hver for sig er det uskyldige data, men sammenstykket er det nok til at tegne et billede, der altså førte til en fængsling. Præsidentens kranke skæbne ville ikke have været ret sandsynlig for få år siden. Det er først i dag, at de forskellige registres dataformater har nået en grad af standardisering, der for alvor muliggør en sammenstykning.

Registerloven har de sidste 25 år udgjort et velfunderet regelsæt for, i hvilket omfang personrelaterede oplysninger, som dem der måske fælder HA præsidenten, har måttet gemmes, tilgås og anvendes i offentligt tilgængelige regi-

stre. Skal man være lidt feststemt i dagens anledning, kan man vel karakterisere registerloven som en fremsynet succes. Allerede i 1979, dengang computere og databaser endnu var en fjern verden for langt de fleste mennesker, trådte loven i kraft, og siden da har den – med regelmæssige opdateringer – beskyttet følsomme persondata. HA præsidenten kunne formodentlig ønske sig en strammere lovgivning, der i endnu højere grad beskyttede de personlige data mod, hvad han måske vil karakterisere som misbrug, mens andre hen over årene har plæderet for en friere adgang til registrene – alt imens flere og flere persondata samles i stadigt flere databaser.

Spørgsmålet er i dag om registerloven – eller loven om persondata – magter at følge med udviklingen. Er registerloven klar til endnu 25 år? Jeg ikke er sikkerhedsekspert - endnu mindre jurist - så jeg vil ikke påstå, at jeg har svaret, men det er dog tydeligt - også for mig, at udfordringen er en helt anden i dag, end den der eksisterede, da loven så dagens lys. For 25 år siden var verden en anden. Vi havde analoge telefoncentraler, og telefaxen var endnu fremtid. Databaser var noget, der kun fandtes på store mainframe computere, som kommunikerede med omverdenen via hulkort og hulstrimler. Flytning af data foregik i bedste fald via store magnetbånd. Siden da er computerne begyndt at tale direkte sammen, i første omgang via dedikerede dataforbindelser og i kommunikationsformater, der i dag kun er husket af en flok ældre gråhårede herrer i IT branchen – og igennem kabler, som computernes indehavere selv måtte bekoste at få anlagt.

Det er for øvrigt lidt sjovt at tænke på, at denne uge – ud over 25 års jubilæet – også bragte et 150 års jubilæum. Jeg var med til i mandags at fejre 150 året for den første kommunikationsforbindelse ud af Danmark. Den gik fra Helsingør – via København og Fredericia – til Hamborg. Det kabel var utæt som en si, ikke alene i datamæssig sammenhæng, men desværre også – og det anså man jo dengang som det største problem - rent fysisk. Hvem som helst kunne opsnappe og aflytte trafikken, og kablet blev nedlagt i guttaperka – rågummi – og i et blyrør. Allerede året efter måtte det lægges om. Så når man ser på de udfordringer, vi nu står med her på tærsklen til den næste store IT bølge – IT i alting – blev kimen til revolutionen – eller miseren – altså lagt i denne uge for 150 år siden. I dag har vi jo nemlig alle sammen computere, som snakker sammen via internet.

Kommunikationen er ikke bundet til nedgravede kabler; et stigende antal af computerne kommunikerer i trådløse net. Datatrafikken er eksponentielt voksende, og den er i høj grad usynlig. I pervasive computing æraen – IT i alting – er det ikke længere blot computeren, der har regnekraft – også mobiltelefonerne får det i stigende grad.

Halvdelen af de telefoner, der bliver solgt i 2006, vil være det vi på godt vestjysk kalder full feature operating system telefoner. Det vil sige, at mobiltele-

fonen - eller hvad vi nu til den tid vil kalde den type enheder, som vi bruger til kommunikation, når vi er på farten – vil få nutidens mobiltelefoner til at ligne stentavler. Almindelige telefoner vil kunne kommunikere via mere end en håndfuld forskellige trådløse teknologier og vil til den tid være udrustet med 3D-skærme, langtidsholdbare batterier, positionsbestemmelse via GPS, lagerplads svarende til nutidens PC'er og frem for alt en voldsom processorkraft. Dermed bliver i første omgang mobiltelefonen et fantastisk kraftfuldt redskab i vores dagligdag. Vi vil afvikle komplekse programmer, og vi vil købe ind og betale over mobiltelefonen – den bliver et knudepunkt for pervasive computing – den computerunderstøttede hverdag – og den vil dermed blande sig i den dialog og udveksling af data, som ellers har været forbeholdt de traditionelle computere.

Yderligere er mange ting omkring os også blevet udstyret med mikroprocessorer. På arbejdspladsen, i hjemmet, i trafikken overalt bliver vi omgivet af intelligent elektronik. Det gælder for bilen, hvor allerede i dag min Saab har mere regnekraft end et lidt ældre Airbus fly. Bilen er også udstyret med en black box, der registrerer min adfærd, hastighed og så videre. Hvem har retten til de data, og hvem må bruge dem?

Køleskabet, vaskemaskinen, kaffemaskinen, legetøjet i børneværelset og meget, meget andet har også i dag ofte regnekraft. Så mange ting omkring os er udstyret med regnekraft, at det faktisk kun er 3 % af de 5 milliarder mikroprocessorer, der hvert år produceres, der ender i computere.

Samtidig betyder de nye trådløse kommunikationsteknologier, at alle disse ting omkring os ikke blot via deres mikrochips kan reagere på omverdenen, de kan også kommunikere med den. Tingene vil begynde at tale sammen. I øvrigt både med og uden vores vidende.

Blandt de klassiske kuriøse eksempler er hjemmets badevægt og køleskabet, der autonomt styrer diæten. Badevægten siger – nu har han taget på igen – og køleskabslågen nægter at lukke op, eller det intelligente tøj og vaskemaskinen, der i forening undgår kogevask af silkeskjorterne. Eller tørretumbleren, der kan fortælle vaskemaskinen, at den er på vej ud i noget snavs – og så hjælpe med at finde det rigtige program til at afhjælpe miseren. Kun fantasien sætter grænser. Teknologien er der.

Man kan selvfølgelig spørge sig selv, om anvendelserne giver mening. Ville deltagerne i TV-serien "Livet er fedt" vinde ved, at en asketisk badevægt overtog kontrollen med det ikke helt fedtfrie køleskab? Måske ikke. Men det er en helt anden og interessant diskussion, som ikke hører hjemme her. Min pointe er, at vi vil blive oversvømmet med digital kommunikation fra ting omkring os, som snakker sammen. Prognoser tyder på, at mere end 95 % af alle netværkssamtaler i 2020 vil foregå mellem maskiner og uden vores indblanding.

I forhold til den verden, hvor registerloven tog sit udgangspunkt, går vi en fantastisk kompleks fremtid i møde. Nøgleordene er mobilitet og pervasive computing. De bliver garanter for en verden, hvor endeløse mængder af data flyder mellem talløse mere eller mindre mobile enheder. Det bliver svært at overskue og svært at regulere.

Med den øgede intelligente kommunikation, som genereres ikke blot af os selv, men også af ting i vores hverdag, er det nemt at forestille sig, hvor store mængder af personrelaterede data, der konstant vil udveksles i det store offentlige rum, som de digitale netværker udgør.

I USA er varehuskæden Wal-Mart for tiden i defensiven efter at have offentliggjort en strategi med den trådløse, digitale varemærkning – små tags, som skal erstatte de traditionelle stregkoder – måske allerede fra år 2010. Tags kan være på størrelse med en Gajol eller et rødt frimærke, de koster i dag en krone og om 2-3 år 10 øre. De kan sættes på hvad som helst, der dermed bærer information om sig selv, information der kan kombineres med information om, hvem der købte varen, og mange andre oplysninger. Forbrugergrupper anført af CASPIAN - Consumers Against Supermarket Privacy Invasion and Numbering - har blæst til kamp mod det, de ser som et stort skridt på vejen mod et ultimativt overvågningssamfund.

Argumentet er, at hvis varens mærkning, som Wal-Mart har skitseret det, kan aflæses trådløst i et supermarked uden kassedamer – i det der er døbt Silent Commerce - kan aflæsningen i princippet foregå overalt, og pludselig kan trådløse sensorer måske spore vores færden via den pågældende vare. Rygterne om Wal-Marts chips nåede at inkludere vanvittige teorier om, at specielle satellitter i lave kredsløb ville være i stand til spore alle de små elektroniske stregkoder. Noget af en bedrift, da læseafstanden for disse stregkoder er mellem 5 millimeter og 5 meter – så for at læse disse tags vil der med andre ord være tale om ret usædvanlige satellitter i yderst spektakulære baner...

Jeg tror, at risikoen for denne form for overvågning er minimal, men den eksisterer i teorien. Både forbrugere og producenter skal forholde sig til den. Debatten i USA har foreløbigt mundet ud i udarbejdelsen af flere sæt af etiske regler for brugen af tags. Disse regler foreskriver blandt andet åbenhed om brug og aktivering af de elektroniske tags, afgrænsning for placering af tags samt muligheden for at de-aktivere eller afmontere tags. Men bekymringerne om datamisbrug stopper langt fra her. I virkeligheden vil dialogen mellem de elektroniske stregkoder kun bidrage til en lille del af de informationer, som vil flyde i det digitale informationsrum.

Når mit køleskab begynder at bestille varer hos købmanden, når min badevægt udveksler data med min privatpraktiserende læge, eller når jeg betaler

taxaen med min mobiltelefon, udveksles og opsamles oplysninger, og med tiden vil mønstre begynde at tegne sig. Dermed står vi foran en ny udfordring med hensyn til beskyttelsen af følsomme persondata. Spørgsmålet er nemlig, om det ikke vil blive muligt at sammenstykke det væld af isoleret set måske trivielle og ligegyldige informationer, som vi udveksler i forbindelse med de enkelte transaktioner til en informationsmængde, der tilsammen udgør følsomme oplysninger. I gamle dage stod privatdetektiverne på hovedet i skraldespandene for at finde kompromitterende materiale – fremtidens detektiver vil måske kunne nøjes med at kaste vod gennem nogle søgninger på Nettet.

Den enkelte udveksling af data mellem den elektroniske stregkode på æsken med slankemidler og en virtuel kassedame er isoleret set uinteressant. Det er min badevægts snak med lægen måske også, men sammenstilles oplysningerne kan det blive interessant. I fremtiden behøver man måske ikke at samkøre formelle offentlige registre for at fælde HA præsidenten. Granskning og krydskorrelation af et større antal mindre databaser og logfiler på nettet vil måske kunne bruges til at samle en digital profil med de samme informationer.

Det giver næppe mening at søge at begrænse trafikken, men kan vi så begrænse muligheden for at opsamle disse oplysninger?

Problemet er, at vi i høj grad kan være anonyme på nettet. Denne fingerregel bliver i stigende grad misbrugt på internettet, og det giver problemer. Vi kender alle til virus og spam, som er internettets pest og kolera. De fleste af internettets brugere fører en ørkesløs daglig kamp mod oversvømmelser af den elektroniske postkasse. De afsenderløse spam mails, som i dag udgør op imod halvdelen af alle emails, faldbyder helt uden hensyntagen til modtagerens køn, volumen og alder alt fra tvivlsomme potenspiller, over slankekure, der på mirakuløs vis kan praktiseres i lænestolen foran fjernsynet til mistænkeligt attraktive studielån. Inden man overhovedet begynder at sortere posten, skal man imidlertid for alt i verden huske at opdatere sit virusskjold, så en anonym, intetsigende mail ikke viser sig ikke blot at være nonsens, men – hvad der er langt værre – viser sig at være et virusprogram, der inficerer computeren.

Allerede i den forbindelse er vi ved at lære, at anonymiteten på internettet giver problemer og har kostbare konsekvenser. I takt med at misbruget bliver flyttet over på mobile enheder – som for eksempel de nye smartphones.

En strategi for at komme misbruget til livs er en bedre identifikation af brugerne, der udveksler informationer på nettet. Dette kan for eksempel ske med udveksling af digitale signaturer. Allerede i dag har alle danskere gennem TDC mulighed for gratis at få et certificeret sæt af krypteringsnøgler,

som anvendes til en sikker signatur på emails og til access til beskyttede webservices, som for eksempel hos Told og Skat. I den ideelle verden, hvor alle bruger – og kræver – en digital signatur, kommer der i teorien afsender på virus og spam – vi vil kunne drage nogen til ansvar. Og vi vil kunne se, hvem der er tilgået for eksempel personfølsomme data. Eller kan vi nu det? Hvad nu hvis nogen har haft adgang til min maskine?

For at undgå den situation må vi beskytte computerne mod uvedkommendes adgang. Dette bliver naturligvis endnu vigtigere, når misbruget om nogle år primært vil foregå via de avancerede mobiltelefoner eller andre små mobile net-terminaler, som vi ofte vil efterlade uden opsyn. Tænk på, hvor mange timer det er siden, I sidst glemte jeres mobiltelefon eller PDA på en kollegas skrivebord. Der forskes i dag i udvikling af adgangskontrol til PDA'er, telefoner og små mobile computere. Biometri, det vil sige adgangskontrol baseret på genkendelse af biologiske karakteristika – fingeraftryk, iris mønster, stemme- og ansigtsgenkendelse – er mulige løsninger. Spørgsmålet er blot, hvor stor sikkerhed disse metoder giver. Automatisk ansigtsgenkendelse, hvor en computer sammenligner en persons aktuelle ansigt med et pasfoto, har foreløbig under ganske stor bevågenhed vist sig utilstrækkelige til passageridentifikation i lufthavne flere steder i verden.

Spørgsmålet er også, hvor svært det vil være at få et ansigt til at ligne et andet. I England er der allerede i dag ventelister for personer, der ønsker en ansigtstransplantation. Altså ikke blot en ny næse, men et helt nyt ansigt. Hvad gør man så? Så er der fingeraftrykkene, kriminalromanernes klassiske trumfkort. Det viser sig desværre, at en del af os har svært ved overhovedet at afsætte fingeraftryk. Og nu hvor vi er på vej ud i fremtiden kunne man også – med hensyn til fingeraftryk – og lidt mere kuriøst – overveje, om klonede individer vil have ens fingeraftryk...

Pointen er, at adgangskontrol baseret på computer identifikation under alle omstændigheder er vanskelig. Og vil man passere adgangskontrollen, vil der oftest vise sig en vej. Derfor er praktiske forhindringer – digitale signaturer og fysisk adgangskontrol – ikke nok til at komme misbrug til livs. Det er nødvendigt at lovgive imod det, og det er måske problemets kerne. Internettet overhalede på mange måder lovgivningen indenom. Det lider vi lidt under i dag.

Før den mobile IT og pervasive computing for alvor bryder igennem vores hverdag, er det væsentligt, at vi ikke blot fokuserer på at begrænse teknologiens sårbarhed, men at vi også igennem lovgivning begrænser spekulationen i sårbarheden. Men uden at kamme over.

Giv teknologien plads til at vise os muligheder. Det er nemt at definere negativt – ved at forbyde, men lad os definere positivt, lade teknologien vise os

lidt muskler og muligheder, inden vi hælder sand på det imaginære bål og kvæler udviklingen med stramme lovgreb. For hver ny teknologi vil der være ca. 3 dårlige anvendelser ud af 10 anvendelser i alt. Hvis man kun fokuserer på de tre, risikerer man at begrænse resten og dermed give Danmark dårlige kår i sit forsøg på at realisere drømme om verdens fremmeste IT – eller videns nation – som man faktisk under samtlige statsministre i Internet-tiden har haft som målsætning.

Registerloven har nu i 25 år taget hånd om beskyttelsen af persondata, det er væsentligt, at vi sørger for, at den fortsætter med at gøre det – ved at tage højde for udviklingen – de kommende 25 år.

Overvågning i et arbejdstagerperspektiv

Ved advokat (L) i Schebye & Jacobsen advokatfirma, kandidatstipendiat Martin Gräs Lind Juridisk Institut, Afdelingen for Offentlig ret, Aarhus Universitet

1. Indledning

Medarbejderovervågning reguleres af en række forskellige retskilder, som ofte har helt forskellige formål og retsvirkninger. Der findes således ikke nogen samlet lovgivning, som særligt vedrører overvågning af medarbejdere.

Retsstillingen må bl.a. stykkes sammen af arbejdsretlige regler og praksis og af databeskyttelsesretten, hvor persondataloven og Datatilsynets praksis har stor betydning. Endvidere indgår strafferetten med dens regler om beskyttelse af privatlivets fred og reglerne i tv-overvågningsloven, som retskilder, når reglerne for overvågning af medarbejdere skal anskueliggøres. Herudover regulerer en række andre nationale og internationale regler, aftaler og forpligtelser området.

Overvågning af medarbejdere kan beskrives som en kontrolform af mere intens og vedvarende karakter. Kontrollen bliver systematisk og forholder sig til medarbejderens adfærd over en periode.

2. Arbejdsgiveren har ret til at overvåge medarbejdere

Ud fra arbejds- og ansættelsesretlige grundsætninger og afgørelsespraksis inden for det kollektivt arbejdsretlige system kan der udledes visse normer for, om og hvorledes arbejdsgiveren lovligt kan overvåge sine medarbejdere.

Et retligt udgangspunkt for arbejdsgiverens overvågningsret kan udledes af grundsætningen om arbejdsgiverens ledelsesret, hvorefter arbejdsgiveren har ret til at lede og fordele arbejdet, herunder at føre tilsyn med medarbejderne.

Arbejdsgiveren kan som udgangspunkt både i det helt individuelle ansættelsesforhold uden for overenskomstområdet og inden for overenskomstbaserede ansættelsesforhold lovligt kontrollere sine medarbejdere. Overvågning er ikke forbudt som kontrolform.

3. Retlige begrænsninger i arbejdsgiverens overvågningsret

Dette er dog ikke ensbetydende med, at arbejdsgiveren har en uindskrænket adgang til overvågning.

Der gælder en række lovbaserede og ulovbaserede begrænsninger.

Arbejdsgiveren kan ikke som en anden Big Brother i Orwells "1984" via teleskærmen lovligt opnå indsigt i alle medarbejderens gøremål, om end det ikke længere er de tekniske muligheder, som sætter grænsen. De fleste medarbejdere, som arbejder dagligt med f.eks. PC, ville blive chokerede, hvis de var klar over, hvor detaljerede oplysninger der kan spores om deres adfærd i løbet af en arbejdsdag via helt almindelige computersystemer og softwareprogrammer. Betegnelsen PC som personlig computer falmer lidt i lyset heraf.

Der er i praksis inden for den kollektive arbejdsret, som i vidt omfang regulerer arbejdsvilkårene i Danmark, udviklet visse retningslinjer for arbejdsgiverens kontrol og overvågning. Overvågning må f.eks. ikke have en krænkende form eller forvolde arbejdstagerne tab eller nævneværdig ulempe. Den må heller ikke iværksættes af ren nysgerrighed, da den skal have et fornuftigt formål og være begrundet i driften.

I en afgørelse fra 1992, som blev afsagt ved faglig voldgift, blev der taget stilling til spørgsmålet, om overvågning af en række medarbejdere uden for arbejdstiden, men på arbejdsstedet, var krænkende.[6]

Den øverste ledelse af en værkstedskoncern havde modtaget flere anonyme henvendelser om, at der på et bestemt værksted foregik en række uregelmæssigheder, herunder organiseret "sort" arbejde uden for arbejdstiden. Et detektivbureau blev sat på sagen og overvågede værkstedet fra observationsvogne og ved hjælp af forskelligt teknisk udstyr over ca. 1,5 måned. Man fandt ikke beviser nok til at kunne afskedige medarbejdere, selvom man observerede en vis mistænkelig adfærd. F.eks. var en medarbejder på arbejde kl. 0500 om morgenen, hvor han reparerede en bil, der tilhørte en tidligere værkfører. Man konstaterede også, at to andre medarbejdere senere på aftenen ødelagde forpartiet på en bil ved at køre den ned af en rampe og ind i en betonvæg.

Ifølge afgørelsen kunne det ikke bebrejdes virksomheden, at den med fremmed bistand iværksatte en observation af værkstedet, hovedsagelig uden for

[6] Jf. kendelse af 17. april 1992 afsagt af landsdommer Preben Kistrup i faglig voldgift mellem Centralorganisationen af Metalarbejdere i Danmark mod Industriens Arbejdsgivere for Bohnstedt-Petersen A/S.

almindelig arbejdstid. Som kontrolforanstaltning fandtes observationen under de givne omstændigheder heller ikke at være så krænkende, at der kunne blive tale om en bod.

Lovgivningen, som har indflydelse på retstillingen vedrørende overvågning, er opstrammet betydeligt siden 1992. Der gælder således i dag flere lovmæssige begrænsninger i adgangen til at overvåge. Persondataloven er f.eks. indført med skærpede krav om information, saglighed, proportionalitet mv. Nu omfatter tv-overvågningsloven også et skiltningskrav i forbindelse med overvågning af ansatte.

En helt central beskyttelse i persondataloven imod arbejdsgiverens overvågning består i oplysningsforpligtelserne i PDL §§ 28-29. Disse regler kræver, at arbejdsgiveren på forhånd på en klar og utvetydig måde orienterer medarbejderen om, at elektronisk overvågning vil og kan finde sted, og med hvilket formål. Dette gælder f.eks. tv-overvågning og overvågning via computeren. Hemmelig tv- og computerbaseret overvågning kan derfor siges at være lovstridig i medfør af persondataloven. Også andre bestemmelser i persondataloven fastsætter grænser for en arbejdsgivers elektroniske overvågning. Persondata må f.eks. kun indsamles til saglige formål og ud fra et proportionalitetsprincip. Praksis fra Datatilsynet viser, at kontrol og overvågning i persondataretlig forstand kan udgøre saglige begrundelser for behandling af persondata om medarbejdere. En elektronisk medarbejderovervågning må dog ikke iværksættes af ren nysgerrighed eller med det formål at snage i registrerede data om medarbejderens surfing på internettet eller i den private e-mailkommunikation.

Overtrædelse af oplysningsforpligtelsen i persondataloven kan med hjemmel i PDL § 70, jf. §§ 28 og 29 sanktioneres med strafferetlige følger, hvis politiet vil prioritere behandlingen af sagen, og hvis der ikke er for meget bevismæssig usikkerhed om, hvad medarbejderen er blevet orienteret om. Her kan politiet ikke hente hjælp fra Datatilsynet, som efter praksis henviser klagere til civilretligt søgsmål ved domstolene omkring eventuel bevismæssig usikkerhed.

Domstolene vil kunne afklare den bevismæssige usikkerhed, men hvis den falder ud til medarbejderens fordel, kan der måske alligevel ikke rejses tiltale, fordi sagen er forældet.

Domstolene har med hjemmel i persondatalovens § 69 mulighed for at tilkende medarbejderen erstatning for den skade, der er lidt ved f.eks. den manglende overholdelse af oplysningsforpligtelsen i persondatalovens § 28. Men forarbejderne til bestemmelsen viser, at det har været meningen med erstatningsreglen, at dansk rets almindelige erstatningsregler skal finde anvendelse.[7] Disse forudsætter, at der er lidt en økonomisk skade. Men hvilken

[7] Jf. Betænkning nr. 1345/1997 om behandling af personoplysninger, s. 387 f.

økonomisk skade er der lidt ved, at en medarbejder med rette føler, at integriteten er blevet krænket ved en hemmelig eller i øvrigt krænkende overvågning?

Erstatningsansvarslovens (EAL) § 26 kan tilkende godtgørelse for tort, altså for ikke økonomisk skade. Der foreligger dog endnu ikke trykte afgørelser, som har tilkendt godtgørelse for tort i forbindelse med overtrædelse af persondataloven.

En afgørelse af 22. oktober 2003 fra Østre Landsret[8] tog stilling til problemstillingen. Afgørelsen vedrørte spørgsmålet om retten til torterstatning for arbejdsgiverens overvågning af en medarbejder via et detektivbureau og for overtrædelse af persondataloven.

En arbejdsgiver mistænkte en kvindelig medarbejder for uberettiget sygemelding og engagerede et detektivbureau til at overvåge hende ved den private bopæl. Overvågningen var særdeles nærgående, og jeg vil citere et par sekvenser fra overvågningsrapporten:

"Overvågningen blev genoptaget kl. 19.45 i.h.t. aftale med klienten, hvor det blev konstateret, at lejligheden var fuldt oplyst. På grund af manglende gardiner konstateredes almindelig aktivitet. En ung mand var til stede. Han forlod adressen kl. 21.00. Kl. ca. 21.30 forlod hun adressen iført sommertøj og uden sko og gik i solcenter. Da hun kom tilbage til lejligheden, indledte hun den vildeste aerobic i en hel time, som efterforskerne længe har set. Kl. ca. 23.45 forlod hun stuen formentlig for at tage et bad og returnerede til stuen, hvor hun iført t-shirt dæmpede lyset ca. kl. 24.00 og rystede dyner. Da der ikke blev iagttaget yderligere aktiviteter, ophørte efterforskerne overvågningen ca. kl. 0.15."

Medarbejderen, der havde lægeerklæring på sin sygdom, følte sig krænket og anlagde sag i medfør af EAL § 26 imod arbejdsgiveren.

Både byretten og Østre Landsret frifandt arbejdsgiveren bl.a. under henvisning til, at det ikke i sig selv kan anses som en retsstridig krænkelse af den ansatte, at en arbejdsgiver – som mistænker en af sine medarbejdere for at have afgivet en urigtig sygemelding – antager et detektivbureau til at overvåge vedkommende for at skaffe bevis for sin antagelse. Efter bevisførelsen fandtes det endvidere ikke godtgjort, at overvågningen var sket på en særlig krænkende måde, herunder fra andet niveau end gadeplan, eller at overvågningen var fortsat efter ansættelsesforholdets afslutning. Endvidere fandtes det ikke i sig selv at udgøre en krænkelse, at arbejdsgiveren med det oplyste formål overlod bureauet et billede af medarbejderen samt en kopi af en skematisk lægeerklæring om medarbejderens uarbejdsdygtighed, selvom videregivelsen af de nævnte personoplysninger til detektivbureauet måtte gå videre end hjemlet i persondataloven.

[8] Jf. ØLR dom i 20. afd. a.s. nr. B-1019-02.

I Norge er retsstillingen anderledes, når det angår arbejdsgiverens hemmelige overvågning og overtrædelser af persondataloven mv.

I en norsk afskedigelsessag fra 2001[9] kom det frem, at arbejdsgiveren ud over en række andre overvågningskameraer, som medarbejderne var bekendt med i form af skiltning mv., havde opsat et ekstra kamera uden medarbejdernes vidende. Det hemmelige kamera havde særligt til formål at overvåge, om medarbejderne tog af kassen. Højesteret bemærkede, at en sådan form for overvågning repræsenterer et vidtgående integritetsindgreb overfor de ansatte, som må opleve overvågningen som stærkt krænkende.[10]

Flere andre norske Lagmanns- og Højesteretsafgørelser har tilsvarende præmisser, og der ydes efter retspraksis også erstatning for ikke økonomisk skade i forbindelse med hemmelig overvågning.

Endvidere må det bemærkes, at der både i den norske og svenske persondatalovgivning er udtrykkelig lovhjemmel til at tilkende den krænkede en godtgørelse for ikke økonomisk skade for overtrædelse af loven. Man kan overveje, om implementeringen af persondatadirektivet på dette område i dansk ret lever op til det EU-retlige krav om "effet utile".

Udover de allerede nævnte teoretiske indskrænkninger i arbejdsgiverens ret til at overvåge medarbejderne gælder særregler i tv-overvågningsloven, som også omfatter andet end tv-overvågning. I det væsentlige er der set ud fra et arbejdstagersynspunkt ikke nogen beskyttelse i tv-overvågnings-loven, som ikke allerede gælder i persondataloven. Samspillet mellem de to love er et kapitel for sig.[11]

Straffeloven indeholder i § 263 en beskyttelse af brevhemmeligheden, som også omfatter e-mails. En arbejdsgiver, som overvåger en medarbejderes private e-mailkommunikation, og som er klar over, at den er privat, bryder brevhemmeligheden og kan straffes. De fleste arbejdsgivere gør dog gældende, at de ikke vidste, at e-mailen var privat. Dermed er det ofte meget vanskeligt at bevise det forsæt til krænkelse af brevhemmeligheden, som er nødvendigt for sanktioneringen af bestemmelsen.

Herudover består der en begrænsning i arbejdsgiverens overvågningsadgang i reglerne om privatlivets fred i forskellige andre bestemmelser i straffeloven, ligesom f.eks. den europæiske menneskerettighedskonvention indeholder regler om beskyttelse af privatlivets fred.

9 Jf. Rt. 2001 s. 668.

10 Kæremålet for den norske Højesteret vedrørte dog spørgsmålet om muligheden for afskærelse af bevis.

11 Se nærmere herom Martin Gräs Lind, Persondataloven og lov om tv-overvågning – gennemtænkt samspil?, Retsvidenskabeligt Tidsskrift, www.rettid.dk, 3. årgang, 1, 2003.

4. Afslutning

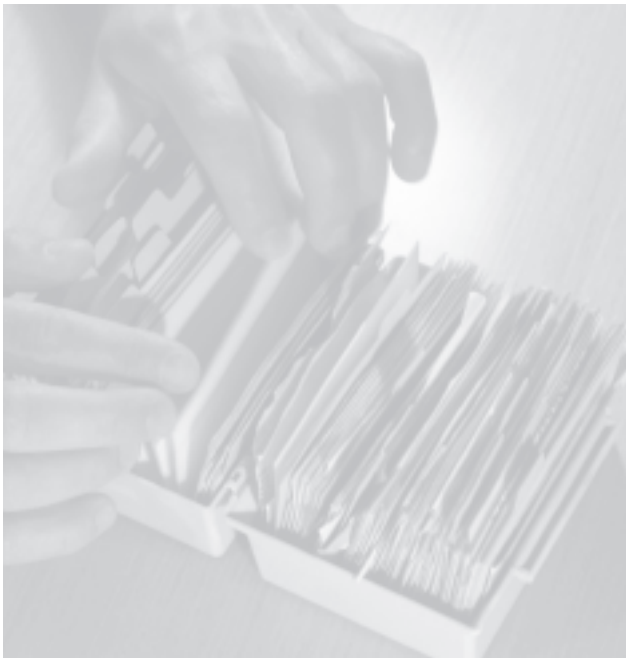
Det har i dette korte indlæg ikke været muligt at opridse alle retsregler af betydning for beskyttelsen imod medarbejderovervågning. Uden at blive alt for retspolitisk kan der godt peges på visse svag-heder i beskyttelsen:

Den integritetsbeskyttende lovgivning, som regulerer overvågning, er for den enkelte medarbejder helt uoverskuelig som følge af den sammensatte og komplekse karakter. Hvis medarbejderen ikke ved, hvori beskyttelsen består, og ikke relativt nemt kan gøre sig bekendt hermed, fordi beskyttelsen må udledes af utallige retskilder, så går en væsentlig del af beskyttelsen tabt. Følelsen af at være blevet krænket ender derfor ofte som en "dårlig smag i munden", hvis medarbejderen overhovedet har opdaget, at vedkommende har været overvåget.

