Datatilsynets årsberetning 2004

DATATILSYNET

Datatilsynets årsberetning 2004

Udgiver: Datatilsynet
Tryk og layout: Schultz Grafisk
Beretningen er sat med Meta
Oplag: 400
December 2005
ISSN nr: 1601-5657
ISBN nr: 87-989860-2-3

Indhold

Til Folketinget

Hermed afgiver Datatilsynet sin årsberetning for 2004.

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 2004 og gengiver Datatilsynets udtalelser til nogle af de lovforslag mv., som tilsynet har fået i høring i 2004.

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.

Siden afgivelsen af sidste årsberetning er Datatilsynet begyndt løbende at offentliggøre udtalelser og afgørelser i sager, som vurderes at være af generel interesse, på tilsynets hjemmeside www.datatilsynet.dk. Denne årsberetning indeholder derfor ikke referater af konkrete sager om behandling af personoplysninger.

Ved løbende offentliggørelse af udtalelser og afgørelser på tilsynets hjemmeside, hvor det bl.a. er muligt at foretage søgninger og at tilmelde sig en elektronisk abonnementsordning, håber Datatilsynet at sikre en effektiv og tidssvarende formidling af information om persondataloven og tilsynets virksomhed.

København, november 2005

Asbjørn Jensen
Formand for Datarådet

Janni Christoffersen
Direktør

Datatilsynets virksomhed i 2004

Datatilsynets opgaver

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

Blandt Datatilsynets forskellige aktiviteter i 2004 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.
- Strukturreformen
- 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
- Indsats over for virksomheder, der yder erhvervsmæssig bistand ved stillingsbesættelse
- Afholdelse af jubilæumskonference
- Afholdelse af konference om pervasive computing (it i alting) i samarbejde med Rådet for IT-sikkerhed
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsynsmyndigheder
- Afholdelse af Nordisk Datachefmøde

• Deltagelse i arbejdsgrupper, udvalg o.l.

Datatilsynet har i 2004 registreret 4.441 nye sager, hvilket er en betydelig stigning i forhold til 2003, hvor der blev registreret 3.521 nye sager. De forskellige kategorier af sager fremgår af oversigten i afsnittet "Statistiske oplysninger". De væsentligste stigninger i antallet af nye sager ses i kategorierne lovforberedende arbejde, forespørgsler og klager vedrørende private dataansvarlige samt anmeldelser.

Rådgivning og vejledning

Tilsynet yder råd og vejledning om persondataloven til myndigheder og virksomheder. Det er tilsynets erfaring, at det ofte er en god ide, at tilsynet inddrages 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 personoplysningerne.

Et vigtigt område for rådgivning og vejledning i 2004 har været digital forvaltning og forberedelserne til den kommende strukturreform, jf. nærmere nedenfor.

Klagesagsbehandling

I klagesagerne træffer Datatilsynet egentlige afgørelser om, hvorvidt en behandling er i overensstemmelse med loven. Det er selvsagt af afgørende betydning, at borgere, der mener sig udsat for behandling af oplysninger i strid med loven, eller som f.eks. ikke får de oplysninger, de mener at have 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 i 2004 registeret en relativt stor stigning i antallet af nye sager (klager og forespørgsler) vedrørende private dataansvarlige (fra 415 i 2003 til 571 i 2004), mens niveauet er faldet i forhold til offentlige myndigheder (fra 495 i 2003 til 394 i 2004).

Ud over de henvendelser, der bliver registreret som nye sager, modtager Datatilsynet et meget stort antal telefoniske henvendelser. De telefoniske henvendelser er bl.a. fra borgere, der vil høre om deres rettigheder som registrerede, men også

myndigheder og virksomheder efterspørger telefonisk vejledning for eksempel om, hvorvidt påtænkte projekter rejser persondataretlige problemstillinger. Det er tilsynets opfattelse, at telefonvejledningen er en vigtig del af tilsynets arbejde, som hjælper alle parter til at undgå problemer senere. Der er i sagens natur også telefoniske henvendelser, som ikke kan klares her og nu, men kræver opfølgende sagsbehandling.

Datatilsynet har siden midten af 2004 forsøgsvis gennemført kvartalsmæssige stikprøvetællinger af antallet af telefoniske henvendelser til tilsynet. Baseret på optællingerne anslås antallet af telefoniske henvendelser til tilsynet at ligge på ca. 17.000 i 2004.