Håndhævelsen er det andet for medarbejderen bestående problem. En "næse" fra Datatilsynet til arbejdsgiveren giver måske en vis tilfredsstillelse. Med den presseopmærksomhed, der efterhånden er blevet omkring større erhvervsvirksomheders optræden, vil kritik fra Datatilsynet også i kraft af øget publicitet omkring Datatilsynets virksomhed være noget, som de fleste virksomheder ønsker at undgå. Arbejdsgiveren kan også have fået en bøde via politiet. Dette er dog sjældent set i praksis. En økonomisk godtgørelse til medarbejderen fra arbejdsgiveren vil også udgøre et plaster på såret, og dette vil have en afskrækkende og præventiv effekt. Der kan argumenteres for, at erstatningsansvarsloven indtil videre må fortolkes mere dynamisk, således at også overtrædelser af integritetsbeskyttende lovgivning såsom persondataloven eller krænkende overvågning i øvrigt sanktioneres med en økonomisk godtgørelse, selvom der ikke er lidt noget økonomisk tab.

Jeg vil afslutte med at citere docent på Handelshøjskolen i Århus, Verner C. Petersen, som forsker i værdibaseret ledelse, fra et interview i Jyllandsposten d. 2. december 2003:

"Man skal stole på sine medarbejdere"... "Tiden burde være løbet fra kontrolmekanismerne. Den form for styring får samme konsekvenser som den sovjetiske planøkonomi, hvor arbejderne ignorerede de forhold, der ikke blev målt, så effektiviteten gik fløjten."... "Det at behandle voksne mennesker som voksne mennesker har vist sig at virke".



Udtalelser over lovforslag mv.

Udtalelser over lovforslag mv.

IT-kriminalitet mv.

Justitsministeriet anmodede Datatilsynet om en udtalelse om udkast om forslag til lov om ændring af straffeloven, retsplejeloven og markedsføringsloven (IT-kriminalitet mv.).

Hovedformålet med lovforslaget var ifølge bemærkningerne at skabe en forbedret strafferetlig beskyttelse mod IT-kriminalitet. Af særlig databeskyttelsesmæssig relevans var navnlig udkastets forslag til bestemmelser om ændring af straffeloven med indsættelse af bestemmelser om såkaldte informationskrænkelser, herunder om uretmæssig brug af adgangsmidler til informationssystemer, og forslaget om indsættelse af en bestemmelse om hastesikring i retsplejeloven.

Med henblik på at øge politiets muligheder for at efterforske IT-relateret kriminalitet blev det således foreslået at indsætte en ny bestemmelse i retsplejeloven, hvorefter politiet har mulighed for at pålægge udbydere af telenet eller teletjenester at foretage såkaldt hastesikring af elektroniske data. Bestemmelsens hovedformål var at hindre, at elektroniske data, der kan være af betydning i politiets efterforskning, slettes som led i den normale drift hos teleudbydere mv. Lovforslaget gav politiet mulighed for at meddele teleudbydere mv. pålæg om at gemme elektroniske data i op til 90 dage, således at dataene eventuelt på et senere tidspunkt kan udleveres til politiet til brug for efterforskning

Forslaget havde endvidere til formål at gennemføre de ændringer i straffeloven og retsplejeloven, der er nødvendige for, at Danmark kan ratificere Europarådets konvention om IT-kriminalitet (Cybercrime-konventionen).

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

Set i lyset af den øgede anvendelse af elektronisk borgerbetjening anså Datatilsynet det for et vigtigt element i beskyttelsen af privatlivets fred, at det fornødne strafferetlige værn mod misbrug af borgerbetjeningsfaciliteter er til stede.

Tilsynet henledte derfor opmærksomheden på, at uberettiget rekvirering og efterfølgende misbrug af certifikater – f.eks. af det nyligt lancerede borgercertifikat OCES[12] – som kan udstedes uden personligt fremmøde, kan tænkes at finde sted med andre formål for øje end økonomisk vinding. Certifikaternes primære anvendelsesområde er således elektronisk selvbetjening samt kommunikation med offentlige myndigheder og kan dermed først og frem-

[12] Offentlige Certifikater til Elektronisk Service. Omtales nærmere i afsnittet om sikkerhedsspørgsmål.

mest anvendes til at skaffe oplysninger om den borger, certifikatet angives at vedrøre. OCES-certifikatet kan bl.a. anvendes til udlevering af følsomme oplysninger omfattet af persondataloven §§ 7 og 8.

Den typiske fremgangsmåde ved udstedelsen af et certifikat er, at borgeren, efter at have oplyst sit personnummer og e-postadresse til certificeringscenteret (CA), modtager en PIN-kode, som sendes til borgerens folkeregisteradresse ved brev.

Certifikatet udstedes ved borgerens indtastning af PIN-koden på certificeringscenterets hjemmeside og kan herefter anvendes i kommunikationen med offentlige myndigheder, hvor det tjener som bevis for borgerens identitet. Via certifikatet kan der nu opnås adgang til fortrolige og følsomme oplysninger om den borger, i hvis navn certifikatet er udstedt.

Misbrug kan således forekomme ved, at et certifikat bestilles uretmæssigt i en andens navn, at PIN-koden til et bestilt certifikat tilegnes uretmæssigt, samt ved at et certifikat anvendes til uretmæssigt at tilegne sig oplysninger om den, i hvis navn certifikatet er udstedt.

Datatilsynet overvejede, hvorvidt den foreslåede bestemmelse i udkastets § 1, nr. 10, kunne tænkes anvendt f.eks. ved uretmæssig anskaffelse af et OCES-certifikat, og tilsynet foreslog, at spørgsmålet herom indgik i ministeriets overvejelser, eventuelt med henblik på nærmere præcisering i lovforslagets bemærkninger.

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

Disse regler fører efter Datatilsynets opfattelse til, at udbydere af telenet og teletjenester kun må behandle oplysninger, som udbyderne selv har et aktuelt behov for af hensyn til varetagelse af deres egne (civile) formål. Udbyderne må også kun opbevare oplysningerne, så længe de selv har behov for dem af hensyn til varetagelse af deres egne (civile) formål, jf. persondatalovens § 5, stk. 5.

Udbydere af telenet og teletjenester kan således ikke i henhold til persondatalovens regler behandle oplysninger alene med henblik på politiets retshåndhævelse, dvs. med den begrundelse, at politiet i efterforskningsmæssig sammenhæng kan få behov for dem.

En behandling med henblik på politiets retshåndhævelse kræver derfor en særskilt lovhjemmel. Ud fra hensynet til privatlivets fred var det Datatilsynets opfattelse, at en særskilt hjemmel, hvorefter det kan pålægges udbydere af telenet og teletjenester at behandle oplysninger i videre omfang, end hvad der følger af persondataloven, kun bør tilvejebringes, hvis vægtige samfundsmæssige hensyn taler herfor. Datatilsynet fandt ikke at burde udtale sig om, hvorvidt dette er tilfældet.

Hvis der tilvejebringes regler, hvorefter udbydere af telenet og teletjenester kan pålægges at opbevare f.eks. indholdsmæssige data vedrørende e-brevskommunikation af hensyn til en konkret efterforskning, var det Datatilsynets opfattelse, at dette bør ske med skyldig hensyntagen til privatlivets fred og de generelle principper for god databehandlingsskik, som følger af persondatalovens § 5. I den forbindelse henviste Datatilsynet navnlig til principperne om saglighed og proportionalitet.

Datatilsynet noterede sig, at det af bemærkningerne fremgik, at politiet forudsættes at foretage en proportionalitetsafvejning ved anvendelse af den foreslåede bestemmelse i retsplejeloven, således at et pålæg om hastesikring alene omfatter de data, som er nødvendige for efterforskningen af den konkrete sag, og at politiet således i almindelighed forudsættes at foretage en afgrænsning i tidsmæssig henseende af den bagudrettede periode, som pålægget om hastesikring skal omfatte, eksempelvis hastesikring af data for 1 uge.

Den foreslåede bestemmelse havde som følge af de lave krav til indikation og kriminalitet et meget bredt anvendelsesområde. Der var samtidig tale om et væsentligt indgreb i privatlivets fred, navnlig henset til at der var tale om sikring af såvel indholdsdata som trafikdata. Disse forhold understregede efter Datatilsynets opfattelse behovet for, at proportionalitetshensyn tillægges betydelig vægt ved anvendelsen af bestemmelsen. Datatilsynet henstillede derfor, at der i selve bestemmelsen indsættes en henvisning til proportionalitetsprincippet.

Enkelte medlemmer af Datarådet gav i den forbindelse udtryk for, at indgrebet alene bør kunne ske efter forudgående retskendelse.

Datatilsynet fandt under alle omstændigheder, at hastesikringsperioden bør være så kort som mulig, og at dette bør fremgå af lovforslaget. Tilsynet var

opmærksom på, at implementering af bestemmelsen i konventionens art. 29, stk. 7, sætter visse rammer for periodens længde i sager omfattet af artiklen, men dette burde imidlertid ikke føre til, at der generelt opereres med en hastesikringsperiode på 90 dage. Der henvistes i den forbindelse særligt til, at der i de almindelige bemærkninger var anført, at "Sikringsperioden foreslås fastsat til 90 dage i overensstemmelse med artikel 16 i Europarådets konvention om IT-kriminalitet".

Efter Datatilsynets opfattelse fremgik det ikke klart af den foreslåede bestemmelse eller af bemærkningerne hertil, hvorvidt et pålæg om hastesikring kan gentages eller forlænges ved pålæggets udløb, eller om der kan udstedes daglige pålæg, hvorved indgrebet reelt gøres fremadrettet og dermed nærmest må sidestilles med indgreb som telefonaflytning og dataaflæsning.

Henset til bestemmelsens indgribende karakter samt til, at hensynet til tidsfaktoren ikke kan formodes at gøre sig gældende med samme vægt i en gentagelsessituation, lagde Datatilsynet umiddelbart til grund, at pålæg om hastesikring af de samme data ikke kan gentages eller forlænges.

Hvis dette – mod forventning – skulle være tilfældet, anbefalede Datatilsynet – af hensyn til effektiv sikring af proportionalitetsprincippets iagttagelse – at kompetencen til at udstede pålægget i gentagelsestilfælde tillægges domstolene, således at anvendelsen af bestemmelsen i sådanne tilfælde undergives en forudgående legalitetskontrol.

Datatilsynet forudsatte i øvrigt, at enhver videregivelse af personoplysninger til udenlandske myndigheder inden for rammerne af Europarådets konvention om IT-kriminalitet sker under iagttagelse af persondatalovens krav, herunder kravet om at enhver behandling af personoplysninger skal have et sagligt formål og ikke omfatte mere end nødvendigt af hensyn til formålet med behandlingen.

Datatilsynet pegede endelig på, at anvendelse af bestemmelsen i nogle situationer vil rejse spørgsmål om, hvem der skal anses for dataansvarlig for hastesikrede data. Dette vil f.eks. gøre sig gældende for så vidt angår sikring af kommunikationsindholdet af e-post.

Almindeligvis må brugeren anses som dataansvarlig for indholdet af de e-breve, som opbevares af udbyderen på brugerens vegne. Ved en hastesikring heraf, som må formodes at ske uden brugerens vidende, sker opbevaringen således ikke længere på brugerens vegne, ligesom denne ikke har rådighed over oplysningerne. Forud for en retskendelse om udlevering af oplysningerne

har politiet imidlertid heller ikke adgang til eller rådighed over de sikrede oplysninger, selv om opbevaringen sker på politiets foranledning.

Spørgsmålet om dataansvar kan navnlig få betydning for håndhævelse af et effektivt tilsyn med behandlingen af oplysningerne. Datatilsynet påpegede i den forbindelse, at personoplysninger, som er tilvejebragt gennem straffeprocessuelle tvangsindgreb, skal behandles og sikres i overensstemmelse med reglerne i persondataloven, hvis oplysningerne behandles ved hjælp af elektronisk databehandling eller indgår i et manuelt register, og at opbevaringen af hastesikrede data vil kunne indebære behandling af følsomme oplysninger omfattet persondatalovens §§ 7 og 8.

Datatilsynet fandt derfor, at der bør tages stilling til spørgsmålet om dataansvar for de hastesikrede oplysninger, og at dette eventuelt bør fremgå af bemærkningerne til bestemmelsen.

Lov om offentlige betalinger (etablering af NemKonto mv.)

Kammeradvokaten anmodede på vegne af Finansministeriet Datatilsynet om bemærkninger til forslag til lov om offentlige betalinger mv. (Etablering af Nemkonto mv.).

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

1. Lovforslaget forudsatte bl.a. etableringen af et såkaldt NemKonto-system indeholdende et "NemKonto-register" med oplysninger om hovedparten af den voksne danske befolknings pengeinstitutkonti. Formålet var at sikre det offentlige adgang til nødvendige kontooplysninger med henblik på at foretage udbetalinger til kontoindehaverne med frigørende virkning uden anvendelse af checks, fakturaer mv.

Efter Datatilsynets opfattelse måtte oprettelsen af et NemKonto-register som beskrevet i lovforslaget siges at tjene et sagligt formål, nemlig at gennemføre en række effektiviseringsinitiativer med efterfølgende ressourcebesparelser.

Det centrale spørgsmål var herefter efter Datatilsynets opfattelse, om den valgte løsning, som indeholdt en omfattende registrering, stod i rimeligt forhold til formålet, jf. persondatalovens § 5.

2. Datatilsynet fandt, at en række forhold havde betydning for denne vurdering:

- Det fremgik af lovforslaget og bemærkningerne hertil, at registrering i NemKonto-registeret for så vidt var frivillig i den forstand, at de borgere, der ikke umiddelbart skulle modtage udbetalinger fra det offentlige, ikke havde pligt til at angive en NemKonto.

- Der bestod efter Datatilsynets opfattelse en vis risiko for ophobning af data uden et aktuelt sagligt behov, idet NemKonto-registeret måtte antages at ville indeholde visse oplysninger, som der ikke var et aktuelt behov for, at offentlige myndigheder besad. F.eks. ville oplysninger om NemKonti tilhørende personer, der kun meget sjældent modtog udbetalinger fra det offentlige, kunne stå registreret i en vis periode ud over det tidsrum, som saglige behov tilsagde. Dette måtte imidlertid sammenholdes med, at de eksisterende decentrale registre, som indeholder borgeres kontooplysninger, fremover ville blive overflødige.

- Datatilsynet noterede sig, at det var tilkendegivet af Finansministeriet, at der ville blive etableret en løsning, hvor NemKonto-systemet selv kæder en oplysning om, at udbetaling skal foretages til en nærmere identificeret borger, sammen med oplysningen om dennes NemKonto. Den enkelte sagsbehandler i de offentlige myndigheder behøver således ikke at få adgang til kontooplysningen.

- Der opstod endelig efter Datatilsynets opfattelse et spørgsmål om fastsættelsen af en sletningsfrist. Ved fastsættelsen af en sletningsfrist var der mulighed for at sikre den del af de registrerede, der inden for et nærmere fastsat tidsrum ikke modtog andre udbetalinger fra det offentlige end den registreringsudløsende udbetaling, mod at skulle stå registreret i NemKonto-registeret på ubestemt tid.

3. Samlet set fandt Datatilsynet, at de i persondatalovens § 5 indeholdte krav til proportionalitet, saglighed og ajourføring var opfyldt. Dette forudsatte dog efter Datatilsynets opfattelse, at der sker en løbende ajourføring af NemKonto-registerets indhold, og at de enkelte medarbejdere i de offentlige myndigheder, som påtænkes tilsluttet NemKonto-systemet, ikke får adgang til oplysningerne om konkrete pengeinstitutkonti indeholdt i NemKonto-registeret.

Datatilsynet fandt samtidig, at bestemmelserne i persondatalovens § 5 tilsagde, at oplysninger om ubenyttede NemKonti ikke kunne opbevares på ubestemt tid.

Idet Finansministeriet havde oplyst, at blot en meget lille gruppe af registrerede ikke modtager pengebeløb fra det offentlige inden for f.eks. en 5-årig periode, fandt Datatilsynet, at en sletningsfrist for registeret efter tilsynets opfattelse passende kunne fastsættes til 5 år.

Da lovforslaget tillige indebar oprettelsen af en fælles administration af offentlige kontaktkasser, henledte tilsynet opmærksomheden på persondatalovens kapitel 11 samt de i sikkerhedsbekendtgørelsen indeholdte regler vedrørende autorisation og adgangskontrol.

Offentlighed i retsplejen

Justitsministeriet anmodede Datatilsynet om en udtalelse om betænkning nr. 1427 om "Offentlighed i civile sager og straffesager" og efterfølgende om en udtalelse om et revideret udkast til lovforslag om ændring af retsplejeloven og forskellige andre love (offentlighed i retsplejen).

Datatilsynets udtalelser gengives i alt væsentligt nedenfor:

1. I overensstemmelse med betænkningen lagde lovforslaget op til en væsentlig udvidelse af adgangen til aktindsigt i domme og kendelser i retssager. Det var således Datatilsynets vurdering, at forslaget ville medføre *videregivelse* af en stor mængde personoplysninger af fortrolig og følsom karakter, hvilket i sig selv gav anledning til databeskyttelsesretlige overvejelser.

Hertil kom, at forslaget efter Datatilsynets opfattelse kunne medføre en øget risiko for *indsamling og opbevaring* af følsomme oplysninger, herunder oplysninger om strafbare forhold, i strid med persondatalovens regler, jf. nedenfor under pkt. 2.

Med hensyn til forslaget om at give enhver adgang til aktindsigt i *straffedomme* indtil 1 år efter sagens afslutning henviste Datatilsynet navnlig til, at oplysninger om bl.a. strafbare forhold i forhold til den offentlige forvaltning karakteriseres som følsomme med deraf følgende behov for at sikre et højt beskyttelsesniveau i forhold til privatlivets fred og den enkelte borgers integritet. Oplysningerne kan som følge heraf kun videregives, hvis de strenge betingelser i persondatalovens § 8, stk. 2, er opfyldt.

For så vidt angik videregivelsen af følsomme oplysninger i forbindelse med *civile* sager fremgik det af det reviderede lovforslags bemærkninger, at reglerne om aktindsigt var udtryk for en vis fravigelse af princippet i persondatalovens § 7 og endvidere af databeskyttelsesdirektivets[13] hovedregel om behandling af visse følsomme personoplysninger. Lovforslaget indebar således, at domstolene i forbindelse med meddelelse af aktindsigt ville skulle videregive følsomme oplysninger i videre omfang, end hvad der ville følge af persondatalovens § 7.

Denne fravigelse var ifølge Justitsministeriet velbegrundet. Formålet med den foreslåede almindelige adgang til aktindsigt i domme og kendelser mv. var således – i overensstemmelse med princippet i grundlovens § 65, stk. 1, om

[13] *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*

videst mulig offentlighed i retsplejen – at udvide adgangen til indsigt i retssager, så reglerne herom kunne leve op til kravene i et moderne rets- og informationssamfund.

Det var endvidere anført i bemærkningerne, at lovforslaget om aktindsigt indeholdt en række begrænsninger og undtagelser, der særligt var udformet med henblik på bl.a. hensynet til persondatabeskyttelse og beskyttelsen af følsomme personoplysninger. Der blev endvidere henvist til, at de foreslåede regler i vidt omfang var begrundet i domstolenes særlige forfatningsmæssige stilling og centrale rolle i retsvæsenet, som efter ministeriets opfattelse kunne begrunde, at domstolenes afgørelser som udgangspunkt burde være tilgængelige for enhver.

Om forholdet til databeskyttelsesdirektivets artikel 8 havde Justitsministeriet anført, at offentlighed i retsplejen var en vigtig samfundsmæssig interesse, jf. direktivets art. 8, stk. 4. Ministeriet fandt, at de foreslåede regler indeholdt "tilstrækkelige garantier", jf. art. 8, stk. 4, som følge af, at der i vidt omfang ville ske anonymisering, at der i vidt omfang ville ske forudgående høring af den person, som oplysningerne vedrørte, at afgørelsen blev truffet af domstolene som led i deres judicielle virksomhed, og at den efterfølgende behandling skulle ske i overensstemmelse med persondatalovens regler.

Datatilsynet fandt, at hensynet til offentlighed i retsplejen meget nøje måtte afvejes i forhold til hensynet til beskyttelsen af følsomme personoplysninger. Forslaget havde efter tilsynets opfattelse databeskyttelsesretlige konsekvenser, der af den enkelte borger ville kunne opleves som en forringelse af beskyttelsesniveauet og en krænkelse af den personlige integritet, f.eks. ved at følsomme oplysninger ville blive videregivet i skriftlig form til uvedkommende personer. Datatilsynet pegede i den forbindelse også på, at de begrænsninger i og undtagelser til aktindsigt, der blev lagt op til i forslaget, havde undtagelsens karakter og i vidt omfang beroede på en konkret vurdering i det enkelte tilfælde.

Forslaget gav således anledning til afvejning af væsentlige og i nogen grad indbyrdes modstridende hensyn. Det måtte derfor efter Datatilsynets opfattelse bero på en politisk vurdering af de forskelligrettede hensyn, om det foreliggende forslag skulle gennemføres.

Som alternativ til de foreslåede aktindsigtsregler pegede Datatilsynet på muligheden for, at domstolenes videregivelse kunne ske i overensstemmelse med de principper, der er udviklet i forbindelse med oprettelse af retsinformationssystemer, jf. persondatalovens § 9.

2. Lovforslaget tilsigtede ikke at regulere *modtagerens* behandling af de oplysninger, som vedkommende havde fået gennem aktindsigt (bortset fra en

særlig regel om offentliggørelse af domme og kendelser i straffesager, jf. nedenfor under pkt. 3).

I det omfang oplysninger, som en person havde fået i hænde gennem aktindsigt, ville være omfattet af persondatalovens anvendelsesområde, ville det således ifølge bemærkningerne være persondatalovens regler, der skulle regulere modtagerens behandling af oplysningerne.

Datatilsynet gjorde opmærksom på, at persondataloven ikke finder anvendelse på behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter, jf. lovens § 2, stk. 3.

Datatilsynet vurderede imidlertid, at der hos en række modtagere, f.eks. interesseorganisationer, advokater og privatpersoner med interesse i at følge retspraksis, ville ske behandling af personoplysninger omfattet af persondatalovens anvendelsesområde, fordi der var tale om en mere systematisk behandling eller behandling i erhvervsmæssig sammenhæng.

De pågældende modtageres *indsamling og opbevaring* af personoplysninger ville derfor indebære en behandling i persondatalovens forstand, hvilket vil medføre, at lovens behandlingsregler mv. vil skulle være opfyldt. Hvis der er tale om følsomme personoplysninger omfattet af lovens §§ 7 og 8, er der meget strenge betingelser for, at behandlingen overhovedet vil kunne finde sted, ligesom behandlingen vil forudsætte anmeldelse til og tilladelse fra Datatilsynet.

Datatilsynet er overordentlig tilbageholdende med at give tilladelse til privates registrering og opbevaring af oplysninger om strafbare forhold, jf. lovens § 8, stk. 4. Det forhold, at en modtager har en almindelig interesse i at følge med i retspraksis, kan efter tilsynets praksis ikke i sig selv begrunde, at behandlingen ligger inden for de meget snævre rammer for registrering af følsomme oplysninger uden samtykke.

Datatilsynet fandt derfor, at adgangen til aktindsigt i domme og kendelser mv. vil kunne indebære en øget risiko for, at der vil ske indsamling, opbevaring og anden behandling af følsomme personoplysninger i strid med persondatalovens regler. Det blev i den forbindelse bemærket, at det formentlig ikke vil forekomme modtagerne særligt indlysende, at domme og kendelser mv. kan videregives fra domstolene, men ikke uden videre kan opbevares lovligt hos modtagerne.

Datatilsynet fandt på denne baggrund, at denne problemstilling i det mindste udtrykkeligt skulle omtales i bemærkningerne til lovforslaget.

Datatilsynet gjorde samtidig opmærksom på, at tilsynet ikke vil have mulighed for at føre en særskilt kontrol på dette område.

3. Lovforslaget regulerede på et enkelt område *modtagerens* behandling, idet forslaget indeholdt en regel vedrørende offentliggørelse af domme og kendelser i straffesager.

Der fastsattes en pligt til at anonymisere ved offentliggørelse af domme og kendelser i straffesager. Denne pligt skulle ikke gælde i civile sager, ligesom bestemmelsen ikke skulle finde anvendelse på retsinformationssystemer, der var omfattet af § 9 i persondataloven, eller på offentlig gengivelse, der byggede på et sådant retsinformationssystem. Undtagelsen vedrørende retsinformationssystemer var tilføjet i det reviderede lovforslag.

Det var tilsynets vurdering, at den anonymisering, der var tale om, ikke udgjorde en fuldstændig anonymisering. Dokumenterne måtte derfor fortsat siges at indeholde personhenførbare oplysninger og dermed være omfattet af persondataloven.

Ud over de databeskyttelsesretlige betænkeligheder, der knyttede sig til offentliggørelse af straffedomme mv. med personhenførbare oplysninger (omtalt under pkt. 1), var det Datatilsynets opfattelse, at det kan give anledning til fortolkningsvanskeligheder, at det i lovforslaget blev lagt til grund, at det er persondatalovens regler, der vil finde anvendelse på modtagerens anvendelse af oplysninger, når forslaget tillige indeholdt en regel, der regulerer modtagerens offentliggørelse af domme og kendelser i straffesager.

Datatilsynet gjorde i den forbindelse særligt opmærksom på, at det er tilsynets praksis, at offentliggørelse af personoplysninger på internettet ikke kan anses for en aktivitet af rent privat karakter.

4. Datatilsynet noterede sig, at Justitsministeriet i bemærkningerne til det reviderede lovudkast lagde til grund, at databeskyttelsesdirektivet ikke finder anvendelse på lovforslagets regler om aktindsigt i straffesager, idet meddelelse af aktindsigt i en straffesag efter Justitsministeriets opfattelse må anses for omfattet af medlemsstaternes "aktiviteter på det strafferetlige område", jf. direktivets art. 3, stk. 2, 2. pind.

Rækkevidden af direktivets artikel 3, stk. 2, 2. pind, i forhold til spørgsmålet om aktindsigt i straffesager er ikke afklaret i praksis. Datatilsynet havde imidlertid ikke på det foreliggende grundlag anledning til at anlægge en anden vurdering end Justitsministeriet af dette spørgsmål.

Af bemærkningerne fremgik endvidere, at Justitsministeriet havde lagt til grund, at databeskyttelsesdirektivet omfatter domstolenes behandling af civi-

le sager, men at det er uafklaret, om direktivet overhovedet har betydning for spørgsmålet om meddelelse af aktindsigt til tredjemand.

Datatilsynet noterede sig i den forbindelse, at ministeriet uanset det anførte havde indsat bemærkninger om forholdet til databeskyttelsesdirektivet ved udformningen af det reviderede lovforslag med bemærkninger.

Datatilsynet bemærkede, at man gik ud fra, at Justitsministeriet var opmærksom på spørgsmålet om underretning af Kommissionen, jf. databeskyttelsesdirektivets art. 8, stk. 6.

5. Datatilsynet noterede sig i øvrigt, at adgangen til aktindsigt i sagsdokumenter mv. var indskrænket betydeligt i forhold til det oprindelige udkast. Det reviderede forslag gav ikke tilsynet anledning til bemærkninger.

6. Datatilsynet noterede sig endeligt, at Justitsministeriet ville udforme en bekendtgørelse vedrørende retslister og henviste til, at rettens udlevering af ikke-offentliggjorte elektroniske retslister, ville være en behandling omfattet af persondatalovens regler.

Ændring af lov om finansiel virksomhed

På Finanstilsynets anmodning afgav Datatilsynet i 2003 tre høringssvar over forslag til ændringer af lov om finansiel virksomhed vedrørende udveksling af oplysninger om erhvervskunder til brug for risikostyring, herunder kreditvurdering og kreditadministration.

Finanstilsynet havde i bemærkningerne anført, at det seneste forslag adskilte sig fra de tidligere forslag ved, at forslaget nu alene omfattede udveksling af oplysninger mellem koncernforbundne penge- og realkreditinstitutter mv. De tidligere forslag omfattede også udveksling af oplysninger med forsikringsselskaber, investeringsforvaltningsselskaber og fondsmæglerselskaber. Ændringen medførte dels en væsentlig reduktion af antallet af virksomheder, der kunne videregive oplysninger efter bestemmelsen, dels en væsentlig reduktion i, hvilke type oplysninger der kunne videregives, fordi der alene kunne videregives oplysninger indsamlet af kreditinstitutter, dvs. penge- og realkreditinstitutter.

Til brug for Datatilsynets behandling af sagen havde Finanstilsynet på forespørgsel supplerende oplyst, at den omstændighed, at danske penge- og realkreditinstitutter ikke må drives i samme virksomhed, intet har med videregivelse af fortrolige oplysninger at gøre. Kravet skyldes, at der i Danmark traditionelt har været ønske om, at realkreditobligationer skal være en sikker investering. Realkreditinstitutter er derfor underlagt strenge krav om, at de kun må låne penge ud mod pant i fast ejendom, og der er grænser for, hvor meget forskellige ejendomstyper må belånes. Almindelige huse må belånes

med 80 % af ejendomsværdien, mens f.eks. industriejendomme kun må belånes med 60 %. Pengeinstitutter er ikke underlagt tilsvarende restriktioner. Ved at holde de to instituttyper adskilt sikres det, at de obligationer, realkreditinstitutterne udsteder for at finansiere instituttets udlån (realkreditobligationerne), er sikre værdipapirer.

Efter at sagen havde været behandlet på et møde i Datarådet, udtalte Datatilsynet, at det reviderede forslag til § 120 a i lov om finansiel virksomhed ikke gav anledning til databeskyttelsesretlige betænkeligheder i samme omfang som de tidligere forslag.

Datatilsynet lagde vægt på, at adgangen til at udveksle oplysninger var begrænset i forhold til tidligere forslag, således at der efter den foreslåede bestemmelse ikke kan ske videregivelse af fortrolige oplysninger om erhvervskunder til og fra forsikringsselskaber, ejendomsmæglervirksomheder, investeringsforvaltningsselskaber og fondsmæglerselskaber. Tilsynet lagde herved til grund, at forslaget indeholdt en udtømmende opregning af, hvilke selskaber der kan udveksles oplysninger mellem.

Datatilsynet lagde desuden vægt på, at begrænsningen i dansk lovgivning om, at penge- og realkreditinstitutvirksomhed ikke må drives i samme virksomhed, ifølge bemærkningerne ikke findes i andre europæiske lande, og at forslaget således bidrog til, at danske penge- og realkreditinstitutter fik mulighed for at foretage risikostyring på linie med finansielle virksomheder i andre lande.

Ved vurderingen af forslaget noterede Datatilsynet sig endvidere, at der i lovforslagets bemærkninger udtrykkeligt var henvist til persondatalovens § 5. Dette indebærer bl.a., at persondatalovens proportionalitetsprincip vil skulle iagttages i forbindelse med konkrete videregivelser af oplysninger. Efter Datatilsynets opfattelse gav lovforslaget således ikke i ethvert tilfælde adgang til at videregive *alle* de i forslaget omtalte oplysninger om erhvervskunder.

Datatilsynet gjorde i den forbindelse navnlig opmærksom på, at oplysningernes alder skulle tages i betragtning. Videregivelse af oplysning om forhold, der ligger et stykke tid tilbage i tiden, vil efter Datatilsynets opfattelse ikke i alle tilfælde være forenelig med persondatalovens § 5.

Datatilsynet bemærkede, at spørgsmål om, hvorvidt en konkret udveksling af oplysninger om erhvervskunder mellem koncernforbundne penge- og realkreditinstitutter er i overensstemmelse med persondatalovens § 5, vil kunne efterprøves af Datatilsynet i forbindelse med en klagesag.

Datatilsynet lagde endvidere til grund, at den ønskede videregivelse kan ske elektronisk, og at forslaget ville give mulighed for samkøring eller sammen-

stilling af oplysninger fra de omhandlede virksomheder. Tilsynet foreslog, at det i bemærkningerne blev præciseret, at en sådan samkøring eller sammenstilling af oplysninger vil kunne ske.

Datatilsynet fandt i den forbindelse anledning til at understrege vigtigheden af, at kun en begrænset personkreds i de berørte virksomheder fik adgang til de sammenstillede/samkørte oplysninger. Der bør således altid foretages en vurdering af nødvendigheden af at have adgang til de fortrolige kundeoplysninger, og der bør etableres autorisationsprocedurer og passende kontrolforanstaltninger for at begrænse adgang til oplysningerne til færrest mulige. Datatilsynet fandt det hensigtsmæssigt, at der i lovforslagets bemærkninger udtrykkeligt blev gjort opmærksom på ovennævnte forhold.

Ændring af tinglysningsloven

Justitsministeriet anmodede Datatilsynet om en udtalelse om udkast til lovforslag om ændring af tinglysningsloven, hvorefter forbudet mod samkøring af – og masseudtræk fra – tinglysningsregistrene blev foreslået ophævet.

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

Ved vurderingen af, om og i hvilken form videregivelse kan ske inden for rammerne af persondataloven, burde det efter Datatilsynets opfattelse inddrages, hvad oplysningerne efterfølgende tænkes anvendt til.

Datatilsynet fandt på denne baggrund anledning til at rejse spørgsmål om, hvilken kontrol domstolene skal føre med videregivelse fra tinglysningsregistrene, og tilsynet henstillede, at dette spørgsmål blev omtalt i lovforslaget.

Datatilsynet lagde til grund, at de dataansvarlige, der indhenter oplysninger fra tinglysningsregistrene, vil skulle iagttage såvel persondataloven som tinglysningslovens § 50 c, stk. 7, og at Datatilsynet som tilsynsmyndighed vil skulle påse lovligheden heraf.

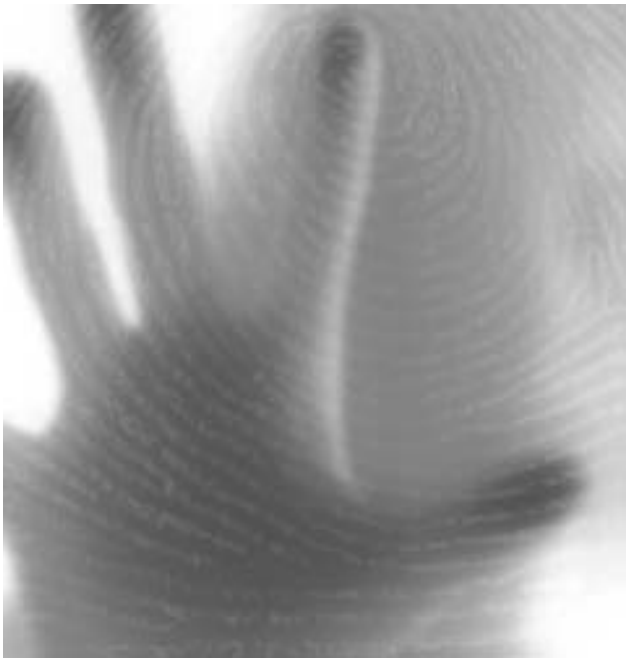
I praksis måtte det efter Datatilsynets opfattelse føre til, at Datatilsynet ved vurderingen af, om behandlingen er lovlig efter persondatalovens regler, må inddrage de begrænsninger i mulighederne for at samkøre oplysninger, som følger af reglen i tinglysningslovens § 50 c, stk. 7.

Datatilsynet kunne i øvrigt umiddelbart tilslutte sig, at kravene i persondatalovens §§ 5 og 6 normalt vil være opfyldt ved udtræk fra tinglysningsregistrene og efterfølgende samkøring til de i tinglysningslovens § 50 c, stk. 7, angivne formål.

Datatilsynet bemærkede imidlertid, at formuleringen i tinglysningslovens § 50 c, stk. 7, 'retsforhold i øvrigt' forekom Datatilsynet noget uklar og burde overvejes nærmere præciseret i bemærkningerne til lovforslaget.

Datatilsynet bemærkede endvidere, at tinglysningslovens § 50 c i visse tilfælde skal suppleres med persondatalovens regler, navnlig når disse giver de registrerede en bedre retsstilling. Dette kan f.eks. være tilfældet ved kreditoplysningsbureauers behandling af personoplysninger, som er særskilt reguleret i persondatalovens kapitel 5 og 6.

Datatilsynet noterede sig Justitsministeriets tilkendegivelse om, at oplysningerne ikke påtænkes videregivet via offentliggørelse på internettet. Datatilsynet fandt i den forbindelse anledning til at tilkendegive, at en sådan videregivelse under alle omstændigheder må anses for svært forenelig med hensynet til en effektiv håndhævelse af anvendelsesbegrænsningerne i tinglysningslovens § 50 c, stk. 7.



Sager om behandling af personoplysninger

Sager om behandling af personoplysninger

Antipiratgruppen

Udtalt, at teleselskaber ikke må videregive oplysninger om deres kunder til Antipiratgruppen uden retskendelse. (Datatilsynets j.nr. 2002-219-0135)

Antipiratgruppen, der er en sammenslutning af brancheorganisationer, forbund og foreninger inden for musik- og filmbranchen, hvis hovedformål er at bekæmpe ulovlig kopiering og distribution, havde som krævet i persondataloven anmeldt sine behandlinger af følsomme oplysninger til Datatilsynet. I den forbindelse havde Datatilsynet udtalt, at det var tilsynets sammenfattende vurdering, at Antipiratgruppens aktiviteter ikke var i strid med persondatalovens regler. Datatilsynet lagde i udtalelsen til grund, at Antipiratgruppen kun behandler oplysninger, som organisationen er kommet i besiddelse af gennem offentligt tilgængelige kilder, eller som organisationen har modtaget ved en lovlig videregivelse, f.eks. efter retskendelse.

På grund af omtale i pressen samt en henvendelse fra Handel, Transport og Serviceerhvervene anmodede Datatilsynet efterfølgende Antipiratgruppen om en redegørelse for gruppens indhentelse af oplysninger fra teleselskaberne. Antipiratgruppen redegjorde for sit samarbejde med teleselskaberne og anmodede samtidig om Datatilsynets stillingtagen til, hvorvidt det vil være i strid med persondataloven, at teleselskaberne – uden indhentelse af retskendelse – udleverer navn og adresse på de af deres kunder, som overtræder ophavsretsloven.

Af sagen fremgik, at det i de fleste sager om krænkelse via internettet alene er muligt at identificere en person, som foretager ulovlig kopiering, via vedkommendes IP-adresse. På baggrund af IP-adressen og eventuelt en tidsangivelse er det muligt for det teleselskab, som har tildelt IP-adressen, at identificere den abonnent, som har haft tilkoblet den computer, hvorfra der er foretaget handlinger i strid med ophavsretsloven. Den enkelte brugers IP-nummer er offentligt tilgængeligt og fremtræder i alle sammenhænge, når en bruger er online på nettet. I relation til eksempelvis brugere af fildelingstjenesten KaZaa sikrer Antipiratgruppen sig således oplysninger om den enkelte brugers IP-nummer og alias samt et skærmprint med oversigt over, hvilke musiknumre, film og/eller spil brugeren i strid med ophavsretsloven har gjort tilgængelig for andre. Antipiratgruppen kan se, hvilken internetudbyder IP-adressen tilhører, og hvorvidt computerejeren er koblet til internettet i Danmark.

Antipiratgruppen anmoder på den baggrund domstolene om at pålægge teleselskaberne at udlevere navn og adresse på personer, som distribuerer piratkopier af film og musik via internettet, jf. retsplejelovens § 299, stk. 1.

Sagen blev behandlet på et møde i Datarådet.

Datatilsynet udtalte, at efter tilsynets opfattelse er sammenhængen mellem en IP-adresse og navn og adresse en oplysning af beskyttelsesværdig karakter. Datatilsynet fandt, at denne oplysning må karakteriseres som fortrolig og dermed omfattet af persondatalovens § 6.

Datatilsynet fandt ikke, at sammenhængen mellem IP-adresse og navn og adresse isoleret set er af en sådan karakter, at den kan henføres under kategorien af følsomme oplysninger i persondatalovens § 8. Dette vil først være tilfældet, når oplysningerne kædes sammen med Antipiratgruppens oplysninger om, at der er sket ulovlig kopiering.

Når der foreligger en retskendelse i medfør af retsplejelovens § 299, stk. 1, vil teleselskabernes udlevering af navn og adresse på kunderne være nødvendig for at overholde en retlig forpligtigelse, jf. persondatalovens § 6, stk. 1, nr. 3.

Med hensyn til spørgsmålet om udlevering af navn og adresse på kunderne uden retskendelse er det den dataansvarlige, der i første række skal foretage en vurdering af, hvorvidt betingelserne for videregivelse i persondatalovens § 6, stk. 1, er opfyldt. Det betyder, at det er det enkelte teleselskab, der i de konkrete sager skal vurdere, hvorvidt betingelserne er opfyldt. I den forbindelse bemærkede Datatilsynet, at persondatalovens regler er "må og kan"-regler. Teleselskaberne har således ikke som følge af persondataloven nogen pligt til at udlevere oplysninger til Antipiratgruppen.

Datatilsynet afgav herefter en vejledende udtalelse om, hvorvidt teleselskaber har mulighed for at videregive uden retskendelse i de omhandlede tilfælde.

Datatilsynet fandt ikke at kunne lægge til grund, at der er samtykke fra kunderne til udlevering af oplysninger. Videregivelse vil således ikke kunne ske efter § 6, stk. 1, nr. 1. Efter Datatilsynets opfattelse kunne der heller ikke uden videre antages at påhvile det dataansvarlige teleselskab en retlig forpligtelse til at udlevere oplysninger om kunder til Antipiratgruppen. Persondatalovens § 6, stk. 1, nr. 3, vil således ikke kunne danne grundlag for videregivelsen. Efter Datatilsynets opfattelse vil udlevering således kun kunne ske, hvis interesseafvejningsreglen i § 6, stk. 1, nr. 7, muliggør dette.

I forhold til interesseafvejningen efter § 6, stk. 1, nr. 7, måtte det lægges til grund, at Antipiratgruppen har en berettiget interesse i at få oplysningerne

fra teleselskaberne. Samtidig måtte det lægges til grund, at udlevering af oplysningerne fra teleselskaberne kan have så betydelige konsekvenser for de registrerede, at der er meget væsentlige hensyn at tage til dem, idet sammenkædningen af oplysningerne om en IP-adresse og Antipiratgruppens materiale fører til oplysninger om formodet strafbart forhold vedrørende en identificeret person.

Efter Datatilsynets opfattelse måtte det endvidere tillægges betydning, at teleselskabernes udlevering til *politiet* af oplysninger om, hvilke kunder der har benyttet en bestemt IP-adresse, ifølge tilsynets oplysninger sker på grundlag af retskendelse. Tilsynet havde samtidig noteret sig, at der i forhold til politiets adgang til oplysninger om kunder med hemmeligt telefonnummer er indsat en særlig hjemmel i lovgivningen[14], således at dette kan ske uden retskendelse. Baggrunden for den særlige hjemmel på dette område var behovet for at skabe en hurtig adgang for politiet til oplysninger om hemmeligt nummer.

Datatilsynet fandt ikke, at sådanne særlige forhold gør sig gældende vedrørende Antipiratgruppens anmodninger om udlevering af oplysninger om IP-adresser. Hertil kommer hensynet til teleselskabernes forhold til kunderne, herunder navnlig den forventning, som kunderne kan have om, at oplysninger om kundeforholdet ikke gøres tilgængelige, medmindre der foreligger retskendelse.

Samlet set fandt Datatilsynet, at der indgår sådanne væsentlige og modsatrettede hensyn i vurderingen af, om teleselskaberne kan udlevere oplysninger om IP-adresse til Antipiratgruppen, at spørgsmålet herom bør forelægges domstolene. Det var derfor Datatilsynets opfattelse, at teleselskaberne ikke kan udlevere oplysninger om IP-adresse efter interesseafvejningsreglen i § 6, stk. 1, nr. 7, uden forudgående retskendelse.

Debatside på internettet

Udtalt, at der skal 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 (Datatilsynets j.nr. 2003-219-148)

En kommune klagede over, at der på hjemmesiden www.borgerdebat.dk var offentliggjort en række oplysninger, herunder karikaturlignende billeder, om én af kommunens ansatte, der i kraft af sin stilling havde deltaget i sagsbehandlingen af en omdiskuteret sag. Selve sagen var på hjemmesiden blevet opkaldt efter den ansatte.

[14] *Lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige*

Redaktøren for hjemmesiden oplyste, at hjemmesiden er en webbaseret nyhedsavis med tilhørende alment og åbent debatforum med debatindlæg indsendt af borgere. Alle indlæg er forsynet med en påtegning om, at synspunkter og udtryk i indlægget står for forfatterens egen regning, og om at indlæg automatisk og ucensureret optages på debatsiden. Med hensyn til de billedlige gengivelser af den ansatte var der ikke tale om fotografier, men om rent grafisk fremstillede illustrationer, dels fremstillet af anerkendte kunstnere som led i deres kunstneriske virksomhed, og dels på Internet Avisernes tegnestue. Der var ingen animationer.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at de oplysninger, som klagen vedrørte, efter tilsynets opfattelse måtte anses for personoplysninger omfattet af persondataloven, idet der var tale om oplysninger om navngivne personer, som blev offentliggjort på internettet ved hjælp af elektronisk databehandling.

Det følger af persondatalovens § 2, stk. 6-9, at loven ikke finder anvendelse på behandlinger, der er omfattet af lov om massemediers informationsdatabaser.

Før en informationsdatabases behandling af personoplysninger kan undtages fra persondataloven, skal Datatilsynet have modtaget en anmeldelse af informationsdatabasen i henhold til lov om massemediers informationsdatabaser § 6, stk. 1. Informationsdatabasen skal ligeledes være anmeldt til Pressenævnet, der herefter har kompetencen til at behandle eventuelle klager.

Pressenævnet havde under sagen oplyst, at www.borgerdebat.dk var anmeldt til Pressenævnet som medie. www.borgerdebat.dk havde ikke anmeldt sig til Datatilsynet, hvorfor tilsynet anså sig for kompetent til at behandle klagen efter persondatalovens regler.

Det fremgår af persondatalovens § 2, stk. 10, at for behandling af oplysninger, som i øvrigt finder sted i journalistisk øjemed, gælder alene lovens §§ 41, 42 og 69.

Bestemmelsen tager ifølge bemærkningerne sigte på den elektroniske behandling af personoplysninger, som udelukkende foretages som led i journalistisk virksomhed i forbindelse med udarbejdelse af artikler mv. under anvendelse af almindelige tekstbehandlingssystemer. Det bemærkes, at databaser mv. alene vil kunne undtages fra lovens område i det omfang, det følger af undtagelsesbestemmelserne i stk. 6-9.

Ifølge forarbejderne er § 2, stk. 10, en følge af, at persondataloven i modsætning til den tidligere registerlovgivning omfatter al behandling af oplysninger og dermed også omfatter løbende journalistisk virksomhed, som ikke nød-

vendigvis indeholdes i et register. Sådan behandling er netop ikke omfattet af persondatalovens § 2, stk. 6-8, medmindre der oprettes en database, der opfylder bestemmelsernes kriterier. Det præciseres dog i bemærkningerne, at der ikke med henvisning til § 2, stk. 10, kan oprettes en database, som ikke opfylder betingelserne i lovens § 2, stk. 6-9, med den konsekvens, at databasen herefter hverken er omfattet af persondataloven eller af medielovene. En informationsdatabase vil således altid enten være omfattet af persondataloven, lov om massemediers informationsdatabaser eller medieansvarsloven.

Efter Datatilsynets opfattelse kunne undtagelsen derfor ikke finde anvendelse, når oplysningerne indgik i en database, som blev offentliggjort på internettet. www.borgerdebat.dk fremstod som en offentligt tilgængelig informationsdatabase indeholdende redaktionelle artikler om lokalpolitiske emner. Databasen ville derfor efter tilsynets opfattelse kun være undtaget fra persondatalovens anvendelsesområde, hvis der var sket anmeldelse til Datatilsynet, jf. § 2, stk. 6.

De oplysninger, der var klagens genstand, måtte efter Datatilsynets opfattelse betragtes som almindelige ikke-følsomme oplysninger omfattet af persondatalovens § 6, og offentliggørelsen skulle vurderes efter § 6, stk. 1.

Datatilsynet fandt, at de regler, der kunne komme på tale i forbindelse med den skete offentliggørelse, var § 6, stk. 1, nr. 1, og § 6, stk. 1, nr. 7, og idet den ansatte efter det oplyste ikke havde givet sit samtykke til offentliggørelsen, vurderede Datatilsynet behandlingen efter interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7.

Efter persondatalovens § 2, stk. 2, finder loven ikke anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10.

Ved vurderingen af, om personoplysninger må offentliggøres f.eks. på internettet, skal hensynet til informations- og ytringsfriheden således medtages i interesseafvejningen for at sikre, at persondatalovens regler ikke unødigt medfører indskrænkninger i disse frihedsrettigheder. Der skal 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.

For så vidt angik offentliggørelsen af den ansattes navn, at sagen blev opkaldt efter den ansatte og kommentarerne om den ansattes person og deltagelse i sagsbehandlingen, fandt Datatilsynet ikke at kunne fastslå, at hensynet til den ansatte oversteg www.borgerdebat.dk´s adgang til og berettigede interesse i at kunne omtale den omhandlede sag og herunder også den ansattes person på hjemmesiden.

Datatilsynet lagde herved navnlig vægt på, at den pågældende hjemmeside i udpræget grad havde karakter af meningstilkendegivelser og subjektive vurderinger af den omhandlede sag, herunder bl.a. af den ansattes rolle i sagen, og at dette måtte stå læsere af hjemmesiden klart.

Datatilsynet fandt således, at hensynet til ytringsfriheden, som med betydelig vægt var indgået i tilsynets vurdering af den konkrete sag, måtte føre til, at der ikke i medfør af persondataloven var grundlag for at gribe ind over for omtalen af den ansatte i kommunen på www.borgerdebat.dk.

Datatilsynet fandt, at tilsvarende forhold gjorde sig gældende for så vidt angik de billedlige gengivelser af den ansatte. Datatilsynet lagde herved vægt på, at billederne i denne sammenhæng var en del af de meningstilkendegivende ytringer på hjemmesiden, og at de måtte opfattes som en form for karikaturtegninger.

Under de foreliggende omstændigheder og henset til, at hensynet til ytringsfriheden også på dette punkt var indgået i tilsynets vurdering, fandtes der ikke at være tilstrækkeligt grundlag for i medfør af persondataloven at gribe ind over for de billedlige gengivelser af den ansatte på hjemmesiden.

Datatilsynet bemærkede afslutningsvist, at tilsynet ikke herved havde taget stilling til, om offentliggørelsen af den ansattes navn og kommentarerne om den ansatte var i strid med anden lovgivning, herunder bestemmelser i medieansvarsloven og i straffelovens kapitel 27 om freds- og æreskrænkelser.

Fingeraftryk på Bornholmerkortet

Udtalt, at et fingeraftryk eller den udregnede værdi af et fingeraftryk, som ligger lagret i et chipkort, er at betragte som en personoplysning omfattet af persondataloven, og at en sådan behandling under visse omstændigheder kan finde sted inden for rammerne af persondatalovens regler (Datatilsynets j. nr. 2003-212-0143)

Datatilsynet modtog en forespørgsel om BornholmsTrafikkens anvendelse af fingeraftryk til identifikation i forbindelse med indførelse af nyt id-kort til pendlere.

BornholmsTrafikken havde indført et nyt person id-rabatkort, "Bornholmerkortet", der var et personligt chipkort indeholdende kundens fingeraftryk. For at få et Bornholmerkort skulle kunden udfylde og underskrive en formular samt oplyse kortnummer og andre relevante data om kundens Dankort eller andet kreditkort.

Ved udstedelse af Bornholmerkort blev der via et "Bio-match-program" udregnet en værdi på 19 målepunkter af kundens fingeraftryk, og det var denne

værdi, der lå i chipkortet. Der lå således ikke en kopi af kundens fingeraftryk i chippen. Ud over værdien af fingeraftrykket indeholdt Bornholmerkortets chip oplysning om kundens kundenummer hos BornholmsTrafikken. Dette kundenummer fandtes ligeledes i BornholmsTrafikkens bookingsystem. Endelig havde Bornholmerkortet et unikt kortnummer trykt på forsiden.

Når en kunde ønskede at rejse, reserverede kunden plads via internet eller telefon. Når kunden kom frem til terminalbygningen, gik kunden direkte til gaten, hvor Bornholmerkortet førtes forbi en kortlæser, der tjekkede, om kundenummeret fandtes i bookingsystemet. Hvis dette var tilfældet, lyste kortlæseren grønt, og kunden kunne herefter sætte sin finger på en scanner. Hvis scanneren kunne matche kundens fingeraftryk med værdien i chippen på Bornholmerkortet, blev kunden herefter givet adgang til færgen. Samtidig hermed blev der udskrevet kvittering for køb af billet og trukket på kundens Dankort/kreditkort.

BornholmsTrafikken oplyste, at der ikke blev opbevaret oplysninger om de udregnede værdier af kundens fingeraftryk, hverken i forbindelse med lagringen af oplysninger på kortet eller i forbindelse med kundens scanning af kort og fingeraftryk ved check-in. Der var således ikke nogen central database med disse oplysninger. Den udregnede værdi blev udelukkende opbevaret på kundens eget kort.

Den overførsel af oplysninger, der skete ved matchningen af den lagrede værdi i chipkortet og scanningen af kundens fingeraftryk, foregik i krypteret form.

Det blev supplerende oplyst, at ifølge teknisk forskrift om optælling og registrering af de ombordværende i passagerskibe skal alle passagerer registreres med navn, nationalitet, køn og fødselsår.

Datatilsynet udtalte, at tilsynet lagde til grund, at de kunder, der indgår aftale med Bornholmstrafikken om erhvervelse af et Bornholmerkort, indgår denne aftale frivilligt og er bekendt med de vilkår, som gælder for aftalen.

Det var Datatilsynets vurdering, at den værdi af kundens fingeraftryk, som ligger lagret i Bornholmerkortet, er at betragte som en personoplysning omfattet af persondataloven. Endvidere var det Datatilsynets opfattelse, at den behandling, der finder sted i forbindelse med såvel lagring af fingeraftryk på chippen (ved udstedelsen) som ved aflæsningen af Bornholmerkort og fingeraftryk ved indcheckning, er behandling omfattet af persondatalovens behandlingsbegreb.

Efter Datatilsynet opfattelse, må et fingeraftryk eller den udregnede værdi af et fingeraftryk anses for en ikke-følsom oplysning omfattet af persondatalovens § 6.

Datatilsynet fandt, at BornholmsTrafikken i forbindelse med lagring af oplysninger på kortet (ved udstedelsen) og i forbindelse med, at kunden identificerer sig ved check-in, kan foretage behandling af oplysninger, hvis kunden har givet sit udtrykkelige samtykke hertil, jf. § 6, stk. 1, nr. 1.

Det var endvidere Datatilsynets opfattelse, at BornholmsTrafikken i forbindelse med lagring af oplysninger på kortet (ved udstedelsen) og i forbindelse med, at kunden identificerer sig ved check-in, kan foretage behandlinger, som er nødvendige for opfyldelsen af den aftale om brug af Bornholmerkortet, som kunden har indgået med BornholmsTrafikken, jf. persondatalovens § 6, stk. 1, nr. 2.

Det var endelig Datatilsynets opfattelse, at hensynet til BornholmsTrafikkens interesse i at sikre entydig identifikation af deres kunder vejede tungere end kundens interesse i, at oplysningerne ikke behandles, og at persondatalovens § 6, stk. 1, nr. 7, således også var opfyldt.

Datatilsynet lagde vægt på, at de kunder, der indgik aftale med BornholmsTrafikken om erhvervelse af et Bornholmerkort, indgik en aftale frivilligt og var bekendt med de vilkår, som gjaldt for aftalen. Datatilsynet lagde endvidere vægt på, at den udregnede værdi af kundens fingeraftryk alene opbevares på kundens eget kort, og at hverken værdien eller fingeraftrykket opbevares eller lagres andre steder.

Endvidere gjorde Datatilsynet opmærksom på, at behandling af personoplysninger skal ske i overensstemmelse med de grundlæggende principper, som er indeholdt i lovens § 5.

Af § 5, stk. 3, følger, at behandlingen af oplysninger skal være relevant og tilstrækkelig og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles. Det betyder, at behandling af oplysninger er undergivet et proportionalitetsprincip.

Det var Datatilsynets opfattelse, at den behandling af oplysninger om kunders fingeraftryk, der skete i forbindelse med BornholmsTrafikkens nye system, ikke var i strid med dette proportionalitetsprincip.

Sammenfattende var det således Datatilsynets vurdering, at den beskrevne behandling af oplysninger om kunders fingeraftryk i forbindelse med "Bornholmerkortet", kunne finde sted inden for rammerne af persondatalovens regler.

Mærsk Olie & Gas A/S's bortvisningsregister

Meddelt Mærsk Olie og Gas A/S, at Datatilsynet var indstillet på at give virksomheden tilladelse til at behandle oplysninger om medarbejdere beskæftiget på offshore installationer i Nordsøen i forbindelse med håndhævelse af virksomhedens alkohol- og narkotikapolitik (Datatilsynets j.nr. 2003-42-0641)

I henhold til persondatalovens § 50, stk. 1, nr. 1, anmodede Mærsk Olie og Gas A/S (Mærsk) Datatilsynet om tilladelse til behandling af personoplysninger i forbindelse med håndhævelse af virksomhedens alkohol- og narkotikapolitik.

Det fremgik af sagen, at Mærsk på sine offshore installationer i Nordsøen beskæftigede ca. 830 personer. Heraf var ca. 25 % ansat hos Mærsk, mens de øvrige var beskæftiget hos leverandører, med hvem Mærsk havde indgået særskilte kontrakter.

Arbejdet med udvinding af råstoffer fra undergrunden var af en sådan karakter, at der var behov for iagttagelse af særlige sikkerhedsforanstaltninger, som dels var fastlagt ved lov og Energistyrelsens bekendtgørelser, dels var fastlagt af Mærsk i medfør af ledelsesretten.

De ansatte, der arbejdede offshore, skulle bl.a. i tilfælde af ulykker kunne varetage en række særlige opgaver såvel under tjenesten som under friperioderne offshore. Det var derfor uforeneligt med tjeneste offshore at være påvirket af alkohol eller narkotiske stoffer.

Det fremgik af Mærsks alkohol- og narkotikapolitik, at hverken alkohol eller euforiserende og lignende stoffer måtte medbringes offshore. Det var ikke tilladt at blive testet positiv (for så vidt angik alkohol var grænsen fastsat til 0,4 promille i blodet), hverken offshore eller ved check-in i lufthavnen forud for offshore tjeneste. Overtrædelse heraf medførte afvisning, hvis overtrædelsen blev konstateret ved check-in, eller hjemsendelse, hvis overtrædelsen blev konstateret offshore, samt forbud mod at opholde sig på enheder opereret af Mærsk i en periode på 5 år regnet fra datoen for afvisning eller hjemsendelse. Var vedkommende beskæftiget i Mærsk, ville der derudover ske afskedigelse uden varsel (bortvisning).

Af anmeldelsen fremgik, at behandlingen omfattede oplysninger om de personer, der var beskæftiget i Mærsk, og som havde ærinde på de af virksomheden drevne havanlæg, samt om de personer, der i henhold til aftale mellem disses respektive arbejdsgivere og Mærsk blev udsendt til havanlæg.