Høring over lovforslag mv.

Datatilsynet skal efter persondataloven 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.

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 har igennem de senere år oplevet et stadigt stigende antal sager i denne kategori. I 2004 steg antallet imidlertid markant, idet tilsynet registrerede 226 nye sager i denne kategori, hvilket er mere end dobbelt så mange som i 2003, hvor der blev registreret 109 sager.

Generelt må Datatilsynet konstatere, at en del af de lovforslag, som tilsynet får i høring, rejser vanskelige spørgsmål om forholdet mellem på den ene side de ønskede nye regler og på den anden side reglerne i persondataloven og databeskyttelsesdirektivet.

I en del tilfælde foreslås regler, som indebærer en behandling af personoplysninger, der ikke umiddelbart kan ske inden for rammerne af persondataloven. Gennemførslen kræver således, at der i særlovgivningen sker en fravigelse af persondataloven. I sådanne tilfælde gør tilsynet i sine høringssvar opmærksom på problemerne i forhold til persondataloven og anbefaler, at det tydeliggøres i lovforslaget, hvorvidt der er tale om en fravigelse af persondataloven, herunder om en sådan fravigelse kan ske inden for rammerne af databeskyttelsesdirektivet. Datatilsynet giver i den forbindelse normalt udtryk for, at en særskilt hjem-

mel til behandling af personoplysninger i videre omfang end, hvad der følger af persondataloven, kun bør tilvejebringes, hvis vægtige samfundsmæssige hensyn taler derfor. Om der konkret er så vægtige offentlige hensyn, der gør det nødvendigt at fravige det generelle beskyttelsesniveau, som lovgivningsmagten har fastlagt med persondataloven, beror i sidste instans på en politisk vurdering, som må udøves af Folketinget selv. På den baggrund undlader tilsynet i sådanne tilfælde ofte at udtale sig om, en sådan fravigelse bør gennemføres.

Datatilsynet ser det imidlertid som en uheldig udvikling, hvis der i betydeligt omfang vedtages regler mv., der giver en dårligere retsstilling for de registrerede end den beskyttelse, som følger af persondatalovens generelle regler. En sådan udvikling bidrager samtidig til at gøre retstilstanden kompleks og uigennemsigtig for borgere, myndigheder og virksomheder.

Strukturreformen

Som nævnt har Datatilsynet i 2004 beskæftiget sig en del med den kommende strukturreform.

I begyndelsen af året fik Datatilsynet Strukturkommissionens betænkning nr. 1434/2004 i høring, og efterfølgende har Datatilsynet udtalt sig om en række af de lovgivningsmæssige initiativer, som strukturreformen har givet anledning til. Af de 226 nye sager registreret i 2004 i kategorien lovforberedende arbejde er de 36 sager registreret i forbindelse med den høring over lovforslag, der som et led i reformen fandt sted i december 2004. Datatilsynets udtalelser om Strukturkommissionens betænkning og nogle af de lovforslag, der er et led i udmøntningen af reformen, er gengivet i afsnittet "Udtalelser over lovforslag mv.".

Udover afgivelse af høringssvar har Datatilsynet i forbindelse med udarbejdelsen og udmøntningen af lovforslagene og en række andre projekter, der direkte eller indirekte har haft tilknytning til strukturreformen, ydet rådgivning og vejledning til de involverede myndigheder. I den forbindelse kan bl.a. nævnes etableringen af kommunale borgerservicecentre, skattecentre og jobcentre.

Særligt vedrørende etableringen af kommunale borgerservicecentre har Datatilsynet tilkendegivet at ville bidrage ved udarbejdelsen af den vejledning, som Indenrigs- og Sundhedsministeriet og KL står for. Datatilsynet har i den anledning bl.a. aflagt besøg hos to borgerservicecentre med henblik på at få større indsigt i den praktiske tilrettelæggelse af centrenes virksomhed.

Herudover har Datatilsynet deltaget i en række møder, konferencer, arbejdsgrupper og workshops, som har behandlet forskellige aspekter af strukturreformen.

Sager på eget initiativ

Datatilsynet har i 2004 registreret 110 sager rejst på tilsynets eget initiativ. Dette svarer til niveauet i 2003, hvor der blev rejst 114 sager på tilsynets eget initiativ. Sagerne omfatter såvel inspektioner som andre "egen drift-sager".