Der ville ske registrering af de testresultater, som overskred de af virksomheden fastsatte grænseværdier for alkohol i blodet, eller som viste indhold af narkotiske eller lignende stoffer. Personlige data for de personer, der blev testet positive, såvel som for de personer, som afviste at lade sig teste, ville

blive registreret. Oplysningerne skulle opbevares og anvendes i forbindelse med ansættelse eller kontrahering af personer til beskæftigelse på virksomhedens havanlæg.

Oplysningerne ville blive videregivet til de pågældende personers arbejdsgivere med henblik på at udelukke disse personer fra beskæftigelse på Mærsks havanlæg for en femårig periode.

Oplysningerne ville blive slettet senest 5 år efter meddelelsen om konsekvenserne af det positive testresultat.

Efter at sagen havde været behandlet på et møde i Datarådet, udtalte Datatilsynet, at det var tilsynets opfattelse, at en oplysning om en medarbejders positive alkohol- og narkotikatest som udgangspunkt må anses for at være en oplysning om "andre rent private forhold" omfattet af persondatalovens § 8. Datatilsynet lagde herved vægt på, at alene det forhold, at en person testes positiv i forhold til den fastlagte alkohol- og narkotikapolitik, ikke kan siges at være en oplysning, som var omfattet af begrebet "helbredsmæssige forhold" i lovens § 7.

Datatilsynet fandt, at Mærsks registrering af oplysninger om resultaterne af medarbejdernes positive alkohol- og narkotikatests var nødvendig af hensyn til virksomhedens interesse i, at medarbejderne på boreplatformene fysisk og psykisk er i stand til at varetage deres arbejdsopgaver, ikke kun af hensyn til medarbejdernes egen sikkerhed, men også af hensyn til kollegernes sikkerhed.

Datatilsynet fandt således, at hensynet til sikkerheden om bord på boreplatformene klart overstiger hensynet til den enkelte ansattes interesse i ikke at blive registreret.

Det var herefter Datatilsynets vurdering, at det er i overensstemmelse med persondatalovens § 8, stk. 4, 2. pkt., at Mærsk registrerer oplysninger om resultaterne af medarbejdernes positive alkohol- og narkotikatests.

For så vidt angik registrering af oplysninger om Mærsks egne ansatte, fandt Datatilsynet endvidere, at kontraktsretlige forhold kan medføre, at Mærsk i medfør af persondatalovens § 8, stk. 6, jf. § 7, stk. 2, nr. 4, kan registrere oplysninger om disse medarbejderes positive alkohol- og narkotikatests.

Datatilsynet lagde herved vægt på, at det efter virksomhedens formaliserede alkohol- og narkotikapolitik ikke er tilladt at blive testet positiv. Mærsk må således kunne registrere de pågældende oplysninger med henblik på at drage ansættelsesretlige konsekvenser af en tilsidesættelse af de fastsatte retningslinjer, herunder fremlæggelse af den fornødne dokumentation i forbindelse med bortvisning af en medarbejder.

Vedrørende vurderingen af, hvorvidt Mærsk kunne videregive oplysninger om medarbejdernes positive alkohol- og narkotikatest, udtalte Datatilsynet, at det var tilsynets opfattelse, at Mærsk i medfør af persondatalovens § 8, stk. 5, 2. pkt., kan videregive oplysninger om en medarbejders positive alkohol- og narkotikatest til den leverandør, hvor den pågældende er ansat. Det var Datatilsynets vurdering, at videregivelsen er nødvendig for, at Mærsk kan varetage virksomhedens interesse i at sikre, at arbejdet på boreplatformene udføres sikkerheds- og sundhedsmæssigt fuldt forsvarligt, og at virksomhedens interesse heri klart overstiger hensynet til den enkelte ansattes interesse i ikke at få oplysningerne videregivet.

Herefter tog Datatilsynet stilling til, om Mærsk kan behandle oplysninger om henholdsvis afvisning, hjemsendelse eller bortvisning af en medarbejder i forbindelse med dennes manglende overholdelse af virksomhedens alkohol- og narkotikapolitik.

En oplysning om, at en medarbejder er blevet afvist, hjemsendt eller bortvist fra en arbejdsplads, var efter Datatilsynets opfattelse en oplysning om "andre rent private forhold" omfattet af persondatalovens § 8.

Datatilsynet fandt, at Mærsk i medfør af lovens § 8, stk. 4, 2. pkt., kan registrere sådanne oplysninger om henholdsvis egne medarbejdere og medarbejdere ansat hos Mærsks leverandører. Datatilsynet vurderede, at virksomhedens interesse i at kunne varetage sine interesser i tilfælde af et retsligt efterspil klart overstiger hensynet til den ansattes interesse i ikke at blive registreret.

Datatilsynet lagde herved vægt på, at registreringen er nødvendig for, at Mærsk i forbindelse med en sag om uberettiget afvisning, hjemsendelse eller bortvisning kan dokumentere sagligheden af en sådan.

Efter Datatilsynets opfattelse kan Mærsk i medfør af lovens § 8, stk. 5, 2. pkt., endvidere videregive oplysninger om, at en person tidligere er blevet afvist, hjemsendt eller bortvist til dennes arbejdsgiver (leverandøren) i forbindelse med planlægning af tjeneste offshore. Datatilsynet forudsatte herved, at videregivelse alene sker i umiddelbar tilknytning til planlægning af offshore tjeneste og således ikke sker i forbindelse med en leverandørs forestående ansættelse af en medarbejder.

Datatilsynet lagde herved vægt på, at videregivelsen er nødvendig for, at Mærsk kan varetage virksomhedens interesse i at sikre, at arbejdet på havanlæggene kan udføres sikkerheds- og sundhedsmæssigt fuldt forsvarligt, og at virksomhedens interesse heri klart overstiger hensynet til den enkelte ansattes interesse i ikke at få oplysningerne videregivet.

Sager om tv- og videoovervågning

Datatilsynet har i 2003 behandlet en række sager om tv- og videoovervågning. Nedenfor omtales først en sag om offentlige myndigheders tv-overvågning, dernæst omtales 2 sager om privates tv- og videoovervågning foretaget med henholdsvis digitalt og analogt kamera, og endelig omtales en sag om opstilling af web-kameraer ved Vidåslusen.

Offentlige myndigheders tv-overvågning

Udtalt, at persondataloven sætter grænser for, hvor tv-overvågning med digitalt udstyr må foretages af offentlige myndigheder, og hvordan det kan ske. En myndighed, der vil foretage tv-overvågning for at forebygge og afsløre kriminelle aktiviteter, skal anmelde dette til Datatilsynet, og tilsynets udtalelse skal foreligge, inden overvågningen går i gang (Datatilsynets j.nr. 2003-313-0149)

Høje-Taastrup Kommune foretog overvågning af flere af kommunens områder, herunder rådhuset og kommunens institutioner. Kameraerne var indstillet, så de fokuserede på kommunens ejendomme og ikke på offentlige veje og stier, dog var der fri færdsel/adgang for offentligheden til visse af de områder, der blev overvåget. Overvågningen foregik som hovedregel i tidsrummet 18.00 - 06.00 og i tidsrummet 21.00 - 06.00 for institutionernes vedkommende. Kassefunktionen på rådhuset blev imidlertid overvåget hele døgnet, mens Kvikservicekontoret i en ventesal på Hedehusene station blev overvåget i arbejdstiden og i 30 minutter efter arbejdstidens ophør.

Der var opsat synlige skilte ved de arealer, der blev overvåget, men uvedkommende blev ikke gjort bekendt med de nøjagtige områder, hvert enkelt kamera dækkede.

Optagelserne blev lagret i en uge på servere hos et privat firma. To ledende medarbejdere i kommunen havde adgang til optagelserne ved anvendelse af brugernavne og adgangskoder, således at de via nettet kunne logge på serverne og hente billeder fra samtlige kameraer samt søge i arkiverne.

Formålet med overvågningen var at stoppe indbrud og hærværk samt tilføre tryghed til borgerne og de ansatte i kommunen. Formålet med kommunens adgang til optagelserne var derfor også, at der i forbindelse med kriminalitet kunne hentes billeder til politiet. Optagelserne ville efter det oplyste kun blive udleveret til politiet i forbindelse med kriminelle handlinger, hvorefter det var op til politiet at vise billederne til personale mv. i forbindelse med efterforskningen.

Efter at sagen havde været behandlet på et møde i Datarådet, udtalte Datatilsynet indledningsvist, at lov om forbud mod tv-overvågning mv. i § 1, stk. 1,

indeholder et forbud mod, at private foretager tv-overvågning af gade, vej, plads eller lignende område, som benyttes til almindelig færdsel. Modsætningsvis gælder forbudet ikke offentlige myndigheder, som herefter alene er omfattet af lovens skiltningskrav i § 3 a.

Offentlige myndigheders digitale tv-overvågning er imidlertid omfattet af persondataloven, da der sker elektronisk behandling af personoplysninger.

Det var Datatilsynets vurdering, at kommunen inden for rammerne af § 6, stk. 1, nr. 6 og 7, konkret kunne beslutte at iværksætte overvågning under hensyn til, at kommunens opgaver som offentlig myndighed også omfatter forvaltning af offentlige ejendomme og beskyttelse af værdier og ansatte, og at kommunens interesse i at forfølge disse formål på nærmere afgrænsede arealer kan antages at overstige hensynet til ikke at udsætte borgerne for overvågning.

Høje-Taastrup Kommunes formål med tv-overvågningen var at stoppe indbrud og hærværk samt tilføre tryghed til borgere og ansatte. Der var derfor formodning for, at der ved tv-overvågningen tillige bliver behandlet oplysninger om strafbare forhold, som er omfattet af persondatalovens § 8.

Det var Datatilsynets vurdering, at kommunen inden for rammerne af § 8, stk. 1, og stk. 2, nr. 2 og 3, kunne behandle og videregive oplysninger om strafbare forhold til politiet i forbindelse med den iværksatte tv-overvågning under hensyn til, at det er nødvendigt med henblik på kommunens og politiets varetagelse af deres opgaver, ligesom behandlingen af de nævnte oplysninger sker til varetagelse af offentlige interesser, der kan antages klart at overstige hensynet til dem, som oplysningerne vedrører.

Kommunen kunne yderligere foretage behandling af oplysninger om strafbare forhold i det omfang, behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. § 8, stk. 6, jf. § 7, stk. 2, nr. 4.

Datatilsynet fandt imidlertid, at det herved er en *klar* forudsætning, at overvågningen foretages med respekt af persondatalovens grundlæggende krav om proportionalitet mv., jf. persondatalovens § 5, stk. 3, 2. led. I forhold til tv-overvågning fører dette princip efter Datatilsynets opfattelse til, at overvågning skal gennemføres på en sådan måde, at den virker mindst muligt integritetskrænkende for den almindelige borger, og at det i første omgang overvejes, om det ønskede formål kan nås med mindre indgribende midler end en tv-overvågning og registrering.

Datatilsynet fandt derfor, at Høje-Taastrup Kommune i samme omfang som private bør undlade at foretage tv-overvågning af områder, hvor der er almin-

delig færdsel, jf. forbudet fastsat i § 1, stk. 1, i lov om forbud mod tv-overvågning.

Efter Datatilsynets opfattelse bør kommunen herefter undgå tv-overvågning af de områder, hvortil der er adgang for almindelig færdsel, eksempelvis visse parkeringsarealer, uanset at overvågningen kun foretages i aften- og nattetimerne.

Som et yderligere element til at sikre overholdelse af proportionalitetsprincippet skulle der ifølge Datatilsynet ske sletning af foretagne tv-optagelser inden for en vis kortere periode.

Høje-Taastrup Kommune havde under sagen oplyst, at kommunen lagrer optagelser i en uge. Tilsynet fandt, at denne frist opfylder kravet om proportionalitet i forhold til sletning. Med hensyn til optagelser, der indeholder oplysninger om strafbare forhold, var det Datatilsynets opfattelse, at disse kun må opbevares kortvarigt med henblik på politianmeldelse og under forudsætning af, at politianmeldelse foretages snarest muligt. Optagelserne skal afleveres til politiet i forbindelse med anmeldelsen og slettes fra kommunens egne systemer umiddelbart derefter.

Datatilsynet noterede sig i øvrigt, at Høje-Taastrup Kommune som hovedregel begrænser tv-over-vågningen til tidspunkter, hvor der som udgangspunkt ikke er publikum til stede, og at kommunen begrænser adgangen til optagelserne til nogle få medarbejdere. Datatilsynet fandt, at denne praksis er i god overensstemmelse med proportionalitetsprincippet og med sikkerhedsbekendtgørelsens regler.

For så vidt angik kassefunktionen på rådhuset var det Datatilsynets opfattelse, at den her foretagne døgn-overvågning ikke kunne antages at være i strid med persondatalovens grundlæggende principper, herunder proportionalitetsprincippet. Datatilsynet lagde i forbindelse vægt på, at der er tale om kommunens indendørs lokaliteter, ligesom tilsynet tillagde det betydning, at overvågningen sker af hensyn til medarbejdernes sikkerhed og beskyttelsen af kommunens formue.

Tilsvarende gjorde sig gældende for overvågningen af Kvikkassen i ventesalen på Hedehusene Station. Datatilsynet vurderede imidlertid, at det fremsendte billede af kameravinklerne viste, at overvågningen i et vist omfang omfatter et område, der anvendes til gående færdsel, og som dermed har karakter af et offentligt rum. Datatilsynet henstillede derfor, at kommunen fokuserer kameraets vinkel alene på Kvikkassen og den person, der ekspederes og derfor befinder sig i umiddelbar nærhed af kassen.

Efter Datatilsynets opfattelse finder reglerne om oplysningspligt i persondatalovens §§ 28-29 anvendelse ved siden af reglerne i § 3 a i lov om forbud mod tv-overvågning mv.

For så vidt angik kommunens overvågning af borgere, der befinder sig i områderne, hvor der foretages tv-overvågning, var det tilsynets opfattelse, at disse personer allerede via skiltningen efter lov om forbud mod tv-overvågning er blevet informeret om, at der finder tv-overvågning sted. Det var Datatilsynets opfattelse, at yderligere underretning af disse personer må kunne siges at være uforholdsmæssig vanskelig, jf. § 29, stk. 3. Tilsynet lagde i den forbindelse vægt på, at det vil være praktisk umuligt og i hvert fald yderst ressourcekrævende at give hver enkelt person, der kommer inden for kameraernes område, selv en standardmeddelelse indeholdende de påkrævede oplysninger efter § 29, stk. 1. Hertil kommer, at en uddybende tekst indeholdende disse oplysninger i sammenhæng med skiltningen ikke nødvendigvis vil blive bemærket og læst af de pågældende personer.

Datatilsynet fandt derimod ikke, at underretning af Høje-Taastrup Kommunes medarbejdere kunne siges at være uforholdsmæssig vanskelig, jf. § 29, stk. 3. Datatilsynet lagde herved vægt på, at det vil være relativt enkelt at give hver enkelt ansat underretning om de i § 29, stk. 1, nævnte oplysninger. Det vil f.eks. kunne ske i forbindelse med ansættelsen af den enkelte eller på anden vis gennem den daglige kommunikation med de ansatte f.eks. via "kontormeddelelser", medarbejderrepræsentanter eller lignende. Dette gjaldt efter Datatilsynets opfattelse alle de personer, der fast udfører arbejde i lokalerne, uanset om ansættelseskontrakten er indgået med Høje-Taastrup Kommune eller en anden virksomhed, f.eks. et rengøringsfirma. Kommunen kan eventuelt lade den anden virksomhed, som de pågældende er ansat i, give informationen, men det er kommunes ansvar, at meddelelse bliver givet.

De ansatte og andre personer, der udfører arbejde på kommunens område, skal have meddelelse om bl.a. *formålene* med den behandling, hvortil oplysningerne er 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 herefter er at forebygge og opklare også *de ansattes* eventuelle kriminalitet mv., fandt Datatilsynet, at dette skal 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, jf. § 29, stk. 1, nr. 3, litra a-c. Opregningen i litra a-c er ikke udtømmende. Der vil derfor efter omstændighederne kunne påhvile kommunen en pligt til at gi-

ve den registrerede anden information end de oplysninger, som følger af bestemmelserne i litra a-c.

Det var Datatilsynets opfattelse, at det i forlængelse af angivelsen af overvågningens formål vil være naturligt, at meddelelsen indeholder oplysning om, at optagelserne vil kunne blive videregivet til politiet, samt om i hvilke tilfælde det vil kunne ske. Det var desuden tilsynets opfattelse, at der bør gives information om, i hvilke tilfælde optagelserne gennemgås af de to medarbejdere i kommunen, f.eks. om dette finder sted i form af stikprøvekontrol eller i forbindelse med mistanke om kriminelle aktiviteter eller lignende.

Det var endvidere tilsynets opfattelse, at der bør gives de ansatte meddelelse om, hvor længe oplysningerne opbevares.

Tilsynet fandt endelig, at oplysningspligten i § 29 må medføre, at de ansatte bliver informeret om, i hvilke lokaler overvågningen foregår, mens der efter Datatilsynets opfattelse næppe kan stilles krav om, at der bliver givet information om, på hvilke tidspunkter der sker overvågning, herunder at der eksempelvis på nærmere angivne områder sker døgnovervågning.

Ifølge persondatalovens § 43, stk. 1, skal der forinden iværksættelsen af en behandling af oplysninger, der foretages for den offentlige forvaltning, af den dataansvarlige eller dennes repræsentant foretages anmeldelse til Datatilsynet, jf. dog § 44 som fastsætter en række undtagelser til anmeldelseskravet.

Når behandlingen bl.a. omfatter oplysninger, der er omfattet af persondatalovens § 7 og § 8, følger det desuden af persondatalovens § 45, at der skal indhentes en udtalelse fra Datatilsynet inden en behandling, som er omfattet af anmeldelsespligten i § 43, iværksættes.

Offentlige myndigheder skal således foretage anmeldelse af tv-overvågning, der er omfattet af persondatalovens § 1, stk. 1, og som foretages med henblik på at forhindre/forebygge kriminalitet, og i den forbindelse skal Datatilsynets udtalelse indhentes, inden behandlingen iværksættes.

Videoovervågning i S-tog

Givet tilladelse til videoovervågning i S-tog. Lovligheden af overvågningen forudsatte, at overvågningen reelt bidrager til at forbedre passagerernes tryghed og modvirke kriminalitet i og ved S-togene. Datatilsynet forudsatte endvidere, at der blev udarbejdet retningslinjer for, i hvilke tilfælde der vil ske gennemgang af optagelserne og videregivelse heraf til politiet (Datatilsynets j.nr. 2003-42-0523)

Datatilsynet modtog en anmeldelse fra DSB S-tog A/S (DSB) vedrørende videoovervågning i S-togene.

DSB havde besluttet at indføre videoovervågning i S-togene med henblik på at forbedre trygheden blandt passagererne. Videoovervågningen skulle primært være et præventivt middel imod kriminalitet begået i S-tog. I tilfælde af kriminelle handlinger i S-tog ville optagelser blive brugt til efterforskning og som bevismateriale i eventuelle retssager. Der var i første omgang tale om et pilotprojekt, hvor der kun skulle ske kameraovervågning i ét S-tog.

Videoovervågningssystemerne var CCTV-systemer, der optog og gemte alle hændelser i toget 24 timer i døgnet. Alene oplysninger om strafbare handlinger ville blive anvendt – og eventuelt udleveret til politiet – for videre efterforskning. Optagelser ville normalt blive overskrevet efter 7 dage. I forbindelse med straffesager (vold, overfald, hærværk osv.) kunne det komme på tale, at DSB ville gemme optagelser i mere end 7 dage på stærkt krypterede medier til brug ved eventuelle retssager.

DSB oplyste, at en undersøgelse havde vist, at i Göteborg var 80 % af al hærværk i tog og sporvogne forsvundet, efter at der var blevet indført kameraovervågning. DSB forventede således, at hærværk i S-togene ville blive reduceret med 50 % ved indførelsen af kameraovervågning. DSB forventede samtidig, at mindre hærværk ville medføre, at folk følte sig mere trygge i toget, idet man føler sig mere tryg ved at komme ind i et pænt og rent tog.

DSB oplyste desuden, at passagererne ville blive informeret om kameraovervågningen i henhold til lov om forbud mod tv-overvågning. Der ville således blive opsat skilte i togene om, at der skete kameraovervågning. For så vidt angik information af DSB's ansatte havde DSB lavet et sæt "Etiske regler for videosystem i DSB S-tog", som udleveredes til de ansatte. Det fremgik bl.a. heraf, hvornår der sker sletning af optagelserne, hvem der har ret til at gennemse optagelserne, samt hvem der har ret til at få udleveret optagelserne.

Endelig oplyste DSB, at der løbende ville blive målt effekt af kameraovervågningen i relation til hærværk, ligesom der også ville blive samlet op på, om kameraovervågningen i øvrigt havde en kriminalitetsforebyggende effekt.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at det var tilsynets umiddelbare vurdering, at de oplysninger af ikke-følsom karakter, som DSB via kameraovervågningen af passagerer og ansatte behandler om disses færden i S-togene, normalt kan ske i medfør af § 6, stk. 1, nr. 7.

Datatilsynet lagde herved vægt på, at DSB har en berettiget interesse i at forbedre passagerernes tryghed, herunder ved at forsøge at forhindre kriminalitet. Datatilsynet lagde endvidere vægt på, at det ifølge lov om jernbane-

virksomhed mv. må anses som en del af DSB's opgaver at sørge for sikkerhed og orden på jernbaneområdet, herunder i S-togene. Datatilsynet lagde ligeledes vægt på, at kameraovervågning af tog og sporvogne i bl.a. Sverige havde haft betydelig præventiv effekt i forhold til hærværkskriminaliteten.

For så vidt angik de kriminelle handlinger, der sker i S-togene, var det Datatilsynets opfattelse, at DSB med hjemmel i § 8, stk. 4, kan foretage optagelse heraf, samt gennemgang af optagelserne. Datatilsynet lagde i den forbindelse vægt på, at DSB har en berettiget interesse i at forbedre passagerernes tryghed, herunder ved at forsøge at forhindre kriminalitet. Datatilsynet lagde endvidere vægt på, at det ifølge lov om jernbanevirksomhed mv. må anses som en del af DSB's opgaver at sørge for sikkerhed og orden på jernbaneområdet, herunder i S-togene. Endelig lagde Datatilsynet vægt på, at DSB har en berettiget interesse i, at oplysningerne fra overvågningen kan anvendes som dokumentation ved en strafferetlig efterforskning.

Det var ligeledes tilsynets opfattelse, at DSB uden samtykke vil kunne videregive oplysninger fra optagelser af konkrete hændelser, der afslører oplysninger om strafbare forhold, til politiet, jf. § 8, stk. 5, 2. pkt. Datatilsynet forudsatte dog, at der alene sker videregivelse af oplysninger om strafbare forhold, når det er til brug for en strafferetlig efterforskning af forhold over en vis bagatelgrænse.

Datatilsynet henstillede, at DSB snarest muligt opstillede nærmere retningslinier for, i hvilke tilfælde der vil ske gennemgang af optagelserne og videregivelse til politiet, og anmodede samtidig om at modtage en kopi af de pågældende retningslinier, når disse forelå.

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

Efter Datatilsynets opfattelse kunne DSB's behandling af oplysninger om strafbare forhold endvidere ske inden for rammerne af § 7, stk. 2, nr. 4, hvis der i forbindelse med f.eks. hærværk eller en ulykke opstår et erstatningskrav for DSB, den registrerede eller tredjemand.

Ifølge persondatalovens § 29, stk. 1, påhviler det den dataansvarlige at give den registrerede meddelelse om dennes og dennes repræsentants identitet, formålene med den behandling, hvortil oplysningerne er bestemt, samt alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser.

Efter bestemmelsen i § 29, stk. 3, gælder bestemmelsen i stk. 1, ikke, hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssig vanskelig. Med udtrykket uforholdsmæssig vanskelig fastsættes det, at der gælder et proportionalitetsprincip ved vurderingen af, om meddelelse som foreskrevet i lovens § 29, stk. 1, skal gives.

For så vidt angik DSB's videoovervågning af *passagererne* var det Datatilsynets umiddelbare opfattelse, at underretning af disse efter § 29, stk. 1, må anses for uforholdsmæssig vanskelig, jf. § 29, stk. 3. Datatilsynet lagde i den forbindelse vægt på, at passagererne allerede via skiltningen efter lov om forbud mod tv-overvågning er blevet informeret om, at der finder tv-overvågning sted. Desuden lagde Datatilsynet vægt på, at det vil være praktisk umuligt og i hvert fald yderst ressourcekrævende at give hver enkelt rejsende en standardmeddelelse indeholdende de påkrævede oplysninger efter § 29, stk. 1. Hertil kommer, at en uddybende tekst indeholdende disse oplysninger i sammenhæng med skiltningen ikke nødvendigvis vil blive bemærket og læst af passagererne.

Imidlertid fandt Datatilsynet, at DSB i det mindste bør foretage kompensatoriske foranstaltninger ud over skiltningen, f.eks. i form af annoncer i dagblade, pjecer eller lignende, og på den måde informere de rejsende på anden vis end via en individuel meddelelse til hver enkelt.

For så vidt angik underretning af DSB's *personale*, herunder kontrollører og lokomotivførere, fandt Datatilsynet, at underretning ikke kan siges at være uforholdsmæssig vanskelig efter § 29, stk. 3. Datatilsynet lagde herved vægt på, at det vil være relativt enkelt at give hver enkelt ansat underretning om de i § 29, stk. 1, nævnte oplysninger. Det vil f.eks. kunne ske i forbindelse med ansættelsen af den enkelte eller på anden vis gennem den daglige kommunikation med de ansatte, f.eks. via "kontormeddelelser", medarbejderrepræsentanter eller lignende.

I den forbindelse havde Datatilsynet noteret sig, at DSB havde udformet et sæt "Etiske regler for videosystem i DSB S-tog", som det var planen at udlevere til de ansatte. Datatilsynet henstillede, at det af disse etiske regler også fremgår, hvornår der vil ske gennemgang af optagelserne og videregivelse til politiet.

Datatilsynet gav på denne baggrund DSB tilladelse til behandlingen "Videoovervågning i S-tog". Tilladelsen gjaldt indtil årets udgang, idet en forlængelse af tilladelsen krævede en fornyet henvendelse herom til Datatilsynet. Datatilsynet anmodede samtidig om at blive orienteret om pilotprojektets forløb, herunder om kameraovervågningen havde haft den ønskede effekt.

DSB anmodede senere på året Datatilsynet om en permanent tilladelse til videoovervågningen.

DSB havde udarbejdet vejledende retningslinier for gennemgang og videregivelse af optagelserne samt en kortfattet opsamling på de foreløbige erfaringer fra pilotprojektet. Det fremgik bl.a. heraf, at tilbagemeldingerne fra togenes klargøringsafdeling meget gik på, at "toget virker meget mere rent end normalt", eller "det er ikke så ramponeret og hærget som dem uden videoovervågning".

Datatilsynet udtalte, at proportionalitetsprincippet i lovens § 5, stk. 3, i forhold til tv-overvågning efter tilsynets opfattelse fører til, at overvågning skal gennemføres på en sådan måde, at den virker mindst muligt integritetskrænkende for den almindelige borger, og at det i første omgang skal overvejes, om det ønskede formål kan nås med mindre indgribende midler end tv-overvågning og registrering.

Det var i den forbindelse Datatilsynets opfattelse, at den omhandlede videoovervågning - selv om den i øvrigt vil kunne ske i medfør af lovens §§ 6 og 8 - som følge af persondatalovens § 5, stk. 3, kun bør finde sted, hvis den reelt bidrager til at forbedre passagerernes tryghed og modvirke kriminalitet i og ved S-togene. Datatilsynet lagde herved vægt på, at videoovervågningen må anses for et væsentligt indgreb over for passagerer og ansatte.

Datatilsynet meddelte herefter, at tilsynet var indstillet på at meddele DSB tilladelse til behandlingen "Videoovervågning i S-tog".

Idet videoovervågningens lovlighed afhænger af, om den reelt bidrager til at forbedre passagerernes tryghed og modvirke kriminalitet i og ved S-togene, anmodede Datatilsynet om løbende at blive orienteret om videoovervågningens forløb, herunder om videoovervågningen har den forventede effekt.

Datatilsynet har i 2003 også givet DSB tilladelse til kameraovervågning på S-togsstationerne. (Datatilsynets j.nr. 2002-42-0438).

Analog tv-overvågning

Udtalt, at analog tv-overvågning i det konkrete tilfælde kunne anses for omfattet af persondataloven, og at der er oplysningspligt selv om ikke elektronisk databehandling (Datatilsynets j.nr. 2002-219-0110)

En fagforening klagede på vegne af et medlem til Datatilsynet over, at en forretning havde foretaget tv-overvågning af medarbejderne. Overvågningen havde bl.a. til formål at afsløre eventuelle strafbare forhold begået af de ansatte. Der var nogen usikkerhed om de faktiske omstændigheder, herunder om – og i hvilket omfang – de ansatte var blevet informeret om overvågningen.

Sagen blev behandlet på et møde i Datarådet.

Datatilsynet lagde til grund, at der i det konkrete tilfælde var sket overvågning ved hjælp at et analogt kamera - det vil sige uden brug af digitalt udstyr – og i overensstemmelse med sin hidtidige praksis fandt Datatilsynet ikke, at analog tv-overvågning kan anses for omfattet af persondatalovens § 1, stk. 1.

Det var imidlertid Datatilsynets opfattelse, at den foretagne overvågning måtte anses for omfattet af § 1, stk. 2. Datatilsynet lagde herved vægt på, at der var tale om tv-overvågning over en periode, hvor der dagligt skete optagelse på et VHS-videobånd, som løbende blev overspillet, hvis der ikke var optaget noget af interesse.

Datatilsynet fandt således efter omstændighederne, at der var tale om en systematisk behandling i et omfang, der falder ind under definitionen i lovens § 1, stk. 2.

Det er en betingelse for anvendelsen af persondatalovens § 1, stk. 2, at der er tale om en behandling, som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden.