I 2004 har Datatilsynet gennemført 68 inspektioner, heraf 41 hos offentlige myndigheder og 27 hos forskellige private virksomheder. Dette svarer ligeledes til niveauet i 2003. I 2002 blev der gennemført i alt 116 inspektioner. Nedgangen i antallet af inspektioner er en følge af dels de pålagte besparelser dels en meget væsentlig forøgelse af sagsantallet på tilsynets andre arbejdsområder.

Datatilsynet har igen i 2004 gennemført en inspektionsrunde i et afgrænset geografisk område – denne gang i området omkring Salling og Mors. Inspektionerne gennemførtes over en periode på 4 dage, hvor 6 af tilsynets medarbejdere var udstationerede i området. Det er Datatilsynets opfattelse, at denne form for koncentreret indsats i områder, der typisk ligger uden for hovedstadsområdet, er effektiv og ressourcebesparende, idet der kan gennemføres et stort antal inspektioner på kort tid, samtidig bidrager en sådan målrettet indsats til en øget fokus på persondatalovens regler og tilsynets opgaver i det pågældende område. Datatilsynets inspektioner er nærmere beskrevet i afsnittet "Tilsynsvirksomhed".

Ud over en koncentreret indsats i afgrænsede geografiske områder tager Datatilsynet også løbende initiativer mod indholdsmæssigt afgrænsede områder. I 2004 har Datatilsynet særligt koncentreret sig om virksomheder, der yder erhvervsmæssig bistand ved stillingsbesættelse. Baggrunden for denne indsats var pressens omtale af såkaldte "headhunter-firmaer", der ikke havde Datatilsynets tilladelse. Datatilsynet kunne konstatere, at antallet af anmeldelser på dette område var lavt, og tilsynet besluttede derfor at gennemføre en målrettet kampagne i forhold til stillingsbesættende virksomheder, således at persondatalovens krav om anmeldelse og tilladelse til denne type virksomhed overholdes.

Datatilsynet tog kontakt til Dansk Management Råd, der herefter udsendte et nyhedsbrev til sine medlemmer om persondataloven. Herudover skrev Datatilsynet på baggrund af registreringer i Krak.dk direkte til over 300 virksomheder. Henvendelsen til virksomhederne indeholdt en kort beskrivelse af persondatalovens regler og en anmodning om, at virksomheden foretog anmeldelse til Datatilsynet, såfremt virksomheden drev stillingsbesættende virksomhed.

Indsatsen resulterede bl.a. i, at Datatilsynet ved udgangen af 2004 havde modtaget knap 250 anmeldelser fra stillingsbesættende virksomheder. Ud over at gennemgå anmeldelserne og meddele tilladelser brugte Datatilsynet i den forbindelse også end del ressourcer på at vejlede virksomhederne om persona-

talovens regler, herunder særligt om reglerne om samtykke fra de registrerede og om kravene til sletning af oplysninger.

Det er overordnet set Datatilsynets vurdering, at de manglende anmeldelser som oftest skyldes ukendskab til persondatalovens regler, og et væsentligt formål med en sådan målrettet indsats er derfor at få skabt opmærksomhed omkring reglerne i den pågældende branche. Et afledt resultat af indsatsen har således også været, at Datatilsynet har modtaget et stigende antal anmeldelser fra virksomheder i "tilstødende" brancher, eksempelvis vikarbureauer, der behandler følsomme oplysninger i forbindelse med eksempelvis personlighedstest.

Det er ofte på baggrund af henvendelser fra pressen, at Datatilsynet tager sager op til nærmere undersøgelse. Fra 2004 kan nævnes en henvendelse, som gjorde Datatilsynet opmærksom på en hjemmeside indeholdende et billedgalleri, der indeholdt fotos af nøgne personer og personer samt en ledsagende tekst. Teksten og en række af de viste fotos gav indtryk af, at de pågældende fotos var taget og offentliggjort på internettet uden de fotograferede personers samtykke – og formentlig uden deres vidende.

Datatilsynets umiddelbare vurdering var, at der var tale om en overtrædelse af persondataloven, eventuelt også af straffeloven, og tilsynet valgte derfor øjeblikkeligt at påbyde den dataansvarlige at ophøre med offentliggørelse af de fotos af genkendelige personer, der fandtes i billedgalleriet på hjemmesiden, hvis der ikke forelå et udtrykkeligt samtykke til offentliggørelsen. Den ansvarlige for hjemmesiden efterkom Datatilsynets påbud. Henset til karakteren af de offentliggjorte oplysninger foretog Datatilsynet tillige politianmeldelse i sagen.

Anmeldelser

Datatilsynet har også i 2004 behandlet mange anmeldelser og ansøgninger om tilladelser. Der er således registreret i alt 2.616 nye anmeldelser, hvilket er en stigning i forhold til 2003, hvor der blev registreret i alt 1.970 nye anmeldelser.

Det er første gang siden 2001, der var det første hele kalenderår efter, at persondatalovens trådte i kraft, at der er registeret en stigning i antallet af anmeldelser vedrørende offentlige myndigheder. Der er i denne kategori i 2004 registreret 1.191 nye anmeldelser mod 743 i 2003.

Der er ligeledes sket en stigning i anmeldelserne fra private dataansvarlige, hvor der i 2004 er registreret 1.425 nye anmeldelser mod 1.227 i 2003. Stigningen i antallet af anmeldelser fra private kan formentlig i vidt omfang tilskrives den indsats, som Datatilsynet i 2004 gennemførte mod de såkaldte "headhunter-firmaer", jf. ovenfor.

Herudover sker der løbende ændringer i de anmeldelser, som allerede er modtaget. Det gælder ikke mindst på forsknings- og statistikområdet, hvor Datatilsynet i 2004 har modtaget ca. 800 ændringer til eksisterende anmeldelser, 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.

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

Tv-overvågning

I løbet af de seneste år – og også i 2004 – har Datatilsynet behandlet en del sager om tv-overvågning. Der har været tale om sager vedrørende såvel den private som den offentlige sektor. Datatilsynet er i den forbindelse stødt på en række problemstillinger, dels i samspillet mellem persondataloven og lov om forbud mod tv-overvågning, dels i forhold til persondatalovens anvendelse på tv-overvågning. Det er derfor Datatilsynets opfattelse, at de nævnte problemstillinger sammenholdt med, at der fra både privat og offentlig sektor kan konstateres en stadig stigende interesse for at anvende tv-overvågning, navnlig i kriminalpræventivt øjemed, aktualiserer behovet for en samlet gennemgang af og stillingtagen til reguleringen på området.

I 2004 udarbejdede Datatilsynet derfor en redegørelse til Justitsministeriet, hvori tilsynet pegede på en række konkrete problemstillinger i relation til tv-overvågning. Redegørelsen og henvendelsen af 13. september 2004 til Justitsministeriet kan ses på Datatilsynets hjemmeside under punktet "Nyheder".

På baggrund af Datatilsynets henvendelse samt en henvendelse fra Finansrådet og Finansforbundet, hvori der blev fremsat ønske om, at der åbnes mulighed for at anvende tv-overvågning med billedoptagelse af pengeinstitutters facadearealer, har Justitsministeriet nedsat et udvalg om tv-overvågning. Udvalget, hvori Datatilsynet er repræsenteret, skal overveje spørgsmålet om en udvidelse af adgangen til tv-overvågning og overveje samspillet mellem tv-overvågningsloven og persondataloven samt de øvrige problemstillinger, som Datatilsynet har peget på. Udvalgets kommissorium og sammensætning er offentliggjort på Justitsministeriets hjemmeside www.jm.dk.

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. Aktiviteterne i de fælles tilsynsmyndigheder omtales nærmere i afsnittet om internationale sager.

Datatilsynet deltager endvidere i det nordiske samarbejde vedrørende persondatabeskyttelse, og Danmark var i 2004 vært for det Nordiske Datachefmøde. Hovedformålet med mødet er at udveksle erfaringer og synspunkter i forhold til de nordiske tilsyns indsats og praksis på databeskyttelsesområdet og at styrke samarbejdet mellem myndighederne.

Andre opgaver

Datatilsynet har 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.

Jubilæumskonference

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. Datatilsynet markerede dette med en stor jubilæumskonference, der blev afholdt den 5. februar 2004 i Landstingssalen på Christiansborg.

Konferencen, der blev åbnet af justitsminister Lene Espersen, er omtalt i årsberetningen for 2003.

Konference om pervasive computing (it i alting)

Rådet for it-sikkerhed og Datatilsynet afholdt den 24. november 2004 en offentlig høring om sikkerhedsaspekter i forbindelse med pervasive computing.