Det var Datatilsynets opfattelse, at behandlingen i denne sag også omfattede oplysninger af en karakter, der kan forlanges unddraget offentligheden. Tilsynet lagde herved vægt på, at overvågningen havde til formål at afsløre eventuelle strafbare forhold begået af de ansatte, og at hensynet til beskyttelse af den personlige integritet og privatlivet må tillægges betydning ved afgrænsningen af § 1, stk. 2.

Datatilsynet konstaterede, at da der i denne sag ikke var tale om elektronisk databehandling eller oplysninger indeholdt i et register, fandt reglerne om oplysningspligt i lovens §§ 28 og 29 ikke anvendelse, jf. § 1, stk. 2, sidste pkt.

Efter Datatilsynets opfattelse medfører princippet om god databehandlingsskik i persondatalovens § 5, stk. 1, imidlertid, at der i forbindelse med tv-overvågning i kontroløjemed som den absolutte hovedregel skal gives forudgående information til de ansatte.

Ved vurderingen af, om der kan ske fravigelse af denne hovedregel, må de hensyn, der kan begrunde fravigelse af oplysningspligt, jf. § 30, jf. §§ 28 og 29, inddrages. Det vil sige, at der skal være tale om afgørende hensyn til private eller offentlige interesser.

Datatilsynet fandt ikke, at der i denne sag forelå oplysninger om sådanne særlige omstændigheder, at der kunne ske fravigelse af kravet om forudgående information.

Det var derfor Datatilsynets opfattelse, at forretningen burde have informeret de ansatte forud for iværksættelsen af tv-overvågningen, og at sådan information skal indeholde nøjagtige og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen.

Medarbejderne burde efter Datatilsynets opfattelse have været informeret om bl.a. formålene med behandlingen og om, i hvilke tilfælde optagelserne ville blive gennemgået, samt om, at optagelserne ville kunne blive videregivet til politiet, og i hvilke tilfælde dette ville kunne ske.

Det var endvidere Datatilsynets opfattelse, at der burde være givet medarbejderne meddelelse om, hvor længe oplysningerne opbevares.

Datatilsynet fandt derimod ikke, at der kan stilles krav om præcis information om, hvornår der sker tv-overvågning, hvis dette kun finder sted i tilfælde af konkrete problemer.

Web-kameraer ved Vidåslusen

Udtalt, at web-kameraer, hvorfra der ønskes offentliggjort billeder på internettet, skal opsættes således, at der ikke kan ske transmission og offentliggørelse af billeder af genkendelige personer. Desuden udtalt, at zoom-funktionen på kameraerne skal sættes ud af kraft (Datatilsynets j.nr. 2003-322-0043)

Et amtscenter for undervisning rettede henvendelse til Datatilsynet i anledning af, at centeret ønskede at opstille to web-kameraer ved Vidåslusen.

Amtscentret havde med et projekt om opstilling af web-kameraer ved Vidåslusen vundet en konkurrence udskrevet af Undervisningsministeriet om, hvordan web-kameraer bedst kan bruges i undervisningen, og formålet med web-kameraprojektet var at give eleverne i Norden adgang til geografisk unikke steder. Det var meningen, at man skulle kunne studere vaden og stormflod og herunder bl.a. sammenligne vejrforholdene, f.eks. via vejrudsigter, med vandforholdene.

Der ville blive opstillet to web-kameraer ved Vidåslusen. Det ene ville pege direkte ud mod Vadehavet og vandhøjdemåleren, det andet ind i landet mod slusen og Vidåen. Fra de to kameraer ville der ske transmission til en hjemmeside, hvor det ville være muligt at se levende billeder fra kameraerne.

Der ville som udgangspunkt ikke blive foretaget optagelse, men det ville via den pågældende hjemmeside være muligt at tage stillbilleder med kameraerne, ligesom det ville være muligt at zoome. Denne kamerastyring var begrænset til 1 minut pr. bruger. Amtscentret havde anført, at disse muligheder for at zoome og optage stillbilleder var af afgørende betydning for et pædagogisk formål.

Amtscentret havde oplyst, at det som udgangspunkt ikke ville være muligt at genkende personer, som kunne ses på billederne fra kameraerne. For så vidt angik det ene kamera ville det dog være muligt at genkende personer, der gik helt op til slusemesterens hus og kiggede ind ad vinduet, hvor kameraet var opsat. Derudover ville det være muligt at genkende personer, der blev zoomet ind på.

Der ville ikke være krav om password for at komme ind på billederne på hjemmesiden. Alle ville således have adgang til billederne.

Der ville blive opstillet skilt med ordlyden "Videoovervågning".

Efter at sagen havde været behandlet i Datarådet udtalte Datatilsynet, at persondataloven ifølge lovens § 1, stk. 1, bl.a. gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling. Digital tv-overvågning vil således som udgangspunkt være omfattet af persondataloven.

For at den digitale behandling kan være omfattet af persondataloven, er det også en betingelse, at behandlingen omfatter "personoplysninger". Ifølge persondatalovens § 3, nr. 1, skal der ved "personoplysninger" forstås enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Omfattet af begrebet er herefter oplysninger, som f.eks. foreligger i form af billede.

Billeder er i Datatilsynets praksis i de tilfælde, hvor der ikke foreligger andre oplysninger end selve billedet til at identificere personen, i hvert fald blevet betragtet som personhenførbare og dermed omfattet af loven, hvis billedet bliver forevist til personer, der vil kunne genkende den fotograferede.

Offentliggørelse via internettet medfører, at de pågældende billeder vil blive tilgængelige for en så bred kreds, at det er sandsynligt, at nogen vil kunne genkende den fotograferede person. Der vil derfor som udgangspunkt være tale om elektronisk databehandling af personoplysninger omfattet af persondataloven.

Efter Datatilsynets opfattelse er de oplysninger, der bliver behandlet i forbindelse med overvågningen, almindelige ikke-følsomme oplysninger.

Ifølge § 6, stk. 1, nr. 1, må der ske behandling af almindelige ikke-følsomme oplysninger, hvis den registrerede har givet sit udtrykkelige samtykke hertil.

Datatilsynet anså det ikke for praktisk muligt at indhente udtrykkeligt samtykke efter § 6, stk. 1, nr. 1, jf. § 3, nr. 8, til den pågældende behandling.

Behandling må efter § 6, stk. 1, nr. 7, ske uden samtykke, 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.

For så vidt angik den behandling af personoplysninger, der vil kunne finde sted ved, at personer bliver filmet, og billederne transmitteret via internettet, når de går helt op til slusemesterens hus og kigger ind af vinduet til slusemesterens hus, var det Datatilsynets opfattelse, at denne ikke vil kunne finde sted i medfør af persondatalovens § 6, stk. 1, nr. 7.

For så vidt angik den behandling af personoplysninger, der vil kunne finde sted, hvis der bliver foretaget zoom, var det Datatilsynets opfattelse, at denne heller ikke vil kunne finde sted i medfør af interesseafvejningsreglen i § 6, stk. 1, nr. 7.

Datatilsynet lagde vægt på, at området omkring Vidåslusen er et offentligt tilgængeligt natur- og udflugtsområde af stor interesse for mange, hvor man som besøgende har en berettiget forventning om at kunne færdes, uden at billedoptagelser af én bliver transmitteret og offentliggjort "live" på internettet. Desuden forelå der efter tilsynets opfattelse ikke tilstrækkeligt tungtvejende grunde til, at de besøgende bør tåle den pågældende behandling af personoplysninger.

Hvis amtscentret ønskede at opsætte kameraer, burde de efter Datatilsynets opfattelse derfor placeres således, at der ikke kunne ske transmission og offentliggørelse på internettet af billeder af genkendelige personer.

Det var endvidere Datatilsynets opfattelse, at der ikke vil kunne ske behandling af personoplysninger via kameraernes zoom-funktion, medmindre der forelå samtykke fra de besøgende i området, jf. § 6, stk.1, nr. 1, jf. § 3, nr. 8.

Datatilsynet anså det imidlertid ikke for praktisk muligt at indhente udtrykkeligt samtykke fra hver enkelt besøgende og fandt derfor, at zoom-funktionen i givet fald burde sættes ud af kraft.

Datatilsynet gjorde opmærksom på, at hvis kameraerne havde andre styringsfunktioner ud over zoom-funktionen, må disse efter tilsynets opfattelse kun finde anvendelse i det omfang, der ikke vil blive behandlet personoplysnin-

ger. Kameraerne må således ikke kunne styres hen på personer, som kan genkendes på de transmitterede billeder.

Afslutningsvist henledte Datatilsynet opmærksomheden på lov om forbud mod tv-overvågning mv, hvoraf bl.a. følger, at offentlige myndigheder, der foretager tv-overvågning af steder eller lokaler, hvortil der er almindelig adgang, eller af arbejdspladser, ved skiltning eller på anden tydelig måde skal give oplysning herom.

Offentliggørelse af afgørelser i forbrugerklagesager

Udtalt, at offentliggørelse af afgørelser i forbrugerklagesager kræver anmeldelse som retsinformationssystem. Tillige udtalt, at en liste over erhvervsdrivende, der ikke efterkommer afgørelser i forbrugerklagesager, kan offentliggøres med henblik på forbrugerinformation (Datatilsynets j.nr. 2003-321-0269)

Forbrugerstyrelsen rettede henvendelse til Datatilsynet med anmodning om, at tilsynet foretog en vurdering af styrelsens påtænkte tiltag i forbindelse med ikrafttrædelsen af lov nr. 456 af 10. juni 2003 om forbrugerklager (herefter forbrugerklageloven). Forbrugerstyrelsen anmodede endvidere om en udtalelse i forbindelse med et udkast til bekendtgørelse om forbrugerklager (herefter bekendtgørelsen).

Ifølge lov om forbrugerklager § 15 kan økonomi- og erhvervsministeren fastsætte regler om offentliggørelse af information og statistik om forskellige forhold inden for forbrugerklageområdet, herunder om klage- og ankenævnenes afgørelser, og om at offentliggørelse kan ske elektronisk. Det fremgik ikke af lovens bemærkninger, om man med loven havde tilsigtet at fravige persondatalovens regler. Datatilsynet var ikke blevet hørt over lovforslaget.

Forbrugerstyrelsen oplyste, at styrelsen i medfør af § 15 ville offentliggøre Forbrugerklagenævnets og de godkendte private klage- og ankenævns afgørelser på internettet. Derudover ønskede Forbrugerstyrelsen at offentliggøre en liste over erhvervsdrivende, der ikke efterlever en afgørelse truffet af nævnene.

Folketingets partier havde i en aftale erklæret sig enige i den beskrevne offentliggørelse. Det var hensigten, at offentliggørelsen skulle ske på baggrund af fastlagte objektive kriterier, ligesom den erhvervsdrivende ville få mulighed for at anføre særlige standardiserede bemærkninger om årsagen til, at afgørelsen ikke blev efterlevet. Det var desuden hensigten, at gentagelsestilfælde skulle fremhæves. Sletning ville ske, når den erhvervsdrivende dokumenterede, at afgørelsen var efterlevet. Oplysninger om en sag måtte i øvrigt ikke fremgå af listen i mere end et år.

Sagen blev behandlet på et møde i Datarådet. Datatilsynets udtalelse gengives i al væsentligt nedenfor.

1. Ifølge Forbrugerstyrelsen skulle offentliggørelsen af afgørelser på internettet omfatte såvel Forbrugerklagenævnets som de private klage- og ankenævns afgørelser.

Forbrugerklagenævnet er en offentlig myndighed og dermed omfattet af bl.a. kapitel 12 i persondataloven, hvorimod de private klage- og ankenævn er private dataansvarlige og dermed omfattet af bl.a. kapitel 13 i persondataloven.

Ifølge persondatalovens § 45, stk. 1, nr. 2, skal der forinden iværksættelse af behandling, der foretages for en offentlig myndighed, og som udelukkende finder sted med henblik på at føre retsinformationssystemer, indhentes en udtalelse fra Datatilsynet.

For behandlinger, som foretages for en privat dataansvarlig, gælder, at Datatilsynets tilladelse skal indhentes inden iværksættelsen af en behandling, der udelukkende finder sted med henblik på at føre retsinformationssystemer, jf. persondatalovens § 50, stk. 1, nr. 5, jf. § 48.

Datatilsynet kan ifølge persondatalovens § 9, stk. 3, meddele nærmere vilkår for behandlinger, der alene sker med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for førelsen af systemerne. Dette gælder i forhold til såvel offentlige myndigheder som private dataansvarlige.

Datatilsynet forudsatte herefter, at dataansvaret for de omhandlede behandlinger snarest blev afklaret, og at de fornødne anmeldelser til Datatilsynet blev foretaget. Datatilsynet gjorde i den forbindelse opmærksom på, at tilsynet havde modtaget anmeldelser fra flere af de private klage- og ankenævn, og at disse sager var under behandling i tilsynet.

Datatilsynet oplyste i den forbindelse, at tilsynet som *udgangspunkt* ikke anser en oplysning om, at der er klaget over en erhvervsdrivende, eller om at en erhvervsdrivende ikke har efterkommet en afgørelse, for at være en fortrolig oplysning. Tilsynet fandt, at den dataansvarlige i hver enkelt sag må foretage en konkret vurdering af, hvorvidt det kan være tilfældet.

2. Offentliggørelsen af navnene på de erhvervsdrivende, der ikke efterkommer en afgørelse, ville som forudsat i forbrugerklagelovens forarbejder kunne ske i medfør bekendtgørelsens § 20. Derimod var der hverken i loven eller i bekendtgørelsen fastsat regler for, hvilken hjemmel modtagerne af oplysningerne har til at behandle oplysningerne.

Forbrugerstyrelsen havde over for Datatilsynet gjort gældende, at det af styrelsens hjemmeside ville fremgå, at oplysninger fra hjemmesiden ikke må bruges uden tilladelse. Styrelsen ville fremhæve dette forhold direkte i forbindelse med listens offentliggørelse.

I den forbindelse understregede Datatilsynet, at persondatalovens regler finder anvendelse på modtagerens behandling af oplysninger, hvorefter modtageren vil kunne behandle oplysningerne i det omfang, det er i overensstemmelse med lovens regler. Samtidig bemærkede Datatilsynet, at tilsynet ikke har ressourcer til at føre særskilt tilsyn med dette område.

Datatilsynet henledte herefter Forbrugerstyrelsens opmærksomhed på persondatalovens § 5, stk. 4, hvoraf følger, at behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges, jf. lovens § 37.

Datatilsynet forudsatte, at Forbrugerstyrelsen efterlever persondatalovens § 5, stk. 4, og § 37. Det vil efter tilsynets opfattelse bl.a. indebære, at styrelsen bør være behjælpelig, hvis der skulle opstå en situation, hvor en erhvervsdrivende er registreret med ukorrekte oplysninger i en søgemaskine eller lignende.

Datatilsynet vurderede i forbindelse med sagen, at der ikke ville være tale om aktiviteter som advarselsregistre omfattet af tilladelseskravet i persondatalovens § 50, stk. 1, nr. 2. Datatilsynet lagde herved vægt på, at formålet med offentliggørelsen af navnene på de erhvervsdrivende, der ikke har efterkommet en kendelse, ifølge forarbejderne var forbrugerinformation.

Ifølge persondatalovens § 57 skal der indhentes en udtalelse fra Datatilsynet ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger. Ifølge bemærkningerne til bestemmelsen forudsættes det endvidere, at der sker høring af Datatilsynet i forbindelse med udfærdigelse af lovforslag.

Datatilsynet fandt det beklageligt, at tilsynet ikke var blevet hørt over lovforslaget til forbrugerklageloven, og anmodede om fremover at blive hørt over lovforslag mv., der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger. Tilsynet udtalte, at høring så vidt muligt bør ske, inden forslagene fremsættes for Folketinget.

Københavns Energi

Udtalt, at Københavns Energis videregivelse af oplysninger til datterselskabet KE Marked A/S med henblik på markedsføring var omfattet af de særlige markedsføringsregler i persondatalovens § 6, stk. 2-3, jf. § 36 (Datatilsynets j.nr. 2002-313-0118)

Datatilsynet modtog en klage over, at Københavns Energi ønskede at videregive kundeoplysninger til datterselskabet KE Marked A/S uden forudgående samtykke fra selskabets kunder.

Det fremgik af sagen, at Københavns Energi efter en række organisatoriske ændringer er opbygget som en koncern med Københavns Energi Forsyningen (KE Forsyningen) som moderselskab. KE Forsyningen er en del af Københavns Kommune og fungerer som netvirksomhed. Koncernen har desuden en række 100 % kommunalt ejede datterselskaber, herunder KE Kunde A/S og KE Marked A/S. I praksis betyder dette, at det er netvirksomheden KE Forsyningen, som ejer datterselskaberne.

KE Marked A/S fungerer som databehandler for både KE Forsyningen og KE Kunde A/S. KE Marked A/S foretager desuden markedsføring af egne ydelser og services (salg af energi på kommercielle vilkår og tjenesteydelser i form af energibesparende tiltag).

I august 2000 udsendte KE Forsyningen et brev til sine kunder. Brevet indeholdt dels information om et nyt afregningssystem dels information om muligheden for at modtage markedsføringsmateriale fra datterselskabet KE Marked A/S samt om at modsætte sig sådanne markedsføringstiltag.

I informationsbrevet var der nederst på forsiden placeret en tekstboks, hvoraf fremgik "Læs venligst også vores meddelelse på bagsiden. Meddelelsen omhandler dine muligheder for at få nyttig information om nye produkter og muligheder fra KE marked A/S samt dine muligheder for at gøre indsigelse overfor tilsendelse af sådan information".

På informationsbrevets bagside var der en tekstboks, hvor det nye selskab KE Marked A/S og dets opgaver blev præsenteret. I tekstboksen blev samtidig beskrevet, at KE Marked A/S skulle bruge kundernes navn og adresse for at kunne tilbyde fordelagtige produkter og services, og at oplysningerne ville blive videregivet, medmindre kunden gjorde indsigelse inden for to uger. Det fremgår, at indsigelse kunne gøres skriftligt til en udtrykkeligt angivet adresse, ved personlig henvendelse eller ved et telefonopkald. Det fremgik endvidere af brevet, at de kunder, der tidligere havde oplyst til Københavns Energi eller Det Centrale Personregister, at de ikke ønskede at få markedsføringsmateriale, ikke behøvede at reagere på brevet, og at Københavns Energi respekterede indsigelserne.

Efter at sagen havde været behandlet på et møde i Datarådet, udtalte Datatilsynet, at det fremgår af persondatalovens § 6, stk. 2, at en virksomhed ikke må videregive oplysninger om forbrugere til andre virksomheder til brug ved markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, medmindre forbrugeren har givet sit udtrykkelige samtykke hertil.

Denne hovedregel om forbud mod videregivelse mv. af forbrugeroplysninger til brug for markedsføring modificeres imidlertid af reglen i § 6, stk. 3, hvorefter videregivelse og anvendelse kan ske uden samtykke, hvis der er tale om generelle kundeoplysninger, der danner grundlag for inddeling i kundekategorier, og hvis betingelserne i § 6, stk. 1, nr. 7, er opfyldt.

Det fremgår af forarbejderne til § 6, stk. 3, at den interesseafvejning, der skal foretages efter reglen i § 6, stk. 1, nr. 7, kun undtagelsesvis vil være til hinder for, at oplysningerne videregives. Dette kunne eksempelvis være, hvor kunden i det oprindelige kundeforhold, er blevet lovet, at der ikke vil ske en videregivelse af oplysninger til brug ved markedsføring.

I de tilfælde, hvor videregivelse eller anvendelse efter reglerne i lovens § 6, stk. 2-4, kan ske uden den registreredes (kundens) samtykke, skal virksomheden (den dataansvarlige) overholde de procedureregler, der er fastlagt i § 36.

I henhold til persondatalovens § 36 gælder følgende procedure:

For det første gælder det generelt, at virksomheden ikke må videregive oplysninger om en kunde (forbruger) til andre virksomheder med henblik på markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, hvis kunden har gjort indsigelse imod det, jf. § 36, stk. 1.

Der er tale om en ubetinget indsigelsesret, som kan gøres gældende direkte over for den dataansvarlige virksomhed på et hvilket som helst tidspunkt. Indsigelsen kan omfatte al videregivelse eller begrænses til videregivelse til bestemte virksomheder eller kategorier af virksomheder. Hvis intet andet angives i indsigelsen, må den almindeligvis forstås som en generel indsigelse mod al videregivelse og anvendelse på vegne af andre, der foretages med henblik på markedsføring.

Der er ingen formkrav til indsigelsen, og den kan derfor fremsættes såvel mundtligt som skriftligt eller via elektronisk post. Virksomheden bør notere og gemme modtagne indsigelser, ligesom den bør tjekke sine optegnelser, hver gang den ønsker at videregive kundeoplysninger til brug for markedsføring.

For det andet gælder det, at hvis kunden ikke har gjort indsigelse direkte over for virksomheden, skal virksomheden - hver gang den ønsker at videregive kundeoplysninger til andre virksomheder med henblik på markedsføring eller anvende oplysninger på vegne af en anden virksomhed i dette øjemed - tjekke i CPR, om kunden efter § 29, stk. 3, i lov om Det Centrale Personregister (CPR) over for bopælskommunen har frabedt sig henvendelser i markedsføringsøjemed, jf. § 36, stk. 2, 1. pkt. I bekræftende fald må oplysningerne ikke videregives til dette formål.

For det tredje gælder det, at den dataansvarlige virksomhed i de tilfælde, hvor kunden hverken direkte over for virksomheden eller gennem en registrering i CPR har gjort indsigelse mod videregivelse og anvendelse i markedsføringsøjemed eller frabedt sig sådanne henvendelser, skal oplyse kunden om retten til at gøre indsigelse, jf. § 36, stk. 2, 2. pkt. Dette skal ske hver gang virksomheden ønsker at videregive eller på andres vegne anvende oplysninger i markedsføringsøjemed, og det skal ske, inden videregivelsen eller anvendelsen finder sted. Forbrugeren har herefter mulighed for inden for en frist på to uger at gøre indsigelse.

Det kræves, at virksomheden, inden oplysningerne videregives eller anvendes til markedsføring, tydeligt og på en forståelig måde oplyser om indsigelsesretten. Det vil i den forbindelse ikke være tilstrækkeligt at beskrive retten til at gøre indsigelse i de almindelige forretningsbetingelser, som måtte blive udleveret til den pågældende forbruger. Oplysning om indsigelsesretten skal i stedet gives som en individuel meddelelse til kunden, uden at dette dog udelukker, at meddelelsen tillige indeholder andre oplysninger.

Virksomheden skal give forbrugeren adgang til på en nem måde og med en frist på to uger at gøre indsigelse. Det kan f.eks. ske ved, at virksomheden medsender en kupon til forbrugeren, hvor der kan krydses "nej" til videregivelsen/anvendelsen. Virksomheden må naturligvis ikke videregive eller anvende oplysningerne til markedsføring, før det ved udløbet af fristen på to uger er konstateret, at forbrugeren ikke har gjort indsigelse.

Ved vurderingen af, om den skete videregivelse af oplysninger til KE Marked A/S var i overensstemmelse med persondataloven, måtte det indledningsvis afklares, om Københavns Energis videregivelse af oplysninger til datterselskabet KE Marked A/S med henblik på markedsføring var omfattet af de særlige regler i persondatalovens § 6, stk. 2-4, og § 36.

Disse bestemmelser finder efter deres ordlyd alene anvendelse, hvis en virksomhed videregiver oplysninger om forbrugere til en anden virksomhed i markedsføringsøjemed eller anvender oplysningerne på vegne af en anden virksomhed i dette øjemed.

Datatilsynet konstaterede, at forarbejderne til persondatalovens § 6, stk. 2-4, og § 36 ikke indeholder bemærkninger, der medfører, at bestemmelserne finder anvendelse på *offentlige* virksomheders videregivelser.

I de almindelige bemærkninger til lovforslag L 147 er anført, at Justitsministeriet finder, at der bør fastsættes særlige regler om videregivelse af oplysninger i markedsføringsøjemed, som på én gang i videst muligt omfang viderefører den gældende retstilstand og er i overensstemmelse med direktivet.

Med udgangspunkt i bestemmelsens formulering og i betragtning af, at det nu er én samlet lov, der gælder i både den private og den offentlige sektor, fandt Datatilsynet, at de særlige markedsføringsregler i persondatalovens § 6, stk. 2-3, jf. § 36, må antages at omfatte behandling, der foretages af eller for en offentlig erhvervsdrivende virksomhed.

Tilsynet lagde navnlig vægt på, at dette resultat stemmer bedst overens med, at der er tale om et liberaliseret marked, hvor Københavns Energi agerer i konkurrence med private virksomheder. Tilsynet lagde også vægt på, at denne fortolkning harmonerer med markedsføringslovens bestemmelser om, at offentlige myndigheder er omfattet af markedsføringslovens regler, hvis de henvender sig i markedet med ydelser til befolkningen i konkurrence med det private erhvervsliv, hvorved det organisatoriske træder i baggrunden i forhold til funktionelle - nemlig om der er tale om erhvervsvirksomhed i bred forstand. Disse regler blev gennemført samtidig med reglerne i persondatalovens § 6, stk. 2-4, og § 36.

Det var herefter Datatilsynets opfattelse, at Københavns Energi havde fulgt proceduren i persondatalovens § 36, jf. § 6, stk. 3, og at selskabet således havde handlet i overensstemmelse med lovens krav.

Datatilsynet lagde herved vægt på, at KE Forsyningen før videregivelsen havde sikret sig, at kunderne ikke havde frabedt sig markedsføringsmateriale over for Københavns Energi eller ved en markering i CPR.

Datatilsynet lagde også vægt på, at Københavns Energi havde givet en tydelig og let forståelig information om kundernes ret til at gøre indsigelse mod videregivelse af oplysninger til KE Marked A/S, idet selskabet havde fremhævet budskabet ved at indsætte det i to tekstbokse – hvoraf den væsentlige meddelelse var placeret alene i en tekstboks på informationsbrevets bagside.

Datatilsynet fandt desuden, at Københavns Energi ved at anvise en adresse samt give mulighed for, at indsigelser kunne meddeles telefonisk eller ved personlig henvendelse, havde givet sine kunder adgang til at gøre indsigelse på en nem måde.

I forhold til klageren noterede Datatilsynet sig, at Københavns Energi på grund af klagen havde undladt at videregive oplysninger om den pågældende til KE Marked A/S i markedsføringsøjemed.

Videregivelse af telefonbogsoplysninger og salg af forbrugerprofiler

Udtalt, at videregivelse af § 34-data ved opdatering af kundedatabaser, f.eks. ved tilførsel af telefonnumre til en navnedatabase, kan ske i medfør af interesseafvejningsbestemmelsen i persondatalovens § 6, stk. 1, nr. 7, og uden iagttagelse af markedsføringsreglerne i § 6, stk. 2-4, og § 36. Endvidere udtalt, at produkter baseret på rent statistiske oplysninger falder uden for persondatalovens anvendelsesområde (Datatilsynets j.nr. 2002-212-0101)

Datatilsynet traf i 2002 afgørelse i en sag vedrørende TDC Forlags videregivelse af telefonbogsoplysninger. Afgørelsen er gengivet i Datatilsynets årsberetning 2002, s. 52.

TDC Forlag anmodede i forlængelse heraf om Datatilsynets stillingtagen til yderligere to spørgsmål med henblik på at sikre, at forlagets øvrige forretningsområder var i overensstemmelse med kravene i persondataloven:

1. Kan forlaget i forbindelse med opdatering af virksomheders kundedatabaser tilføre kundedatabasen yderligere § 34-data[15] eksempelvis ved tilførsel af telefonnumre til en navnedatabase?

2. Indebærer berigelse af kundedatabaser og Database Danmark med ikke-personhenførbare statistiske oplysninger problemer i forhold til persondataloven?

Ifølge TDC Forlag blev de statistiske oplysninger erhvervet som færdige produkter, der herefter anvendtes af forlaget til analyse og berigelse af virksomheders kundedatabaser, herunder salg af forbrugsprofiler. Ved modtagelse af en kundedatabase fra en virksomhed kunne forlaget ved brug af de statistiske oplysninger fordele kunderne på forbrugertyper inkl. demografiske variabler som f.eks. familiestruktur, antal biler og indtægt.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at tilførsel af yderligere § 34-data i forbindelse med opdatering af kundedatabaser efter Datatilsynets opfattelse må betragtes som en videregivelse i persondatalovens forstand.

I Datatilsynets tidligere afgørelse tilkendegav tilsynet, at videregivelse af rene nummeroplysningsdata omfattet af § 34 i lov om konkurrence- og forbrugerforhold på telemarkedet ikke var omfattet af de særlige markedsføringsregler i persondatalovens § 6, stk. 2-4, og § 36.

[15] jf. § 34 i lov om konkurrence- og forbrugerforhold på telemarkedet

I overensstemmelse hermed fandt Datatilsynet, at TDC Forlags videregivelse af § 34-data ved opdatering af kundedatabaser, f.eks. ved tilførsel af telefonnumre til en navnedatabase, kunne ske i medfør af interesseafvejningsbestemmelsen i persondatalovens § 6, stk. 1, nr. 7. Datatilsynet lagde herved vægt på, at der alene var tale om videregivelse af nummeroplysninger omfattet af § 34 i lov om konkurrence- og forbrugerforhold på telemarkedet[16].

Om TDC Forlags brug af statistiske oplysninger var omfattet af persondatalovens anvendelsesområde afhang i første omfang af, om de benyttede forbrugerprofiler udgjorde personoplysninger i lovens forstand.

Persondatalovens § 3, nr. 1, definerer personoplysninger som enhver form for information om en identificeret eller identificerbar fysisk person. Det følger af bemærkningerne, at der ved en *identificerbar person* skal forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Det følger endvidere af bemærkningerne, at det er uden betydning, om identifikationsoplysningen er alment kendt eller umiddelbart tilgængelig. Også de tilfælde, hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører, vil være omfattet af definitionen.

Oplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke længere kan identificeres, er derimod ikke omfattet af begrebet *personoplysninger*. Ved afgørelsen af, om en person er identificerbar, skal alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den dataansvarlige eller af enhver anden person, tages i betragtning.