Pervasive computing er baseret på anvendelse af RFID-chips. En RFID-chip er et lille elektronisk lagringsmedium, som kan aflæses på afstand ved hjælp af radio-

bølger. I sin simpleste form kan en RFID-chip erstatte en stregkode og indeholder da en produktkode (svarende til en stregkode) suppleret med en entydig identifikation af et bestemt eksemplar af det givne produkt.

RFID-chips er ganske små og kan benyttes til mærkning af alle typer produkter, herunder almindelig dagligvarer og beklædningsgenstande.

Mere avancerede typer af RFID-chips kan indeholde større datamængder, f.eks. et digitalt foto eller fingeraftryk. RFID-chips kan f.eks. også være forsynet med sensorer til registrering af temperatur e.lign.

Høringens formål var at drøfte de it-sikkerhedsmæssige aspekter ved pervasive computing med henblik på at foreslå nærmere rammer for udviklingen. Det blev endvidere drøftet, om det er muligt og hensigtsmæssigt allerede nu at etablere branchekodeks for virksomheders udvikling og brug af pervasive computing i forhold til bl.a. privacy-spørgsmål.

Yderligere oplysninger om høringen kan ses på Rådet for it-sikkerheds hjemmeside www.rfits.dk.

Folketingsdebat om Datatilsynets ressourcer

Folketinget behandlede den 18. november 2004 en forespørgsel (F 11) fra SF og Enhedslisten til justitsministeren om Datatilsynets ressourcer og opgaver. Overskriften var: »Hvad vil regeringen gøre, for at Datatilsynets ressourcer kommer til at svare til de opgaver, Datatilsynet har og løbende får tildelt, herunder de stærkt øgede opgaver i forbindelse med strukturreformen?«

Justitsministeren oplyste under forhandlingerne, at hun havde besluttet midlertidigt at tilføre Datatilsynet yderligere ressourcer til bl.a. en personalemæssig styrkelse. Det skete med henblik på, at tilsynet kan løfte den merbelastning, der bl.a. er en følge af strukturreformen og indførelsen af nye it-systemer. Den midlertidige styrkelse var et beløb på 1,5 mio. kr., som blev optaget på tillægsbevillingen for 2004.

Debatten findes på Folketingets hjemmeside, og på Datatilsynets hjemmeside er tilsynets udtalelse af 26. januar 2004 til Justitsministeriet om bl.a., hvilke opgaver Datatilsynet har fået tildelt i de sidste 10 år, offentliggjort.

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 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 2004

Formand, højesteretsdommer Asbjørn Jensen
Næstformand, advokat Janne Glæsel
Professor, dr. jur. Peter Blume
Direktør Jakob Lyngsø
Overlæge Hans Henrik Storm
Direktør Rasmus Kjeldahl
Kommunaldirektør Estrid Oxlund

Medlemmerne beskikkes for 4 år ad gangen, og de er personligt udpeget i kraft af deres sagkundskab inden for bestemte sagsområder og er ikke repræsentanter for bestemte interesseorganisationer eller lignende.

Ved udgangen af beskikkelsesperioden 1. juli 2000 til 30. juni 2004 forlod højesteretsdommer Hugo Wendler Pedersen – efter 13½ år som formand – Datarådet. Fhv. formand for forbrugerrådet Kirsten Nielsen og rådmand Birgit Ekstrøm forlod endvidere Datarådet.

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.

Ansatte i sekretariatet

Pr. 31. december 2004

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. Anders Ankerstjerne
Fuldmægtig, cand.jur. Tine Asmussen
Fuldmægtig, cand.jur. Maiken Christensen Breüner (orlov)
Fuldmægtig, cand.jur. Kira Kolby Christensen (orlov)
Fuldmægtig, cand.jur. Stine Dyhr
Fuldmægtig, cand.jur. Camilla Sonne Kristensen
Fuldmægtig, cand.jur. Henriette Vincens Nielsen
Fuldmægtig, cand.jur. Thomas Gønge Pedersen
Fuldmægtig, cand.jur. Jakob Gøtze Pedersen
Fuldmægtig, cand.jur. Anne Broberg Rasmussen
Fuldmægtig, cand.jur. Frederik Siegumfeldt
Fuldmægtig, cand.jur. Mia Romanko Staal
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. Tina Wesselhoff Davidsen
Stud.jur. Marie-Louise Ehmer
Stud.jur. Marie Gjesing Fynsk
Stud.jur. Karina Kok Jørgensen

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 2004 løbende udarbejdet nye tekster og informationsmateriale, som er offentliggjort på hjemmesiden. Som noget nyt har Datatilsynet i 2004 i videre omfang end hidtil offentliggjort tilsynets udtalelser og afgørelser i sager, der vurderes at være af generel interesse. Tilsynet har i første omgang offentliggjort udvalgte udtalelser og afgørelser for perioden 2000 – 2004, men det er hensigten, at offentliggørelsen af navnlig sager, som har været behandlet i Datarådet, fremover vil ske løbende.