På grundlag af de oplysninger, som TDC havde givet Datatilsynet om de statistiske oplysninger var det tilsynets opfattelse, at de forbrugerprofiler, som anvendtes, måtte betragtes som statistiske oplysninger, der ikke kunne henføres til bestemte personer.

TDC Forlags brug af statistiske oplysninger faldt på denne baggrund uden for persondatalovens anvendelsesområde, idet forlaget ikke behandlede personoplysninger omfattet af definitionen i lovens § 3, nr. 1. Indsigelsesproceduren i lovens § 36 skulle således ikke iagttages ved tilførsel af de statistiske oplysninger til Database Danmark.

Datatilsynet præciserede for god ordens skyld, at TDC Forlags brug heraf alene faldt uden for persondatalovens anvendelsesområde i det omfang, der var tale om rent statistiske oplysninger, som på ingen måde vedrørte identificerede eller identificerbare fysiske enkeltpersoner.

16 Datatilsynet har i en afgørelse i juni 2004 præciseret denne udtalelse, således at tilførsel af oplysninger til en kundedatabase uden iagttagelse af markedsføringsreglerne i persondataloven må forudsætte, at der er tale om en virksomheds database over eksisterende *kunder, dvs. at der forudgående er etableret en kontakt mellem kunden og virksomheden. Datatilsynet fandt yderligere anledning til på ny at overveje, hvilke oplysninger der kan tilføres kundedatabaser uden iagttagelse af proceduren i § 36, stk. 2, og fandt, at der alene kan tilføres oplysninger om navn, adresse og telefonnummer (Datatilsynets j.nr. 2004-215-0160).*

Opbevaring af e-post

Udtalt, at en e-postserviceudbyders opbevaring af sikkerhedskopier af e-post i et år ligger langt ud over, hvad en almindelig bruger må formodes at forvente, hvorfor sådan opbevaring forudsætter en udtrykkelig og klar aftale mellem udbyderen og kunden (Datatilsynets j.nr. 2002-215-0094)

Datatilsynet modtog en klage over, at en e-postserviceudbyder, havde opbevaret en kundes e-postkommunikation i lang tid efter, at korrespondancen var blevet slettet af kunden. Det pågældende materiale var efter retskendelse blevet udleveret til politiet.

Det fremgik af sagen, at der var tale om opbevaring af sikkerhedskopier af e-postkommunikation foretaget af et teknisk system til sikring mod datatab i tilfælde af nedbrud. Systemet sørgede således for passende arkivering og sikkerhedskopiering af programmer og data fra driftssystemerne, herunder den e-post, der lå på e-postserverne på det tidspunkt, hvor der blev taget sikkerhedskopi.

På tidspunktet for klagen tilstræbte e-postserviceudbyderen generelt, at arkiverede data kunne genskabes inden for et år. Dette blev efterfølgende revideret således, at sikkerhedskopier opbevares i op til 3 måneder tillagt 14 dage.

Formålet med at opbevare sikkerhedskopierne var at give kunden sikkerhed mod at miste vitale data og information, og denne målsætning fremgik af de dokumenter, der sædvanligvis blev fremsendt til kunden ved etableringen af kundeforholdet. Materialet indeholdt dog ikke nogen nærmere beskrivelse af sikkerhedskopieringsproceduren eller oplysninger om, hvor længe data ville blive gemt, ligesom abonnementsbetingelserne ikke indeholdt oplysninger om opbevaring af sikkerhedskopier.

Datatilsynet lagde ved sagens behandling til grund, at den omhandlede e-postkommunikation var blevet opbevaret i mindst et år i forbindelse med sikkerhedskopieringen.

Efter behandling af sagen i Datarådet udtalte Datatilsynet bl.a., at det følger af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Det var Datatilsynet opfattelse, at opbevaring af sikkerhedskopier af e-post, som af brugeren er slettet fra den e-postboks, der er til rådighed på e-postserviceudbyderens server, i en periode på et år eller mere, ligger langt

ud over, hvad en almindelig bruger må formodes at forvente. Datatilsynet fandt således, at opbevaring hos udbyderen af sikkerhedskopier af slettet e-post i en så lang periode ikke kunne antages at følge af udbyderens forpligtelser efter persondatalovens § 41, stk. 3, og derfor måtte forudsætte en udtrykkelig og klar aftale mellem udbyderen og kunden.

Datatilsynet fandt ikke, at opbevaringen i den konkrete sag kunne anses for sket på kundens vegne. Tilsynet lagde i den forbindelse lagt vægt på, at udbyderen ikke havde godtgjort, at der havde foreligget en udtrykkelig og klar aftale om at opbevare oplysninger som sket, ligesom det heller ikke fandtes godtgjort, at kunden i øvrigt var blevet orienteret om denne service og dermed havde haft mulighed for at fravælge den.

Da e-postserviceudbyderen efter Datatilsynets opfattelse ikke selvstændigt opfyldte persondatalovens betingelser for at opbevare de omhandlede oplysninger, jf. persondatalovens §§ 6-8, og da tilsynet ikke vurderede, at udbyderen havde haft anden hjemmel til opbevaring af oplysningerne, fandt Datatilsynet, at udbyderen havde handlet i strid med persondataloven ved at opbevare den pågældende e-postkommunikation i så lang en periode som sket. Datatilsynet fandt dette meget beklageligt. Datatilsynet havde i øvrigt noteret sig, at oplysningerne nu var slettet.

På baggrund af sagen har Datatilsynet i samarbejde med IT-Brancheforeningen iværksat en undersøgelse af e-postserviceudbydernes praksis for opbevaring af indholdet af e-postkommunikation. Formålet med undersøgelsen er at belyse problemstillingen om opbevaringen af sådanne data og at afdække de hensyn, som bør indgå i Datatilsynets videre overvejelser om eventuelle retningslinier for, hvor længe oplysningerne kan opbevares inden for persondatalovens rammer.

Udvidet anvendelse af Landspatientregisteret/eLPR

Udtalt, at Sundhedsstyrelsens videregivelse af oplysninger fra Landspatientregisteret til sundhedspersoner i behandlingsøjemed kan ske inden for rammerne af persondataloven, men at denne udvidede anvendelse af Landspatientregisteret bør overvejes lovreguleret. Oplysningspligt. Slettefrist. Sikkerhed (Datatilsynets j.nr. 2003-082-0112)

Datatilsynet modtog en anmeldelse af en ændring til Sundhedsstyrelsens anmeldelse af "Behandling af oplysninger om sygehuspatienter". Ændringen bestod i at give sundhedspersoner adgang til Landspatientregisterets/eLPR medicinske og administrative data til behandlings- og plejeformål.

I Landspatientregisteret registreres på baggrund af indberetninger fra sygehusene mv. oplysninger om personer, der har været i stationær, ambulant eller skadestuebehandling på et offentligt eller privat sygehus/klinik. Landspatientregisteret er et administrativt register, som Sundhedsstyrelsen er dataansvarlig for.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at videregivelsen fra Landspatientregisteret skal ske i overensstemmelse med persondataloven og ikke lov om patienters retsstilling, idet der er tale om et administrativt register, som Sundhedsstyrelsen er dataansvarlig for.

Efter persondatalovens § 7, stk. 5, må oplysninger om helbredsmæssige forhold videregives, hvis videregivelsen 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 underlagt tavshedspligt.

Datatilsynet noterede sig, at der var foretaget en lægefaglig vurdering af, hvilke oplysninger fra Landspatientregisteret der er behov for at videregive til brug for patientbehandling mv., og at konklusionen var, at der er behov for oplysninger om alle de kontakter, som en patient tidligere har haft til sygehusene mv.

Datatilsynet havde ikke grundlag for at anlægge en anden vurdering af dette spørgsmål. Det var derfor Datatilsynets opfattelse, at de oplysninger om en persons tidligere kontakter med sygehuse mv., som findes i Landspatientregisteret, kan videregives i medfør af persondatalovens § 7, stk. 5. Videregivelsen kan efter denne regel ske uden samtykke fra patienten, idet oplysningerne er nødvendige med henblik på patientbehandlingen mv. som beskrevet i bestemmelsen. Datatilsynet lagde i den forbindelse til grund, at der alene sker videregivelse til behandlende læge på den behandlende afdeling på det behandlende offentlige sygehus. Datatilsynet noterede sig desuden, at videregivelsen vil ske således, at lægen skal angive, om der er behov for at se somatiske, psykiatriske eller begge typer af kontakter.

I tilfælde hvor patienten er bevidstløs, vil videregivelsen tillige kunne ske i medfør af lovens § 7, stk. 2, nr. 2, om videregivelse, der er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke.

Datatilsynet noterede sig, at det var Indenrigs- og Sundhedsministeriets og Sundhedsstyrelsens hensigt at basere videregivelsen af oplysninger om personer, der ikke er bevidstløse, på persondatalovens § 7, stk. 2, nr. 1, hvoref-

ter der kan ske videregivelse, hvis den registrerede har givet sit udtrykkelige samtykke til videregivelsen.

Samtykke er ifølge persondataloven § 3, nr. 8, defineret som: "Enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling."

Efter Datatilsynets opfattelse kunne der stilles spørgsmål ved, om et samtykke i en behandlingssituation som den beskrevne vil kunne leve fuldt ud op til kravene i persondataloven § 3, nr. 8.

Efter Datatilsyntes opfattelse må spørgsmålet om, hvorvidt videregivelsen fra Landspatientregisteret skal baseres på et samtykke fra den registrerede, desuden give anledning til overordnede principielle overvejelser. I den forbindelse må ønsket om at give patienterne selvbestemmelse afvejes med de mulige konsekvenser af, at oplysninger, der er nødvendige for patientbehandlingen, ikke bliver tilgængelige, hvis patienten ikke ønsker at give samtykke til videregivelsen.

Datatilsynet henledte herefter opmærksomheden på persondatalovens regler om oplysningspligt ved registrering i Landspatientregisteret.

Hvor oplysninger ikke er indsamlet hos den registrerede, påhviler det den dataansvarlige eller dennes repræsentant ved registreringen, eller hvor de indsamlede oplysninger er bestemt til videregivelse til tredjemand, senest når videregivelsen af oplysningerne finder sted, at give den registrerede meddelelse om den dataansvarliges eller dennes repræsentants identitet samt formålet med behandlingen. Den dataansvarlige skal endvidere give meddelelse om alle yderligere oplysninger, der efter forholdets særlige omstændigheder er nødvendige for, at den registrerede kan varetage sine interesser, herunder f.eks. indsamlede oplysningstyper og kategorier af modtagere, jf. persondatalovens § 29, stk. 1.

Bestemmelsen i § 29, stk. 1, gælder bl.a. ikke, hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssig vanskelig, jf. § 29, stk. 3.

Datatilsynet noterede sig, at Indenrigs- og Sundhedsministeriet fandt, at det vil være uforholdsmæssigt vanskeligt at underrette om registrering i Landspatientregisteret. Tilsynet gjorde i den forbindelse opmærksom på muligheden for at træffe kompensatoriske foranstaltninger, f.eks. ved orientering i en pjece, der udleveres ved indlæggelse eller behandling på et sygehus. Datatilsynet forbeholdt i øvrigt sin stillingtagen i forbindelse med en konkret klage.

I relation til oplysningspligt for den modtagende myndighed (sygehuset), fandt Datatilsynet, at det umiddelbart må lægges til grund, at en patient, der har afgivet samtykke, som lever op til persondatalovens krav om bl.a. information, derved tillige er gjort bekendt med de oplysninger, der er relevante at give efter persondatalovens § 29.

For så vidt angår patienter, der på grund af bevidstløshed eller lignende ikke kan give samtykke, forudsatte Datatilsynet, at oplysningspligten efterfølgende opfyldes.

I relation til datasikkerhed henviste Datatilsynet til sikkerhedsbekendtgørelsens § 19, stk. 1, hvoraf følger, at der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Efter Datatilsynets opfattelse burde det overvejes, om Sundhedsstyrelsen i forbindelse med videregivelse fra Landspatientregisteret har et særligt behov for at opbevare loggen for at kunne forebygge og opklare misbrug. Under hensyntagen til oplysningernes karakter var det tilsynets umiddelbare vurdering, at loggen bør opbevares i 5 år.

Slettefristen for oplysninger, der behandles i Landspatientregisteret, er ifølge anmeldelsen 35 år efter optagelsen i registeret. I relation til videregivelsen i eLPR havde Indenrigs- og Sundhedsministeriet oplyst, at der om nødvendigt kan indføres en tidsmæssig afgrænsning, f.eks. på 10 år tilbage i tiden, dog altid 1 år tilbage fra sidste sygehuskontakt.

Under hensyntagen til, at oplysningerne er nødvendige for patientbehandlingen fandt Datatilsynet ikke grundlag for at stille krav om en kortere slettefrist end for de øvrige behandlinger i Landspatientregisteret.

Afslutningsvis bemærkede Datatilsynet, at den ønskede registrering og videregivelse fra Landspatientregisteret vil omfatte oplysninger om en stor del af den danske befolkning, og at der er tale om videregivelse af meget følsomme oplysninger.

Det var Datatilsynets opfattelse, at den nærmere tilrettelæggelse af registreringen og videregivelsen fra Landspatientregisteret giver anledning til afvejning af væsentlige og til en vis grad indbyrdes modstridende samfundshensyn. På den ene side hensynet til en korrekt og effektiv patientbehandling og på den anden side hensynet til at give de personer, der har behov for behandling, selvbestemmelse i relation til behandling af oplysnin-

ger. Datatilsynet foreslog derfor, at Indenrigs- og Sundhedsministeriet og Sundhedsstyrelsen overvejer, om en udvidet anvendelse af Landspatientregisteret bør lovreguleres, således at de principielle spørgsmål knyttet til en udvidet anvendelse af registeret underkastes en overordnet politisk beslutningsproces.

Offentliggørelse af oplysninger om mulig jordforurening

Udtalt, at oplysninger om en ejendoms mulige jordforurening som udgangspunkt kan offentliggøres på et amts hjemmeside efter persondatalovens § 6, stk. 1, nr. 7. I det konkrete tilfælde imidlertid fundet, at offentliggørelsen ikke var i overensstemmelse med persondatalovens regler, fordi offentliggørelsen skete i meget summarisk form og på et meget spinkelt grundlag (Datatilsynets j.nr. 2003-322-0044)

Sagen blev behandlet på baggrund af en klage til Datatilsynet over Vestsjællands Amts offentliggørelse på internettet af en mulig forurening på klagerens sommerhusgrund.

Amtet havde ved søgning i kommunens byggesagsarkiver, tankarkiver og gamle telefonbøger fundet en oplysning om, at der på klagerens ejendom havde været metalstøberi, som kunne have medført en forurening af grunden. Selv om grunden ikke var formelt kortlagt som forurenet, havde amtet lagt oplysningen ud på amtets hjemmeside og udleverede oplysningerne ved henvendelse fra advokater og ejendomsmæglere.

Amtet henviste til, at amtet ifølge lov om forurenet jord skal kortlægge (registrere) forurenede og muligt forurenede arealer. Der kortlægges på to vidensniveauer – vidensniveau 1 (begrundet mistanke om forurening) og vidensniveau 2 (dokumenteret forurening). Den pågældende grund var omfattet af en indledende kortlægning, der lå forud for en afgørelse om kortlægning på vidensniveau 1. Den indledende kortlægning omfatter indsamling af oplysninger om muligt forurenende aktiviteter, og hvor disse aktiviteter har været. Oplysningerne indhentes fra forskellige kilder, og hvis der i en kilde er en oplysning om en aktivitet, som kunne have medført en forurening, og aktiviteten på en eller anden måde kan henføres til en bestemt ejendom, så skal amtet oprette en sag med henblik på at træffe afgørelse om, hvorvidt der er grundlag for en kortlægning i henhold til lov om forurenet jord.

Oplysningerne om indledende kortlægninger er omfattet af retten til aktindsigt, og amtet havde oplevet et stigende antal aktindsigtsanmodninger vedrørende enkeltejendomme. Amtet havde derfor set en mulighed for at begrænse ressourceanvendelsen ved at lægge oplysningerne om også den indledende kortlægning ud på internettet.

Amtet henviste endvidere til, at det af Århus Konventionen bl.a. fremgår, at der skal være offentlighed i miljøoplysninger, og at borgerne af hensyn til økonomiske og sundhedsmæssige interesser skal have mulighed for at gøre sig bekendt med miljøoplysningerne, herunder oplysninger om muligt eksisterende forureninger.

Formålet med offentliggørelsen var at beskytte mulige købere, skabe åbenhed omkring forureningsoplysninger og at informere grundejerne, så disse kan tage deres forholdsregler.

De konkrete oplysninger om den i sagen omhandlede ejendom stammede fra Kongeriget Danmarks Handelskalender fra 1970. Kalenderen indeholdt oplysning om en navngiven person, som var anført sammen med adressen på ejendommen og oplysningen om et metalstøberi. Amtet havde ikke kunnet få bekræftet oplysningen andre steder, og amtet oplyste, at der kunne være tale om, at den pågældende havde været ejer af ejendommen, mens selve virksomheden havde ligget et andet sted.

Efterfølgende havde amtet sammenholdt oplysningen med andre oplysninger, herunder at ejendommen var en sommerhusgrund, og herefter ikke fundet det sandsynligt, at der rent faktisk skulle have ligget et metalstøberi på ejendommen. Der havde derfor ikke været grundlag for at kortlægge ejendommen som muligt forurenet jord i henhold til lov om forurenet jord, og ejendommen blev udtaget af amtets kortlægning.

Amtet opretholdt dog en registrering af ejendommen på hjemmesiden under overskriften "forurenet jord" med teksten: "Amtet har ingen oplysninger om kortlægning på vidensniveau 1 eller 2 i henhold til lov om forurenet jord på den pågældende matrikel". Denne tekst anvendes på alle øvrige ejendomme, der ikke er kortlagt på vidensniveau 1 eller 2.

Amtet var ophørt med at offentliggøre forureningsoplysninger om ejendomme, der alene er omfattet af den indledende kortlægning, på hjemmesiden.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at tilsynet fandt, at amtet i forbindelse med den skete offentliggørelse havde behandlet personoplysninger omfattet af persondatalovens § 1, stk. 1. Datatilsynet lagde i den forbindelse vægt på, at selv om ejerens navn ikke blev registreret, ville dette kunne findes på anden vis, f.eks. via tinglysning eller andre offentlige registre. Datatilsynet tillagde det yderligere vægt, at offentliggørelsen kunne få betydning for grundejernes anvendelse af ejendommen, herunder – som også oplyst af amtet til grundejerne i forbindelse med offentliggørelsen – en betydning for værdiansættelsen af ejendommen.

Datatilsynet udtalte herefter, at spørgsmålet om, i hvilket omfang amtet kan offentliggøre almindelige ikke-følsomme oplysninger, herunder f.eks. oplysninger om navn, adresse, telefonnummer og oplysninger om ejendomsforhold, der ikke afslører oplysninger om følsomme forhold efter persondatalovens § 7 og § 8, skal afgøres efter persondatalovens § 6, stk. 1, nr. 1-7.

Det var Datatilsynets vurdering, at Vestsjællands Amt efter § 6, stk. 1, nr. 7, og under iagttagelse af de almindelige principper i persondatalovens § 5, kan offentliggøre oplysninger om en jordforureningskortlægning på amtets hjemmeside. Datatilsynet lagde i den forbindelse vægt på, at Vestsjællands Amts interesse i at offentliggøre de pågældende oplysninger og offentlighedens interesse i at få kendskab til muligt forurenede grunde fandtes at veje tungere end hensynet til den pågældende ejers interesse i ikke at få offentliggjort oplysninger om sin ejendom på internettet.

Datatilsynet bemærkede i den forbindelse også, at det følger af Århus Konventionens principper, at der skal være offentlighed i miljøoplysninger, og at borgerne skal have mulighed for at gøre sig bekendt med miljøoplysninger, herunder oplysninger om muligt eksisterende forureninger, ikke blot af hensyn til økonomiske interesser, men også til sundhedsmæssige interesser. Endelig tillagde Datatilsynet det vægt, at oplysningerne i forvejen er tilgængelige via aktindsigtsreglerne og derfor ikke kan anses som fortrolige.

Datatilsynet fandt imidlertid, at amtets *konkrete* offentliggørelse på internettet af klagerens grund som muligt forurenet ikke var i overensstemmelse med persondatalovens § 6, stk. 1, nr. 7, og principperne i persondatalovens § 5.

Datatilsynet lagde i den forbindelse vægt på, at amtets offentliggørelse af oplysningen om, at klagerens sommerhusgrund muligvis var forurenet skete i en meget summarisk form, således at besøgende på hjemmesiden ikke havde mulighed for at se det konkrete grundlag for amtets registrering af ejendommen, herunder at registreringen af klagerens sommerhusgrund alene var baseret på en oplysning fra en handelskalender fra 1970.

Det indgik endvidere i tilsynets vurdering, at amtet meget kort tid efter den skete offentliggørelse vurderede, at der ikke var grundlag for at kortlægge klagerens ejendom som muligt forurenet i henhold til lov om forurenet jord, og amtet havde derfor udtaget den af amtets jordforureningskortlægning.

Vedrørende de fortsatte registreringer af ejendommen lagde Datatilsynet til grund, at amtet offentliggjorde oplysninger om alle ejendomme i amtet på hjemmesiden under samme overskrift – "Forurenede grunde".

Datatilsynet fandt ikke, at offentliggørelsen af oplysninger om alle amtets ejendomme på hjemmesiden kan antages at være i strid med persondatalo-

vens § 6, stk. 1. Datatilsynet lagde i den forbindelse vægt på, at der ikke er tale om fortrolige oplysninger, men alene en tilkendegivelse om, at den pågældende ejendom ikke er kortlagt i henhold til jordforureningsloven, ligesom tilsynet fandt, at offentlighedens interesse i at få kendskab til, at en ejendom ikke er omfattet af en kortlægning, vejer tungere end grundejernes interesse i ikke at få offentliggjort oplysninger om deres ejendomme. Datatilsynet lagde yderligere vægt på, at alle ejendomme i amtet behandles på lige fod, således at man ikke nødvendigvis kan have en formodning for, at en ejendom har været under mistanke for at være forurenet. Endelig tillagde Datatilsynet det betydning, at ejendomsoplysninger generelt er omfattet af retten til aktindsigt.

Med hensyn til den valgte overskrift – "Forurenede grunde" – fandt Datatilsynet ikke helt at kunne udelukke, at overskriften ved umiddelbar læsning kunne give de besøgende anledning til at tro, at alle de nævnte grunde er forurenede. Datatilsynet tilkendegav derfor over for amtet, at det efter tilsynets opfattelse ville være ønskeligt at ændre overskriften.

Internationalt arbejde

Internationalt arbejde

Indledning

Som beskrevet i tidligere årsberetninger, senest i Datatilsynets Årsberetning for 2002, 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 FN's 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 2003. Desuden omtales også det mere uformelle, internationale samarbejde, som har udviklet sig gennem årene.

Europarådet

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 2003 bl.a. beskæftiget sig med spørgsmålet om overførsel af oplysninger til tredjelande og med strukturen af arbejdet i Europarådet, herunder om sammenlægning af T-PD og Databeskyttelseseksperтgruppen (CJ-PD). 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, og i konsekvens heraf blev det i 2003 besluttet at nedlægge CJ-PD, hvis arbejde vil blive fortsat i T-PD.

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 Ministerkomitéen og efterfølgende fremlagt til underskrivelse. I slutningen af 2003 har 23 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, når alle parter til Den europæiske konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger har accepteret ændringen. Alle medlemslandene har endnu ikke accepteret, og De Europæiske Fællesskaber har derfor endnu ikke tiltrådt konventionen.

Inden sammenlægningen med T-PD færdigbehandlede CJ-PD retningslinier for anvendelsen af smart cards. CJ-PD har i 2003 bl.a. også arbejdet med behandling af personoplysninger ved brug af biometriske data. Dette arbejde vil fortsætte i T-PD.

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 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 2003 afholdt 5 møder, hvor man bl.a. har behandlet spørgsmål, som vedrører oprettelse af analysedatabaser, se konventionens artikel 10 og artikel 12, og relationerne til Europol.

Kontrolinstansen har i 2003 afgivet sin første aktivitetsrapport for perioden fra oktober 1998 til oktober 2002. Rapporten er tilgængelig på Datatilsynets hjemmeside. Det er hensigten, at kontrolinstansen fremover skal udgive en aktivitetsrapport hvert andet år.

I 2003 gennemførte et inspektionshold fra kontrolinstansen en inspektion af Europol i Haag. Inspektionen gav anledning til visse anbefalinger - særligt i forbindelse med Europols arbejde med at etablere informationssystemet som beskrevet i konventionens artikler 7-9.

Det Fælles Klageudvalg har i 2003 afholdt 6 møder. Klageudvalget afgjorde bl.a. sin 2. klagesag i september og modtog i december endnu en klage. I begge sager har personer klaget over, at de ikke har kunnet få oplyst, hvorvidt Europol har registreret oplysninger om dem.

Klageudvalget udtalte i forbindelse med sin afgørelse i september 2003, at Europol i overensstemmelse med artikel 19, stk. 7, skulle have meddelt klageren, at Europol ikke behandlede oplysninger om ham.

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 Rigspolitichefens 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 Benelux, 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.

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.

Den fælles Tilsynsmyndighed har i 2003 afholdt 5 møder. Tilsynsmyndigheden har bl.a. diskuteret myndighedens fremtidige arbejde set i lyset af et kommende SIS II system. En del af tilsynsmyndighedens medlemmer deltog i den forbindelse i et seminar om SIS II arrangeret af Europa-Parlamentet, hvor bl.a. tilsynsmyndighedens formand holdt et indlæg.

Derudover har Den fælles Tilsynsmyndighed som led i en informationskampagne i 2003 lanceret en hjemmeside. Hjemmesiden er på nuværende tidspunkt ikke tilgængelig på dansk, men den engelske udgave findes på følgende adresse: http://www.schengen-JSA.dataprotection.org.

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 personoplysninger. 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 2003 blev der afholdt et enkelt møde i den fælles tilsynsmyndighed, hvor repræsentanter for OLAF præsenterede CIS-toldinformationssystemet. Derudover diskuterede den fælles tilsynsmyndighed det fremtidige arbejde efter informationssystemets ibrugtagen.

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. Tilsynet med den forordningsregulerede del af systemet (søjle I) føres af den uafhængige kontrolinstans, der er omhandlet i EU-traktatens artikel 286, se nedenfor.

Sekretariatet for de fælles tilsynsmyndigheder

EU-Rådet har den 17. oktober 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.

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.

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 mv.) 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.

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 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 an-

vendelse 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.

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.

Arbejdsopgaver: 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 2003 afholdt 6 to-dagsmøder og 1 et-dagsmøde. 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 teknologi. Derudover har Datatilsynet deltaget i en underarbejdsgruppe "Task Force on Simplification of Notification Requirements", som arbejder med en mulig forenkling af anmeldelsesordningen.

Artikel 29-gruppen har i 2003 vedtaget en række henstillinger, udtalelser mv.

Der er således vedtaget dokumenter om følgende:
- Arbejdsdokument om online-autentificeringstjenester (WP 68)
- Udtalelse nr. 1/2003 om lagring af trafikdata til debiteringsformål (WP 69)
- Artikel 29-gruppens arbejdsprogram for 2003 (WP 71)
- Arbejdsdokument om e-forvaltning (WP 73)
- Arbejdsdokument om overførsel af personoplysninger til tredjelande: Anvendelse af artikel 26 (2) af EU's databeskyttelsesdirektiv på bindende branchekodekser for internationale dataoverførsler (WP 74)
- Udtalelse nr. 2/2003 om anvendelse af databeskyttelsesprincipperne på Whoisregistre (WP 76)
- Udtalelse nr. 3/2003 om FEDMAs europæiske adfærdskodeks for brug af personoplysninger i forbindelse med direkte markedsføring(WP 77)
- Udtalelse nr. 4/2003 om beskyttelsesniveauet i USA ved overførsel af passagerers personoplysninger (WP 78)
- Udtalelse nr. 5/2003 om databeskyttelsesniveauet i Guernsey (WP 79)
- Arbejdsdokument om biometri (WP 80)
- Udtalelse nr. 6/2003 om databeskyttelsesniveauet i Isle of Man (WP 82)
- Udtalelse nr. 7/2003 om genanvendelse af personoplysninger fra den offentlige sektor og databeskyttelse (WP 83)
- Udtalelse nr. 8/2003 om udkast til standardkontrakt indgivet af en gruppe forretningsforeninger (WP 84)

Artikel 29-gruppens dokumenter er tilgængelige på Kommissionens hjemmeside, hvortil der er adgang via link fra Datatilsynets hjemmeside. Tilsynets hjemmeside indeholder yderligere informationer 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 direktivet 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.

Ved Europaparlamentets og Rådets afgørelse af 22. december 2003 blev hollænderen Peter Johan Hustinx udpeget til europæisk tilsynsførende for databeskyttelse for en femårig periode.

Eurojust

Retsgrundlag: Rådets afgørelse af 28. februar 2002 om oprettelse af Eurojust for at styrke bekæmpelsen af grov kriminalitet (Eurojust-afgørelsen).

Ikrafttræden: Rådsafgørelsen nødvendiggjorde ikke lovgivningsmæssige foranstaltninger i Danmark og trådte således i kraft ved offentliggørelsen den 6. marts 2002, jf. afgørelsens artikel 43.

Formål: Eurojust har til opgave at lette den egentlige koordinering mellem medlemslandenes retsforfølgende myndigheder og støtte efterforskningen i

kriminalsager vedrørende organiseret kriminalitet, især med udgangspunkt i Europols analyser. Eurojust skal endvidere arbejde tæt sammen med det Europæiske Retlige Netværk vedrørende forenkling og efterkommelse af retsanmodninger.

Arbejdsopgaver: I henhold til Eurojust-afgørelsens artikel 23 oprettes der en fælles kontrolinstans til overvågning af Eurojusts aktiviteter med henblik på at sikre, at disse aktiviteter finder sted i overensstemmelse med Eurojust-afgørelsens bestemmelser vedrørende datasikkerhed. Den fælles kontrolinstans har endnu ikke påbegyndt sit arbejde, da en forretningsorden først forventes vedtaget i løbet af 2004.

Datatilsynet er repræsenteret i den fælles kontrolinstans.

Det følger af Eurojust-afgørelsen, at den fælles kontrolinstans ved behandlingen af konkrete sager vedrørende databeskyttelsesspørgsmål skal bestå af tre faste dommere suppleret af ad hoc-dommere fra de lande, der er parter i den konkrete sag. En medlemsstats udpegede dommer bliver fast medlem i året op til den pågældende medlemsstats overtagelse af formandskabet for Det Europæiske Råd. Datatilsynets repræsentant vil således kun deltage i kontrolinstansens arbejde i de perioder, hvor Danmark har formandskabet for Det Europæiske Råd, og når der indbringes sager for kontrolinstansen vedrørende Danmark.

EU-datakommissærernes 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 2003 blev den årlige EU-datatilsynskonference afholdt i Sevilla, arrangeret af det spanske tilsyn (Agencio de Protección de Datos). På konferencen drøftedes en række spørgsmål af fælles interesse, bl.a. uafhængige tilsynsmyndigheders rolle, internationale overførsler af data og databeskyttelse i telesektoren.

International konference for datatilsyns-myndigheder mv.

Det 25. årlige internationale møde for datatilsynsmyndighederne blev i september 2003 afholdt i Sydney, arrangeret af det australske datatilsyn. På konferencen beskæftigede man sig med en række emner af fælles interesse, herunder bl.a. uafhængige tilsynsmyndigheders rolle og beskyttelse af personoplysninger i international sammenhæng.

I forbindelse med det 25. årlige internationale møde afholdt de europæiske databeskyttelseskommissærer et lukket møde. I den anledning afgav databeskyttelseskommissærerne udtalelser vedrørende overførsel af oplysninger om passagerer, RFID ("radio-frequency identification"), forbedring af kommunikation af praksis vedrørende databeskyttelse, automatisk software opdatering og databeskyttelse og internationale organisationer.

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/indeks.htm). Gruppen og dens dokumenter beskrives nærmere på Datatilsynets hjemmeside under Internationalt.

Nordisk samarbejde

Det nordiske samarbejde mellem datatilsynsmyndighederne i Danmark, Finland, Island, Norge og Sverige er blevet fortsat, og i 2003 stod det finske datatilsyn for afholdelse af det fællesnordiske datachefmøde.

På mødet udvekslede deltagerne oplysninger om såvel generelle som konkrete spørgsmål. Bl.a. diskuterede deltagerne særlige spørgsmål i tilknytning til elektronisk overvågning på arbejdspladser, biometri, e-government, genanven-

delse af offentlige data og forhåndskontrol af behandling af oplysninger til genforskning.

I 2003 blev der endvidere afholdt Nordisk Teknikermøde i Oslo og Nordisk Sagsbehandlermøde i Stockholm. I Stockholm blev særligt spørgsmålet vedrørende anvendelse af biometri diskuteret, mens det Nordiske Teknikermøde bl.a. drøftede inspektionsstrategier og afrapportering, formidling og information om persondatabeskyttelse og konkrete sikkerhedstiltag, de danske OCES-certifikater, regler og praksis i forhold til tv-overvågning, sikkerhed i trådløse netværk samt beskyttelse af persondata på internettet og ved brug af e-post.

Sikkerhedsspørgsmål

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 Datatilsynets hjemmeside.

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 mv. Det er således Datatilsynets opfattelse, at persondatalovens § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i private virksomheder mv. 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.

Herudover kan det ved brug af digital signatur sikres, at dokumentet kommer fra den angivne afsender og ikke er ændret undervejs.

Børnetelefonen

Anbefalet etablering af en særlig facilitet ved indhentelse af digitalt samtykke, samt udtalt, at der for at opnå et tilfredsstillende sikkerhedsmæssigt niveau skal etableres et miljø, der som minimum sikrer fortrolighed og serverautenticitet (servercertifikat) (Datatilsynets j.nr. 2002-42-0365)

"Børns Vilkår" ansøgte Datatilsynet om tilladelse til oprettelse af et chat-forum på internettet, hvor børn og unge kan hente rådgivning ("Børnetelefonen på nettet").

Datatilsynet behandlede i den forbindelse spørgsmål om samtykke og sikkerhed:

1. Samtykke

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

I kravet om, at et samtykke skal være specifikt, ligger, at samtykket skal være konkretiseret således, at det klart og utvetydigt fremgår, hvad der meddeles samtykke til, herunder hvilke oplysninger der må behandles på baggrund af samtykket, af hvem og til hvilke formål.

Samtykket vil kunne gives digitalt eller på anden måde, der indebærer en aktiv handling fra den registreredes side. Det er således ikke en betingelse, at samtykket gives skriftligt.

Tilsynet vurderede umiddelbart, at et barn, der er i stand til selv at logge sig på chatrummet og dér afgive oplysninger, som udgangspunkt normalt også gyldigt vil kunne samtykke til den omhandlede databehandling.

Tilsynet lagde i denne forbindelse især vægt på, at barnet selv aktivt skal logge sig på chatrummet, at barnet selv skriver og dermed afgiver de omhandlede oplysninger, og at oplysningerne efter det oplyste i øvrigt ikke ville blive lagret og senere anvendt til andre formål.

Datatilsynet understregede dog, at afgørelsen af, hvorvidt der foreligger et gyldigt samtykke, beror på en konkret vurdering i hver enkelt situation, hvor bl.a. barnets individuelle modenhed har betydning. Tilsynet forbeholdt sig derfor sin stilling ved en eventuel senere klagesag.

Tilsynet anbefalede i øvrigt, at Børns Vilkår for at undgå tvivl på den side, der giver adgang til chatten, etablerer en særlig facilitet, der sikrer, at de registrerede afgiver et samtykke, der opfylder lovens krav. Dette kunne eksempelvis gøres ved en kort tekst, som de besøgende obligatorisk skal klikke "ja" til at have læst og accepteret for at få adgang til chatten.

2. Sikkerhed

Der er udover persondatalovens § 41, stk. 3, ingen specifikke regler for private organisationers transmission af persondata over det åbne internet, men for offentlige myndigheder gælder sikkerhedsbekendtgørelsen.

Datatilsynet fandt, at der for at opnå et tilfredsstillende sikkerhedsmæssigt niveau skulle etableres et miljø, der som minimum sikrer fortrolighed og serverautenticitet (servercertifikat).

Efter Datatilsynets opfattelse skulle disse elementer indføres for at imødegå risikoen for, at uvedkommende kan læse kommunikationen, samt for at sikre chatsidens identitet. F.eks. vil der være risiko for, at andre på internettet udgiver sig for at være Børns Vilkårs netrådgivning ved at etablere en side, som har næsten samme navn, og som vil kunne forveksles med den ægte side.

Iagttagelse af de nævnte krav vil i praksis kunne ske f.eks. ved anvendelse af (korrekt opsat) SSL (Secure Sockets Layer).

E-post fra et psykiatrisk hospital i Århus

Anbefalet, at arbejdsrelaterede fortrolige og følsomme personoplysninger ikke behandles på medarbejderes private pc'er. Hvis sådan behandling undtagelsesvist skal ske, bør der foreligge en aftale mellem myndigheden og den ansatte herom, og myndigheden bør konkret have sikret sig, at beskyttelsen af personoplysninger er tilstrækkelig (Datatilsynets j.nr. 2003-632-0056)

Datatilsynet blev gennem pressen opmærksom på, at Psykiatrisk Hospital i Århus havde sendt en e-post med fortrolige oplysninger om en patient til en speciallæge i psykiatri, og at der efterfølgende var sket en spredning af patientoplysninger fra dennes computer.

Speciallægen var fastansat som konsulent på deltid ved Psykiatrisk Hospital i Århus. Derudover drev speciallægen en privat speciallægepraksis samt et privat firma.

Speciallægen oplyste, at personoplysninger vedrørende patienter i hans private praksis blev opbevaret på en "stand-alone" computer, der hverken var tilsluttet lokale netværk eller internettet.

Til brug for sin private virksomhed havde speciallægen desuden en computer, der var tilsluttet internettet, som også blev anvendt til at sende og modtage e-post meddelelser. Der var installeret et antivirus program på computeren. På trods af, at dette program løbende blev opdateret via internettet, havde det i det foreliggende tilfælde ikke været i stand til at beskytte mod, at computeren blev virusinficeret. En virus på speciallægens computer bevirkede således, at en e-post fra Psykiatrisk Hospital blev videresendt til en række e-postadresser indeholdt i speciallægens adressekartotek.

Den pågældende e-post var sendt fra Retspsykiatrisk afdeling til speciallægen for at underrette denne om, at en patient var mødt til en aftale en time tidligere end aftalt. Formålet hermed var at foranledige speciallægen til at møde snarest muligt på afdelingen, således at patientens ventetid kunne begrænses. Man havde fra afdelingens side forsøgt at træffe speciallægen telefonisk, men da dette ikke var muligt, blev der i stedet afsendt en e-post. E-posten indeholdt navnet på patienten samt oplysninger om, at han var i politiets varetægt.

Århus Amt oplyste, at det klart fremgik af psykiatriens/hospitalets retningslinier for håndtering af e-post, at en e-post ikke må indeholde patientoplysninger eller andre personhenførbare oplysninger, såfremt e-posten sendes til en modtager uden for psykiatriens e-postsystem.

Når den konkrete e-post indeholdt fortrolige oplysninger, var der efter amtets opfattelse tale om en enkeltstående meget beklagelig fejl, der blev forstærket af den uheldige omstændighed, at speciallægens computer var inficeret med virus.

Datatilsynet fandt, at den omhandlede e-post indeholdt fortrolige oplysninger, som tillige var af følsom karakter. Det forhold, at en person er patient ved et psykiatrisk hospital udgør således efter Datatilsynets opfattelse en oplysning om helbredsmæssige forhold omfattet af lovens § 7. Derudover fandt Datatilsynet, at oplysningen i e-posten om, at den pågældende person var i politiets varetægt, afslørede følsomme oplysninger om strafbare forhold, jf. persondatalovens § 8.

Datatilsynet måtte således konstatere, at der fra Psykiatrisk Hospital i Århus var sendt en almindelig e-post indeholdende oplysninger omfattet af såvel § 7 og § 8 i persondataloven. Der var hverken anvendt kryptering eller digital signatur. Datatilsynet anså det skete som en alvorlig tilsidesættelse af såvel kravene til datasikkerhed som kravet om god databehandlingsskik, og tilsynet fandt den skete overtrædelse af persondataloven kritisabel.

Datatilsynet henstillede derfor, at Århus Amt i overensstemmelse med persondatalovens krav om god databehandlingsskik og behandlingssikkerhed etablerer hensigtsmæssige sagsbehandlingsprocedurer i forbindelse med ekstern e-post og giver den fornødne instruktion til medarbejdere, der behandler personoplysninger, herunder såvel fuldtids- som deltidsansatte.

Vedrørende medarbejderes brug af privat pc i arbejdsmæssig sammenhæng udtalte Datatilsynet, at dette indebærer en risiko for, at eventuelle personoplysninger kommer til uvedkommendes kendskab eller i øvrigt behandles i strid med persondataloven.

Brug af private pc'ere til behandling af personoplysninger for en offentlig myndighed må efter Datatilsynets opfattelse kun ske, hvis myndigheden har sikret sig, at der derved ikke sker nogen forringelse af beskyttelsen af oplysningerne, jf. sikkerhedsbekendtgørelsens § 7, stk. 2, der omhandler behandling af personoplysninger på pc-arbejdspladser uden for den dataansvarliges lokaler.

Behandling af fortrolige oplysninger medfører skærpede krav til sikkerheden. Samtidig medfører udbredelsen af internet, at den private pc i mange tilfælde har internet opkobling, hvilket alt andet lige medfører en øget risiko for, at oplysningerne utilsigtet kommer til uvedkommendes kendskab, f.eks. på grund af virus som i den konkrete sag.

Datatilsynet anbefalede derfor generelt, at fortrolige og følsomme personoplysninger ikke behandles på medarbejderes private pc'er. Hvis sådan behandling undtagelsesvist skal ske, bør der foreligge en aftale mellem myndigheden og den ansatte herom, og myndigheden bør konkret have sikret sig, at beskyttelsen af personoplysninger er tilstrækkelig.

Datatilsynet anmodede på denne baggrund Århus Amt om at oplyse, hvorvidt amtet accepterer, at medarbejdere behandler personoplysninger på egne pc'ere, og i givet fald på hvilke vilkår.

Amtet har herefter meddelt, at det følger af gældende datasikkerhedsregler for ansatte i Psykiatrien i Århus Amt, at ansatte ikke må sende må sende e-post med personoplysninger uden for psykiatriens e-postsystem, og at det følger af reglerne, at ansatte ikke må benytte private pc'ere til behandling af personoplysninger.

Forskellige spørgsmål i relation til OCES certifikater

Datatilsynet udtalte i 2002, at såkaldte OCES certifikater generelt vil kunne benyttes ved borgernes indsendelse af oplysninger til myndigheder. For så vidt angår selvbetjeningsløsninger med en facilitet til forudfyldte blanketter udtalte Datatilsynet, at persondatalovens krav vil være opfyldt, hvis der anvendes digital signatur med et OCES certifikat (omtalt i årsberetningen for 2002, s. 93).

Datatilsynet var af den opfattelse, at en registreringsprocedure i forbindelse med certifikatudstedelse, som er baseret på brug af folkeregisteradressen ved identitetskontrol, må anses for at være tilstrækkelig sikker i relation til de databeskyttelsesmæssige krav.

Datatilsynet har i 2003 taget stilling til en række spørgsmål vedrørende OCES certifikater, herunder om certifikatpolitikken (CP'en) og om registreringsprocedurerne. Derudover har Datatilsynet generelt udtalt sig om behovet for at beskytte personoplysninger i de løsninger, der bliver etableret, og hvor OCES certifikatet vil kunne bruges (Datatilsynets j.nr. 2002-321-0142):

Indholdet af certifikatpolitikken (særligt mht. personnumre)

I relation til udstedelse af OCES certifikater har Datatilsynet særligt henledt opmærksomheden på, at persondatalovens § 11, stk. 2, medfører, at et certificeringscenter (CA) kun må indsamle og registrere oplysninger om en borgers personnummer, hvis borgeren har givet sit udtrykkelige samtykke hertil.

I CP'en henvises generelt til persondataloven. Persondataloven sætter således grænser for, hvad et certificeringscenter må gøre med de personoplysninger, som en virksomhed som certificeringscenter kommer i besiddelse af.

Registreringsprocedurer

Datatilsynet har endvidere tilkendegivet, at tilsynet lægger overordentlig stor vægt på, at sikkerheden i OCES er tilstrækkelig høj, idet OCES certifikaterne efter det oplyste skulle anvendes til alle typer af oplysninger, herunder også til udlevering af følsomme oplysninger omfattet af persondatalovens §§ 7 og 8.

Datatilsynet forudsatte, at brugerne gives mulighed for at få en oversigt over udstedte, udløbne og spærrede certifikater, f.eks. ved opslag på certifikat.dk. En sådan service er efter Datatilsynets opfattelse et væsentligt element i den samlede sikkerhedsløsning.

Ministeriet for Videnskab, Teknologi og Udvikling beskrev over for Datatilsynet forskellige registreringsprocedurer, der påtænktes anvendt.

Datatilsynet fandt to af disse metoder tilstrækkelig sikre, men forbeholdt sig dog sin stillingtagen, hvis der i praksis i relation til persondataloven skulle vise sig uhensigtsmæssigheder ved brugen af de skitserede sikkerhedsløsninger. Datatilsynet har siden fået forelagt forskellige registreringsprocedurer for særlige situationer.

Beskyttelse af følsomme oplysninger med stærk kryptering

Datatilsynet udtalte endvidere, at ansvaret for, at oplysninger, der udveksles ved hjælp af en selvbetjeningsløsning, er tilstrækkeligt beskyttede, påhviler den dataansvarlige myndighed eller virksomhed, der stiller servicen til rådighed.

Efter Datatilsynets opfattelse bør selvbetjeningsløsninger ikke give borgerne mulighed for at fravælge de sikkerhedsforanstaltninger, der skal beskytte oplysningerne. Datatilsynet har således tidligere udtalt, at sikkerhedsreglerne hverken kan fraviges ved en orientering af borgeren om sikkerhedsmanglerne eller ved indhentelse af et samtykke fra borgeren til fravigelsen.

Efter Datatilsynets opfattelse bør den myndighed eller virksomhed, der er dataansvarlig i forbindelse med en selvbetjeningsløsning, sikre sig, at anvendelsen af selvbetjeningsløsningen sker med de fornødne sikkerhedsforanstaltninger. Dette er navnlig relevant ved transmission af følsomme oplysninger over internet, hvor oplysningerne efter Datatilsynets opfattelse skal beskyttes ved stærk kryptering.

Efter Datatilsynets opfattelse afhænger sikkerheden i forbindelse med brug af digital signatur således ikke kun af, om det benyttede certifikat, f.eks. OCES, er tilstrækkelig sikkert, men tillige af, om myndigheder og borgere ved deres brug af certifikatet er opmærksomme på at beskytte oplysningerne.

Det er derfor vigtigt, at såvel borgere som myndigheder informeres om, hvordan OCES certifikater anvendes med henblik på at opnå den ønskede grad af sikkerhed ved udveksling af oplysninger i konkrete situationer.

Tilsynet noterede sig, at IT- og Telestyrelsen ville offentliggøre såvel borgerrettet information som vejledninger og informationsmateriale til myndigheder, samt at en del information er tilgængelig på TDC's hjemmesider.

Yderligere detaljer omkring Datatilsynets afgørelser omkring ovenstående kan findes på www.datatilsynet.dk under "Værd at vide" – elektronisk borgerservice.

Tilknytning af personnummer til OCES medarbejdercertifikater (j. nr. 2003-321-0240)

I forbindelse med udviklingen af Sundhedsportalen viste der sig et behov for at kende brugerens personnummer i de tilfælde, hvor sundhedspersonale i arbejdsmæssig sammenhæng logger på Sundhedsportalen ved hjælp af deres OCES medarbejdercertifikat. IT- og Telestyrelsen rettede på denne baggrund henvendelse til Datatilsynet vedrørende muligheden for at tilknytte personnumre til medarbejdercertifikater, således at det ved opslag på et løbenummer i certifikatet vil være muligt at få oplyst det tilknyttede personnummer.

Denne funktion vil modsvare den tilsvarende funktion på OCES personcertifikater, hvor der til certifikatets PID nummer er knyttet brugerens personnummer.

Datatilsynet vurderede, at offentlige myndigheder på baggrund af løbenumre i medarbejdercertifikater kan foretage opslag af de tilhørende personnumre, når dette sker med henblik på entydig identifikation. Datatilsynet vurderede endvidere, at private kan foretage sådanne opslag, når den registrerede har givet sit udtrykkelige samtykke dertil.

Datatilsynet havde i øvrigt ikke bemærkninger i forhold til registrerings- og verificeringsproceduren

Datatilsynet måtte dog forbeholde sig sin stillingtagen, hvis der i praksis skulle vise sig uhensigtsmæssigheder i ved brugen af procedurerne.

Sikkerhedsbrist i Helsingør Kommunes trådløse net

Udtalt, at tilsynet anser et trådløst netværk for en ekstern kommunikationsforbindelse, og at der allerede fra det tidspunkt, hvor der etableres trådløse netværk, bør etableres forretningsgange til kontrol af konfigurationsændringer i det trådløse netværk (Datatilsynets j.nr. 2003-632-0054)

En borger havde til et borgermøde i rådhusets byrådssal medbragt en bærbar computer. Borgeren blev i den forbindelse opmærksom på, at han kunne se et trådløst netværk tilhørende Helsingør Kommune, herunder netværkets navn og et antal servere og arbejdsstationer på netværket. Borgeren henvendte sig derfor først til kommunen og siden til Datatilsynet.

Helsingør Kommune oplyste over for Datatilsynet, at borgeren ikke havde været logget ind på kommunens netværk og dermed ikke havde haft adgang til at læse, modificere eller slette data. Kommunen oplyste endvidere, at borgeren ikke umiddelbart havde haft mulighed for adgang til data. Kommunen konstaterede ved sin fejlsøgning, at årsagen til fejlen var en konfigurationsfejl, som, efter at den var fundet, hurtigt kunne rettes. For at undgå fremtidi-

ge fejlkonfigureringer havde kommunen udarbejdet nye skærpede sikkerhedsprocedurer for konfigurationsændringer.

Foruden de skærpede sikkerhedsprocedurer beskrev kommunen det løbende arbejde med at kontrollere og verificere sikkerheden i kommunens netværk samt de sikkerhedsmekanismer, der findes i det trådløse netværk. Kommunen redegjorde desuden for forløbet af fejlsøgning, -rettelse og verifikation af rettelsen.

Datatilsynet noterede sig på grundlag af kommunens redegørelse bl.a.:

- at borgeren, der konstaterede ovennævnte sikkerhedsbrist, ikke havde haft adgang til personoplysninger,
- at kommunen for at undgå fremtidige fejlkonfigureringer havde udarbejdet nye skærpede sikkerhedsprocedurer, hvori der blandt andet indgik efterfølgende kontrol af konfigurationsændringer,
- at fejlen blev konstateret en fredag, efterforsket henover weekenden og rettet den følgende mandag, hvor også effekten af fejlrettelsen blev kontrolleret, og
- at kommunen havde fulgt udviklingen omkring trådløse netværk, hvilket løbende havde ført til etablering af sikkerhedsforanstaltninger af forskellig art samt planer for mere gennemgribende forbedringer.

Datatilsynet udtalte, at et trådløst netværk er at anse for en ekstern kommunikationsforbindelse, idet det område, som nettet radiomæssigt dækker, typisk vil kunne strække sig uden for det geografiske område, hvori det trådløse netværk ønskes anvendt. Det var derfor Datatilsynets opfattelse, at enhver enhed i et trådløst lokalnet er et potentielt angrebspunkt, som vil kunne angribes udefra. Derfor fandt Datatilsynet, at kommunen allerede fra det tidspunkt, hvor der etableres trådløse netværk, bør have etableret forretningsgange til kontrol af konfigurationsændringer i det trådløse netværk.

I forbindelse med behandlingen af sagen, blev Datatilsynet opmærksom på, at Helsingør Kommunes trådløse netværk på anden vis ikke opfyldte de sikkerhedskrav, som Datatilsynet stiller til trådløse netværk, hvori der transporteres følsomme personoplysninger.

Datatilsynet fandt dette forhold kritisabelt og henstillede, at Helsingør Kommune straks bragte forholdet i orden.

Helsingør Kommune har herefter – i overensstemmelse med planer, der allerede forelå forud for den sikkerhedsmæssige hændelse – anskaffet et nyt trådløst netværk til rådhuset og taget det gamle netværk ud af drift. Udskiftningen har medført, at kommunens netværk nu er i stand til at opfylde de

sikkerhedskrav, som Datatilsynet stiller til trådløse netværk, hvori der transporteres følsomme personoplysninger.

Sikkerhedsbrist hos Socialministeriet

Fundet, at den dataansvarlige i overensstemmelse med persondatalovens § 41, stk. 3, bør drage omsorg for, at der foretages de nødvendige skridt til at afhjælpe problemer snarest muligt efter, at en sikkerhedsbrist er blevet kendt. Endvidere konstateret, at § 41, stk. 3, ikke havde været overholdt, idet det på trods af iværksatte foranstaltninger i form af kodeord mv. var lykkedes uvedkommende at få adgang til personoplysninger, som efter omstændighederne kunne indeholde fortrolige eller følsomme oplysninger (Datatilsynets j.nr. 2002-632-0050)

Datatilsynet blev via pressens omtale af sikkerheden i trådløse netværk opmærksom på, at uvedkommende havde haft adgang til et netværk i Socialministeriet.

En nærmere belysning af sagen viste, at der var tale om kablet og ikke et trådløst netværk, idet Socialministeriet ikke benyttede trådløse netværk. Det omtalte indbrud var sket på et netværk, som blev benyttet af Ligestillingsafdelingen, og som var helt uafhængigt af Socialministeriets netværk.

Socialministeriet oplyste i den forbindelse, at Ligestillingsafdelingens centrale servere – efter en ressortomlægning i november 2001 – i løbet af juli 2002 var blevet overført til Socialministeriet fra Boligministeriets edb-afdeling, som indtil da havde været ansvarlig for implementering og drift af Ligestillingsafdelingens edb-systemer. Ministeriet oplyste endvidere, at det med særlig viden og på grund af nogle sikkerhedsbrister i en ældre Lotusapplikation havde været muligt at skaffe sig adgang til Ligestillingsafdelingens journalsystem. Journalsystemet indeholdt oplysninger om ind- og udgående post, ligesom udgående post og e-post m.m. var tilgængeligt i systemet.

Datatilsynet konkluderede, at der havde været adgang til at læse oplysninger, som efter omstændighederne kunne indeholde følsomme personoplysninger, idet der i følge ministeriet f.eks. kunne være registret oplysninger om fagforeningsmæssige tilhørsforhold. Det var Socialministeriets opfattelse, at der ikke havde været adgang til at modificere disse data, da dette krævede opstart af en kodeordsbeskyttet applikation.

Socialministeriet oplyste, at den funktion, som skabte den sikkerhedsmæssige brist, straks var blevet fjernet, og at systemet var under en modernisering, der skulle bringe det op på samme sikkerhedsmæssige niveau som Socialministeriets øvrige edb-systemer.

Afslutningsvis oplyste Socialministeriet, at det umiddelbart efter ressortomlægningen var blevet besluttet at udskifte det omtalte journalsystem blandt andet på grund af de konstaterede mangler. Det nye system var planlagt til at skulle gå i drift i august 2002. En forsinkelse medførte imidlertid, at dette først skete i oktober 2003.

Sagen gav Datatilsynet anledning til at komme med bemærkninger vedrørende følgende forhold:

1. Sikkerhedsforhold omkring systemet
2. Manglende anmeldelse til Datatilsynet
3. Manglende efterlevelse af sikkerhedsbekendtgørelsens § 5 og § 19

1. Sikkerhedsforhold omkring systemet

Datatilsynet noterede sig, at såvel Ligestillingsafdelingens netværk som afdelingens journalsystem var sikret med adgangskoder, at data på serveren var lagret i en form, der ikke var umiddelbart læselig, og at den eksterne server, som blev anvendt ved indbruddet, var søgt sikret ved hjælp af adgangskoder og kryptering.

Af Socialministeriets redegørelse fremgik det, at der var tale om en "ikke ukendt sikkerhedsbrist" i det anvendte programmel. Datatilsynet opfattede Socialministeriets svar således, at en korrekt udført konfiguration ville kunne have afhjulpet problemet.

Datatilsynet fandt, at den dataansvarlige i overensstemmelse med persondatalovens § 41, stk. 3, burde have draget omsorg for, at der var blevet foretaget de nødvendige skridt til at afhjælpe problemet snarest muligt efter, at sikkerhedsbristen i det anvendte programmel var blevet kendt.

Datatilsynet måtte konstatere, at det på trods af iværksatte foranstaltninger i form af kodeord mv., var lykkedes uvedkommende at få adgang til personoplysninger, som efter omstændighederne kunne indeholde fortrolige eller følsomme oplysninger, og at persondatalovens § 41, stk. 3, således ikke havde været overholdt, idet der efter denne regel skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab.

2. Manglende anmeldelse til Datatilsynet

Det fremgik af ministeriets redegørelse, at Ligestillingsafdelingens journalsystem ikke havde været anmeldt til Datatilsynet. Systemet kunne derfor ikke benyttes lovligt, før der var foretaget anmeldelse, og der eventuelt var modtaget en udtalelse fra Datatilsynet. Tilsynet indskærpede derfor reglerne i persondatalovens kapitel 12 om anmeldelse af behandlinger, der foretages for

den offentlige forvaltning, og henstillede, at der blev foretaget en anmeldelse, eller at Ligestillingsafdelingens journalsystem blev taget ud af drift.

3. Manglende efterlevelse af sikkerhedsbekendtgørelsens § 5 og § 19
Datatilsynet noterede sig, at den eksterne adgang til pågældende server var blevet lukket.

Det fremgik af ministeriets redegørelse, at der ikke i Ligestillingsafdelingen havde været fastsat regler for området. Det fremgik endvidere af ministeriets redegørelse, at der - ud over lukning af den eksterne adgang til serveren – ikke blev foretaget yderligere foranstaltninger i form af organisatoriske ændringer e.l.

Datatilsynet henstillede i den forbindelse, at der i overensstemmelse med sikkerhedsbekendtgørelsens § 14 fastsættes regler i form af en politik eller lignende for netværksadgang til Socialministeriets edb-systemer. Tilsynet henstillede endvidere, at der placeres et organisatorisk ansvar for at iværksætte procedurer, som skal sikre periodisk kontrol af, at reglerne på området efterleves, at de foranstaltninger, der værksættes som følge af reglerne, er tidssvarende, samt at foranstaltningernes effektivitet løbende kontrolleres.

Da journalsystemet efter omstændighederne kan indeholde følsomme oplysninger, skal det opfylde sikkerhedsbekendtgørelsens kapitel 3 om bl.a. logning af systemets anvendelse. Af ministeriets redegørelse fremgik det, at journalsystemet ikke indeholdt mulighed for at logge i henhold til sikkerhedsbekendtgørelsens § 19. Datatilsynet henstillede derfor, at der blev iværksat logning, eller at systemet blev taget ud af drift, indtil forholdet var bragt i orden.

Socialministeriet har efterfølgende oplyst, at et nyt journalsystem til afløsning af Ligestillingsafdelingens fejlbehæftede system er sat i drift. Det nye journalsystem indeholder faciliteter til logning og adgangskontrol. Systemet er omfattet af Departementets sikkerhedsinstrukser og procedurer vedrørende adgang til ministeriets netværk og edb-systemer.

Sundhedsportalen

Udtalelse om, i hvilke tilfælde Sundhedsportalen er dataanvarlig eller databehandler, om videregivelse via portalen og om sikkerhed mv. (Datatilsynets j. nr. 2003-082-0128)

Den fælles offentlige sundhedsportal rettede henvendelse til Datatilsynet med en række spørgsmål.

Datatilsynet behandlede sagen i Datarådet.

Dataansvar/databehandler

I persondatalovens § 3, nr. 4, defineres "den dataansvarlige" som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.

I lovens § 3, nr. 5, defineres "databehandleren" som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

Datatilsynet var enig i, at Sundhedsportalen kan optræde enten som databehandler eller dataansvarlig, og at der kan være tilfælde, f.eks. ved brug af links, hvor der end ikke er tale om en databehandlerrolle.

I relation til en række tilfælde, som Sundhedsportalen havde beskrevet, bemærkede Datatilsynet følgende:

- Datatilsynet var umiddelbart enig i, at Sundhedsportalen hverken er dataansvarlig eller databehandler ved etablering af link på portalen til data, der opbevares hos en indholdsleverandør. Det samme er tilfældet ved online data, der bliver "framet" ind på portalen, således at indholdsleverandørens webside eller data bliver vist direkte i portalens "portlets". Datatilsynet forudsatte herved, at det er klart for brugerne, at data stammer fra en ekstern leverandør.

- Herudover kan online data indgå i Sundhedsportalens interaktive services, således at Sundhedsportalen på baggrund af visse parametre angivet af en bruger fremsender en forespørgsel til en ekstern datakildeleverandør. Denne returnerer svar indeholdende de forespurgte data til Sundhedsportalen, som formaterer det modtagne svar og præsenterer modtageren for resultatet.

  Datatilsynet var umiddelbart enig i, at Sundhedsportalen må anses for at være databehandler i forhold til disse data, og at den eksterne datakildeleverandør derfor er dataansvarlig for videregivelsen via portalen. Datatilsynet forudsatte også i dette tilfælde, at brugeren kan se, hvem vedkommende kommunikerer med.

- Sundhedsportalen anførte vedrørende "ikke-online data", der indgår i en af Sundhedsportalens tjenester på samme måde som online data, at det afgørende for, om Sundhedsportalen må anses for databehandler eller dataansvarlig, må anses for at være aftalen vedrørende disse data mellem Sundhedsportalen og indholdsleverandøren – herunder om indholdsleverandøren helt har opgivet råderetten over disse data.

Datatilsynet havde ikke umiddelbart bemærkninger hertil. Datatilsynet henledte dog opmærksomheden på, at dataansvar for Sundhedsportalen i praksis kun vil kunne foreligge, hvis indholdsleverandøren lovligt kan videregive oplysningerne til Sundhedsportalen, og hvis Sundhedsportalen opfylder lovens betingelser for behandling af oplysninger. I hvilket omfang dette vil være tilfældet kan ikke angives generelt, men må bero på de enkelte tilfælde.

- Herudover var det oplyst, at ikke-online data kan indgå i en tjeneste på portalen. Dataene er grundlaget for tjenesten, men fremvises ikke for brugerne. Som eksempel var nævnt autorisationsregisteret, som Sundhedsportalen ønsker at modtage fra Sundhedsstyrelsen.

  Datatilsynet var umiddelbart enig i, at det er nærliggende at anse Sundhedsportalen som dataansvarlig i denne forbindelse.

- Med hensyn til såkaldte CMS-data (CMS = Content Management System), som forskellige indholdsleverandører leverer til profilområder på portalen, lagde Datatilsynet til grund, at Sundhedsportalen som udgangspunkt vil være at betragte som databehandler i det omfang, der indgår personoplysninger.

- Sundhedsportalen stiller desuden en personlig postkasse til rådighed for borgerne. Sundhedsportalen vil være dataansvarlig for de oplysninger, der er forbundet med at administrere postkasserne. I forhold til opbevaring og anden behandling af e-post meddelelser måtte Sundhedsportalen efter Datatilsynets opfattelse anses for databehandler.

  I den forbindelse gjorde Datatilsynet opmærksom på, at det skal være klart for brugeren, hvorledes han kan slette beskeder fra systemet. Det skal ligeledes oplyses, i hvilket omfang der tages sikkerhedskopier af beskeder, hvor længe de opbevares, og under hvilke omstændigheder beskederne kan genetableres fra sikkerhedskopierne.

Hvad gælder i de situationer, hvor Sundhedsportalen er databehandler?
Som anført ovenfor vil Sundhedsportalen i en række tilfælde kunne anses for databehandler i forbindelse med, at data fra forskellige kilder kommunikeres via portalen.

I den forbindelse gjorde Datatilsynet opmærksom på, at det af persondatalovens § 42, stk. 1, følger, at når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse at dette sker.

Det følger endvidere af persondatalovens § 42, stk. 2, at gennemførelse af en behandling ved en databehandler skal ske i henhold til skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren.

I øvrigt gjorde Datatilsynet opmærksom på, at der i disse tilfælde kun vil kunne videregives oplysninger via portalen i det omfang, den dataansvarlige for oplysningerne lovligt kan og vil foretage en sådan videregivelse. Efter Datatilsynets opfattelse medfører kravet om, at databehandleren alene må handle efter instruks fra den dataansvarlige, at de dataansvarlige, der vil videregive oplysninger via portalen, må fastlægge, hvordan og til hvem videregivelsen må ske. Retningslinjerne herfor bør tillige indgå i de sikkerhedsbestemmelser, som myndigheden efter sikkerhedsbekendtgørelsens § 5 har pligt til at fastsætte og vedligeholde (uddybende regler).

Vurderingen af, om der kan ske videregivelse, skal ske efter de regler, der gælder for den aktuelle videregivelse fra den pågældende dataansvarlige. Afhængigt af omstændighederne vil videregivelsen således skulle vurderes efter lov om patienters retsstilling, persondataloven eller andre regler, som gælder for den konkrete behandling. Videregivelse fra Lægemiddelstyrelsens Centrale Tilskudsregister vil skulle vurderes efter den derom gældende bekendtgørelse.

En videregivelse vil endvidere skulle være inden for rammerne af den dataansvarliges anmeldelse til Datatilsynet. Hvis der via portalen sker behandlinger, som ikke er angivet i anmeldelsen, f.eks. videregivelse til nye modtagere, vil der skulle indsendes ændringsanmeldelse til Datatilsynet, og Sundhedsportalen vil skulle angives som databehandler i anmeldelserne. Datatilsynet gik ud fra, at Sundhedsportalen gør de dataansvarlige opmærksomme på, at der eventuelt skal ske en ændring af deres anmeldelser.

Selvstændig behandling af personoplysninger om borgere i Sundhedsportalen og hos modtagere af kommunikation via portalen

I det omfang Sundhedsportalen vil opbygge egne databaser med oplysninger om borgerne og/eller sundhedspersonale, skal bl.a. behandlingsreglerne i persondataloven opfyldes.

Videregivelse af personnummeroplysninger

Det var Datatilsynets opfattelse, at kravet om god databehandlingsskik i persondatalovens § 5, stk. 1, medfører, at kommunikationen via portalen bør indrettes således, at personnumre ikke uden samtykke udleveres til private, som kun må behandle oplysninger om personnumre med samtykke. Det bør desuden være gennemskueligt for borgeren, hvem vedkommendes personnummer udleveres til.

Hvis borgeren kommunikerer med en privat dataansvarlig, f.eks. med et apotek eller en privatpraktiserende læge eller tandlæge, forudsætter udlevering af personnummeret (fra en registrering hos portalen eller fra TDC via portalen) efter Datatilsynets opfattelse som udgangspunkt, at borgeren har givet udtrykkeligt samtykke til, at den private dataansvarlige modtager borgerens personnummer. Det kan dog forekomme, at den private dataansvarlige i medfør af anden lov er berettiget til at modtage og registrere personnummeret. Om dette er tilfældet, må bero på, hvilke regler der gælder for den pågældende dataansvarlige. I tvivlstilfælde må Datatilsynet anbefale, at der indhentes samtykke. Private må efter persondatalovens § 11, stk. nr. 1, behandle oplysninger om personnummer, når det følger af lov eller bestemmelser fastsat i henhold til lov.

Samtykket skal leve op til kravene i persondatalovens § 3, nr. 8. Dette indebærer bl.a., at samtykket skal være specifikt og informeret. Derfor vil det efter Datatilsynets opfattelse ikke være tilstrækkeligt at indhente et generelt samtykke i forbindelse med, at borgeren opretter sig som bruger på portalen. Der bør i forbindelse med enhver videregivelse af personnummeret til en privat dataansvarlig indhentes specifikt samtykke fra borgeren, f.eks. ved brug af en særlig tekst, som borgeren skal acceptere ved at klikke ja.

Hvis modtageren ikke har noget sagligt behov for personnummeret, bør dette end ikke med samtykke behandles hos den dataansvarlige. Dette gør sig gældende i forhold til både private virksomheder og offentlige myndigheder. Dette kan f.eks. være tilfældet, hvis der etableres mulighed for at rekvirere informationsmateriale eller andre tjenester, hvor der ikke er behov for personnummeret. Indhentelse af personnummeret i tilfælde, hvor der ikke er behov for dette, vil efter omstændighederne kunne være i strid med persondatalovens § 5, stk. 2 og 3.

Datatilsynet fandt endvidere, at det altid bør være fuldt gennemskueligt for borgeren, at vedkommendes personnummer udleveres. For at opnå dette, bør løsningerne efter Datatilsynets opfattelse indrettes således, at der gives information til borgeren i de tilfælde, hvor personnummeret videregives uden samtykke. Dette kan f.eks. ske ved, at borgeren i alle tilfælde præsenteres for en tekstboks om videregivelsen af personnummeret. Ved videregivelse til en privat dataansvarlig uden særlig lovhjemmel til at behandle personnumre, bør tekstboksen indeholde en egentlig samtykkeerklæring, borgeren skal klikke ja til. Ved videregivelse til offentlige myndigheder og private dataansvarlige, som har lovhjemmel til at behandle personnumre, bør der som minimum gives information om, at personnummeret videregives.

Sikkerhedsforanstaltninger

I forbindelse med anmeldelsen af Sundhedsportalen modtog Datatilsynet tillige en redegørelse for sikkerhedsforanstaltningerne. Det fremgik bl.a., at au-

tentificering kun kan ske ved anvendelse af OCES person- eller medarbejdercertifikat, at der over det åbne internet anvendes sikker kommunikation med stærk kryptering, og at der foretages logning af alle anvendelser af personoplysninger.

Ud fra det oplyste var det Datatilsynets vurdering, at sikkerhedsforanstaltningerne er i overensstemmelse med kravene i sikkerhedsbekendtgørelsen.

I forbindelse med en vurdering af Sundhedsportalens sikkerhedsforanstaltninger traf Datatilsynet afgørelse i to spørgsmål af sikkerhedsmæssig karakter:

Tilknytning af personnummer til OCES
Beskrivelse af denne problemstilling er nærmere omtalt under afsnittet om OCES-certifikater.

Opbevaring af sammenhæng mellem RID/PID og personnummer
Efter at Datatilsynet havde accepteret, at der kunne tilknyttes et personnummer til OCES medarbejdercertifikater gennem en sammenhæng mellem certifikatløbenummer på medarbejdercertifikater (RID) og personnummer, rettede Sundhedsportalen henvendelse til Datatilsynet med henblik på afklaring af, om denne sammenhæng og den tilsvarende sammenhæng for personcertifikater (PID – CPR) kan opbevares hos Sundhedsportalen. Ved en lokal opbevaring af disse sammenhænge kan man undgå et opslag hos den certifikatudstedende myndighed, og det var Sundhedsportalens vurdering, at nødvendigheden af et sådant opslag vil udgøre en unødig stor risiko for systemets tilgængelighed for såvel borgere som sundhedsfaglige brugere.

Datatilsynet accepterede, at denne sammenhæng opbevares på betingelse af, at der iagttages visse sikkerhedsforanstaltninger, at sammenhængen kun anvendes i forbindelse med autorisationsprocedurer, og at behandlingen af oplysningen om personnummer sker under iagttagelse af persondataloven.

Udsendelse af e-post adresser

Udtalt, at en e-postadresse er en personoplysning omfattet af persondataloven, og at e-postadresser på modtagere af nyhedsbreve og lignende masseudsendelser ikke bør fremgå af sådanne meddelelser. Modtageradresser bør placeres i meddelelsens bcc-felt el. lign. (Datatilsynets j.nr. 2003-216-0142)

En borger gjorde Datatilsynet opmærksom på, at hans e-postadresse sammen med en lang række andre personers e-postadresser var blevet videregivet til samtlige modtagere af en humanitær organisations kampagneskrivelse.

Det var Datatilsynets opfattelse, at en e-postadresse er en personoplysning og derfor omfattet af persondataloven. Datatilsynet fandt, at e-postadresser

på modtagere af nyhedsbreve og lignende masseudsendelser ikke bør fremgå af sådanne meddelelser.

Organisationen oplyste, at videregivelsen af de i alt 672 e-postadresser til kampagneskrivelsens modtagere skyldtes, at man ved udsendelsen af pågældende e-post fejlagtigt ikke placerede modtageradresserne i meddelelsens bcc-felt[17].

For at undgå yderligere spredning af de videregivne e-postadresser fremsendte organisationen en undskyldning til de pågældende modtagere med en orientering om fejlen og en appel om, at man afstod fra videre spredning og slettede den fejlbehæftede e-post.

For at forhindre gentagelse af fejlen eller lignende fejl i fremtiden ville organisationen nedskrive den hidtidige mundtlige instruks i udbygget form med en klar understregning af de ansættelsesretlige konsekvenser af ikke at følge instruksen.

Endvidere ville organisationen iværksætte et egentligt program for at styrke datasikkerheden i organisationen. Programmet skulle tage udgangspunkt i en af ledelsen fastlagt IT-sikkerhedspolitik suppleret med instrukser og driftsregler samt et såkaldt awareness-program for samtlige relevante medarbejdere.

Datatilsynet noterede sig organisationens redegørelse.

Under henvisning til, at det havde været muligt at se andre modtageres e-postadresser i en masseudsendelse, var det Datatilsynets opfattelse, at persondatalovens § 41, stk. 3, ikke havde været overholdt.

Tilsynet fandt, at organisationen havde truffet de rigtige beslutninger som konsekvens af det passerede ved at beslutte at udsende en beklagelse til de berørte personer med anmodning om at slette de fejlagtigt udsendte e-postmeddelelser, ved uddybning og skriftlig indskærpelse af gældende regler samt ved gennemførsel af et program for styrkelse af datasikkerheden i organisationen.

[17] Bcc-feltet (eller Bc-feltet) benyttes i stedet for til- eller cc-feltet til angivelse af modtageradresser ved afsendelse af e-post i tilfælde af, at afsenderen ikke ønsker, at modtagere af en masseudsendelse skal kunne se hinandens e-postadresser og evt. navne i den udsendte postmeddelelse.


F5
F6
F7
F8
6
7
8
9
T
Y
U
I
O

Tilsynsvirksomhed

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 dog 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 omfat-

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

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

Gennemførelse af inspektioner

Inspektioner tager oftest udgangspunkt i de behandlinger, den dataansvarlige har anmeldt til Datatilsynet. De anmeldte behandlinger gennemgås, og behandlinger, som den dataansvarlige har vurderet ikke-anmeldelsespligtige, diskuteres.

Herefter gennemgås en række emner af generel karakter samt emner, som vurderes at være særlig relevante for den pågældende dataansvarlige. Eksempler på emner kan være

- Logning og sletning
- Oplysningspligt, indsigtsbegæringer og samkøring i kontroløjemed
- Billeder og andre informationer på internettet
- Videoovervågning
- Kontrol af medarbejderes brug af internet og e-post
- Elektronisk borgerbetjening og transmission af oplysninger via myndighedens hjemmeside
- Hjemmearbejdspladser og mobile arbejdspladser
- Trådløse netværk

Efter gennemgang af relevante emner gennemgås hos offentlige myndigheder de uddybende sikkerhedsregler, som myndigheden har fastsat i henhold til sikkerhedsbekendtgørelsens § 5, og som myndigheden forud for inspektionen har indsendt til Datatilsynet. Tilsynet tilkendegiver sit overordnede indtryk og eventuelle specifikke kommentarer til de uddybende regler. Herefter kan man eventuelt gå i en dybere dialog om enkelte emner og undersøge særlige forhold vedrørende driftsprocedurer, anvendelse af sikkerhedsforanstaltninger mv.

Før inspektionen afsluttes, foretages en besigtigelse af lokaler, hvor personoplysninger behandles. Herunder foretages diverse stikprøver i systemer, den fysiske indretning gennemgås, og der vil eventuelt blive gennemført min-

dre interviews af medarbejdere, som behandler personoplysninger eller administrerer edb-udstyr.

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.

Formidling af resultater af inspektioner

Datatilsynet formidler resultaterne af sine inspektioner ved i årsberetningen og på hjemmesiden at nævne, hvor inspektioner har været gennemført og den eventuelle kritik, som tilsynet har udtalt.

Som omtalt i årsberetningen for 2002, s. 99-100, offentliggjorde Datatilsynet i 2002 forsøgsvis resultatet af 28 inspektioner ved tildeling af karakterer på en skala fra 1 til 3. Forsøget medførte en del omtale af - og interesse for - inspektionerne, men da tildeling af karakterer også medvirker til at fjerne fokus fra formidlingen af det egentlige budskab om tilsynets observationer, har Datatilsynet besluttet, at der indtil videre ikke tildeles karakterer ved formidling af inspektionsresultater.

Datatilsynets observationer ved inspektioner i 2003

Ved planlægningen af Datatilsynets inspektioner i 2003 fandt tilsynet, at Lolland/Falster-området i forhold til landet som helhed havde haft et relativt lavt antal inspektioner siden persondatalovens ikrafttræden. Der blev derfor iværksat en målrettet indsats i denne region.

Indsatsen bestod i, at tilsynet udstationerede seks medarbejdere i området i tre dage. Der blev i løbet af de tre dage gennemført inspektioner i hovedparten af kommunerne i området, ved Sygehusledelsen for Storstrøms Amt, på et af amtets sygehuse, hos politikredsene i regionen samt ved et kontaktbureau – i alt blev der foretaget 17 inspektioner.

Datatilsynet gennemførte første gang denne form for målrettet indsats i et geografisk område i 2002, og efter at have benyttet denne form igen i 2003 er det fortsat tilsynets indtryk, at man ved i en periode at koncentrere sig om veldefinerede områder – her geografiske – kan opnå stor opmærksomhed omkring persondatalovens regler, tilsynets opgaver og datasikkerhed generelt.

I det følgende beskrives i store træk de observationer, som Datatilsynet har gjort i forbindelse med inspektionerne i 2003. Der er ikke foretaget en egentlig statistisk bearbejdning af inspektionsresultaterne, men beskrivelsen er egnet til at illustrere de generelle tendenser, som tilsynet har oplevet på inspektionerne.

Anmeldelser

Det overordnede indtryk efter inspektionerne afholdt i 2003 er fortsat, 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 synes i det hele taget at være god bevågenhed omkring persondatalovens regler.

Opfyldelse af logningskrav

Et problem, som tilsynet stødte på også i 2003, er offentlige myndigheders manglende opfyldelse af sikkerhedsbekendtgørelsens regler om logning af brug af fortrolige personoplysninger eller sletning af oplysningerne efter en vis kortere periode. Formålet med disse regler er dels at forebygge dels at 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.

Den manglende opfyldelse af logningskravet ses fortsat typisk, hvor der er sket opbygning af egentlige registre eller småsystemer, f.eks. journallignende systemer i tekstbehandlingsprogrammer, regneark eller primitive databasesystemer, hvori der behandles fortrolige eller følsomme personoplysninger. Som et eksempel på et sådant system kan fra politiets område nævnes, at der i nogle politikredse har været opbygget lokale systemer parallelt med politiets centrale sagsbehandlingssystem til visse former for efterforskning.

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. Ligeledes udtages stikprøver fra log-oplysninger med det formål at undersøge den tjenstlige baggrund for de udførte transaktioner. Disse stikprøver skal bl.a. ses som et supplement til den kontrol af systemernes anvendelse, som de dataansvarlige myndigheder forventes at foretage, jf. bestemmelserne i sikkerhedsbekendtgørelsens § 5, hvoraf det fremgår, at der skal fastsættes retningslinier for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

Oplysningspligt, indsigtsret og samkøring i kontroløjemed

De fleste offentlige myndigheder er opmærksomme på reglerne på disse områder. På det kommunale område ses der dog af og til eksempler på, at oplysningspligten opfyldes mere på grund af god skik og sædvane hos medarbejderne end på grund af formelt fastsatte regler og instrukser på området.

Tilsynet anbefaler derfor fortsat i en række tilfælde udarbejdelse eller gennemgang af instrukser og forretningsgange på området samt gennemgang af fortrykte tekster på blanketter mv., idet de registreredes rettigheder i vid udstrækning kan tilgodeses ved hensigtsmæssige tekster på blanketter, i pjecer osv. De dataansvarlige skal dog være særligt opmærksomme på opfyldelse af oplysningspligten for så vidt angår situationer, hvor oplysninger modtages fra 3. mand.

Særligt på sygehusområdet er der en tendens til, at oplysningspligten overses, om end der efterhånden er flere sygehuse, der har gjort et stort stykke arbejde for at opfylde oplysningspligten. Dette sker bl.a. ved brug af fortrykte pjecer, som udsendes sammen med indkaldelsesbreve mv., samt ved at personale ved modtagelse af patienter mundtligt orienterer om stedets behandling af personoplysninger - f.eks. den videregivelse af oplysninger, der sker til patientens egen læge.

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. Det er tilsynets indtryk, at kendskabet til reglerne for offentliggørelse af billeder på internettet generelt er blevet noget bedre siden 2002. Datatilsynets praksis vedrørende offentliggørelse af billeder på internettet er nærmere beskrevet i tilsynets årsberetning for 2002 på side 44 – 46.

Tv-overvågning

Datatilsynet støder i stigende omfang på brug af tv-overvågning, som har et kriminalpræventivt formål. Tilsynet påpeger i nogle tilfælde mangelfuld skiltning ved tv-overvågning, og der ses eksempler på, at den dataansvarlige ikke har været opmærksom på at foretage anmeldelse i de tilfælde, hvor overvågningen er anmeldelsespligtig. Datatilsynets praksis på området er nærmere omtalt under "Sager om behandling af personoplysninger".

Elektronisk borgerbetjening

Datatilsynet kræver, 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.

De dataansvarlige er tilsyneladende generelt opmærksomme på reglerne for transmission af personoplysninger over internettet. Reglerne fremgår af værd-at-vide-tekster på Datatilsynets hjemmeside, og tilsynet besvarer en del spørgsmål på området. En medvirkende årsag til det gode kendskab til reglerne kan også være den information, der blev udsendt vedrørende eDag, hvor det blev fremhævet, at myndigheders udveksling af fortrolige personoplysninger ikke er omfattet af det generelle krav om elektronisk udveksling af information mellem myndigheder.

Hjemmearbejdspladser og mobilt udstyr

Hjemmearbejdspladser og mobilt computerudstyr bliver anvendt i stigende omfang, og 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 hjemmearbejdspladser/mobilt udstyr og myndighedens systemer, sikring af data, der opbevares på hjemmearbejdspladser og mobilt udstyr, vedligeholdelse af antivirusprogrammel, regler for anden brug af udstyret 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 og andet udstyr uden for den dataansvarliges lokaliteter, er nærmere beskrevet i Datatilsynets vejledning til sikkerhedsbekendtgørelsen.

Trådløse netværk

Det er Datatilsynets indtryk, at trådløse netværk endnu ikke er særlig udbredte hos offentlige myndigheder. Der har været en del omtale i bl.a. pressen af de sikkerhedsproblemer, som knytter sig til trådløse netværk, hvilket har medført, at der generelt er en god bevidsthed om disse forhold hos de dataansvarlige.

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. Man bør bl.a. i denne forbindelse være særlig opmærksom på, om der kan etableres en tilstrækkelig stærk kryptering af den trådløse trafik.

Uddybende sikkerhedsregler

Ved tilsynets inspektioner viser det sig typisk, at de dataansvarlige følger god praksis i forhold til IT-sikkerhed. Tilsynet har dog også i 2003 i flere tilfælde konstateret manglende, mangelfulde eller forældede uddybende sikkerhedsregler hos offentlige myndigheder.

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, arbejdsgange osv.

Besigtigelse af fysisk sikkerhed

I Datatilsynets inspektioner indgår oftest en besigtigelse af publikumsområder, serverrum og arkiver, hvor der behandles eller opbevares personoplysninger.

Der synes at være en tendens til, at printere og fax-maskiner i højere grad end tidligere opstilles på en måde, der gør det svært for uvedkommende at læse eller tilegne sig udskrifter med personoplysninger.

Ved besigtigelse af serverrum undersøger Datatilsynet forhold vedrørende fysisk adgang, sikring mod brand- og vandskader, forsyningssikkerhed mv.

Der ses en del eksempler på serverrum, som er præget af omtanke ved indretningen og med god orden i rummet. Dog ses der også eksempler på, at serverrum ikke er låst i dagtimerne, så uvedkommende har uhindret adgang. Det er heller ikke ualmindeligt at se, at serverrum benyttes til opbevaring af materialer, som er den daglige drift uvedkommende. Det kan f.eks. dreje sig om nyt endnu ikke ibrugtaget udstyr, udrangeret edb-udstyr, tom emballage og forskellige forbrugsartikler. Ved en brand i et serverrum kan oplagring af brandbart materiale medføre, at skaderne efter branden bliver langt større, end de ellers ville være blevet. Datatilsynets generelle anbefaling er derfor, at lokaler med centralt edb-udstyr altid holdes aflåst, når de ikke er bemandede, at kredsen af personer med adgang til sådanne lokaler er så lille som mulig, at der alene opbevares materialer og andet udstyr, som er absolut nødvendigt for den daglige drift, og at tobaksrygning er forbudt i sådanne lokaler.

Inspektioner hos politiet

Som det fremgår af oversigten på side 104 i årsberetningen fra 2002, gennemførte Datatilsynet i 2002 inspektioner i en række politikredse.

Datatilsynet konstaterede i den forbindelse, at kravene i persondataloven og regler udstedt i medfør heraf i en række tilfælde ikke blev overholdt. Det gjaldt navnlig reglerne i sikkerhedsbekendtgørelsen om logning.

Inspektionerne gav anledning til, at Datatilsynet i 2003 orienterede Rigspolitichefen om de konstaterede problemer med manglende sletning af tekstbehandlingsdokumenter, og der henvistes særligt til inspektionerne i en række kredse, hvor Datatilsynet havde konstateret, at der enten aktuelt på tidspunktet for tilsynets inspektion eller tidligere var blevet behandlet oplysninger fra telefonaflytninger i edb-registre, uden at anvendelsen heraf kunne logges i overensstemmelse med sikkerhedsbekendtgørelsens § 19, stk. 1.

Flere kredse havde således under drøftelser med Datatilsynet peget på, at fravælgelsen af de kendte systemer i POLSAS (Politiets sagsbehandlingssystem) til håndtering af telefonaflytninger var sket for at imødegå tab af oplysninger, idet der kunne være problemer af teknisk art forbundet med anvendelsen af POLSAS til håndtering af dokumenter med meget store mængder af oplysninger, hvilket ofte er tilfældet i telefonaflytningssager.

Datatilsynet udtalte, at der syntes at være tale om et generelt problem med håndtering af oplysninger indsamlet i forbindelse med telefonaflytning, og pegede på behovet for at iværksætte foranstaltninger, som sikrer den fornødne databeskyttelse i forbindelse med udførelsen af disse opgaver.

Rigspolitichefen har efterfølgende underrettet Datatilsynet om, at Rigspolitichefens Dataafdeling for tiden søger at udarbejde en løsning på de konstaterede problemer.

Oversigt over udførte inspektioner i 2003

På nedenstående oversigt er der indsat markeringen **"i"** ved de inspektioner, som har givet Datatilsynet anledning til at underrette kommunalbestyrelsen/amtsrådet eller en overordnet myndighed om resultatet af Datatilsynets inspektioner. Enkelte inspektionssager er endnu ikke færdigbehandlet.

Staten

Danmarks Nationalbank
Erhvervs- og Boligstyrelsen
Miljø- og Energiministeriet
Politimesteren i Nakskov
Politimesteren i Nykøbing-Falster
Politimesteren i Vordingborg
Politimesteren i Køge
Forsvarets Sundhedstjeneste
Rigsarkivet
Rigspolitichefen, N-SIS
Kirkeministeriets departement
Skatteministeriets departement
Forsvarsministeriets departement
Beskæftigelsesministeriets departement
Fødevareministeriets departement

Kommuner og amter

Holeby Kommune
Højreby Kommune
Københavns Amts specialundervisningskontor
Møn Kommune
Nakskov Kommune
Nykøbing F. Kommune
Nysted Kommune
i Nørre Alslev Kommune
Ravnsborg Kommune
Rudbjerg Kommune
Rødby Kommune
Sakskøbing Kommune
Storstrøms Amt, herunder et sygehus
Stubbekøbing Kommune
Sydfalster Kommune
Hadsten Kommune
Langå Kommune
Lundtoft Kommune
Tinglev Kommune
i Græsted-Gilleleje Kommune

Offentlige sygehuse

Hvidovre Hospital
Skejby Sygehus
Statshospitalet i Vordingborg
i Odense Universitetshospital
Centralsygehuset i Næstved

Private forskere

Astra Zeneca, generel tilladelse
Hans Bisgaard, Astra Zeneca
Flemming Madsen, Astra Zeneca
Lundbeck, generel tilladelse
Henrik Lublin, Lundbeck
Coloplast, Kontinensafdelingen
Christina Gunnergaard, Coloplast
Anders Kjær, Rigshospitalet
Kamran Akram, Steno Diabetes Center
Christian Stjer, Catinet
Peter Gimsing, Rigshospitalet
Torben Jørgensen, Center for Sygdoms-
forebyggelse, Amtssygehuset i Glostrup
Lene Mellemkjær, Kræftens Bekæmpelse
Mads Melbye, Statens Serum Institut
Anders Koch, Statens Serum Institut
Henrik Hjalgrim, Statens Serum Institut
Lone Graff Stensballe, Statens Serum Institut
Boehringer Ingelheim Danmark A/S
Nete Munk Nielsen, Statens Serum Institut

Øvrige private

Accept Finans A/S
Almindelig Brand forsikring
Antipiratgruppen
COOP Danmark A/S
Kontaktbureau Symbirosen
Magasin du Nord A/S
Personaleservice A/S
PKI A/S
Sygesikringen danmark
RKI
Temp-team
Din vikar