Enhver kan – gratis – tegne elektronisk abonnement på Datatilsynets hjemmeside. Abonnenterne modtager automatisk en e-post, når hjemmesiden opdateres. Ved udgangen af december 2004 var der i alt ca. 3.620 abonnenter på Datatilsynets hjemmeside mod 3.170 abonnenter i 2003 og 2.700 i 2002.

Statistiske oplysninger

Oplysningerne i dette afsnit er baseret på registreringerne af nye sager i tilsynets journalsystem i 2004. 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 2004 har modtaget ca. 800 ændringer til eksisterende anmeldelser af private forsknings- og statistikprojekter.

Datatilsynet registrerede 4.441 nye sager i perioden 1. januar 2004 til 31. december 2004. Disse sager fordeler sig som følger:

Datatilsynets egen administration mv.	313
Lovforberedende arbejde	226
Forespørgsler og klager vedrørende private	571
Forespørgsler og klager vedrørende offentlige myndigheder	394
Anmeldelser for den private sektor	1.425
Anmeldelser for den offentlige forvaltning	1.191
Sager på Datatilsynets eget initiativ	110
Sikkerhedsspørgsmål	26
Internationale sager	168
Kompetence i henhold til anden lovgivning	17

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

Forespørgsler og klager vedrørende private
Datatilsynet registrerede i alt 571 sager med forespørgsler og klager vedrørende private dataansvarlige.

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

Klager	ca. 22 %
Forespørgsler	ca. 78 %

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	73
Den finansielle sektor	36
Fagforeninger, a-kasser, pensionskasser mv.	26
Telesektoren	72
Foreninger og organisationer	69
Sundhedssektoren (medicinalvirksomheder, klinikker, læger mv.)	17
Kreditoplysningsbureauer	97
Advarselsregistre	15
Stillingsbesættende virksomheder	8
Ansøgninger om tilladelser	59
Diverse	99
Sager af generel karakter	0

Forespørgsler og klager vedrørende offentlige myndigheder
Datatilsynet registrerede i alt 394 sager med forespørgsler og klager vedrørende offentlige myndigheder.

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

Klager	ca. 8 %
Forespørgsler	ca. 92 %

I de afsluttede sager var ca. 30 % af klagerne berettigede, mens resten var uberettigede.

Sagerne var fordelt således:

Statslige myndigheder	147
Amtskommuner	23
Kommuner	113
Ansøgning om tilladelser	98
Diverse	13
Sager af generel karakter	0

Anmeldelser for den private sektor

Datatilsynet registrerede i alt 1.425 sager om anmeldelser. Fordelingen af sagerne var følgende:

Forskning og statistik	1.136
Privates behandling af oplysninger om rent private forhold	134
Advarselsregistre	6
Spærrelister	6
Kreditoplysningsbureauer	4
Stillingsbesættende virksomheder	115
Edb-servicebureauer	24
Diverse sager af generel karakter	0

Anmeldelser for den offentlige forvaltning

Datatilsynet registrerede i alt 1.191 sager om anmeldelser. Fordelingen af sagerne var følgende:

Fællesanmeldelser	11
Kommuner	393
Amtskommuner	174
Statslige myndigheder	247
Tilslutninger til fællesanmeldelser fra kommuner	255
Tilslutninger til fællesanmeldelser fra amtskommuner	0
Tilslutninger til fællesanmeldelser fra statslige myndigheder	111
Diverse/sager af generel karakter	0

Sager på Datatilsynets eget initiativ
Datatilsynet registrerede i alt 110 sager oprettet på tilsynets eget initiativ. Sagerne var fordelt på følgende sagstyper:

Inspektion og kontrol vedrørende private	38
Inspektion og kontrol vedrørende offentlige myndigheder	42
Sager rejst på grundlag af presseomtale o.l.	29
Diverse/sager af generel karakter	1

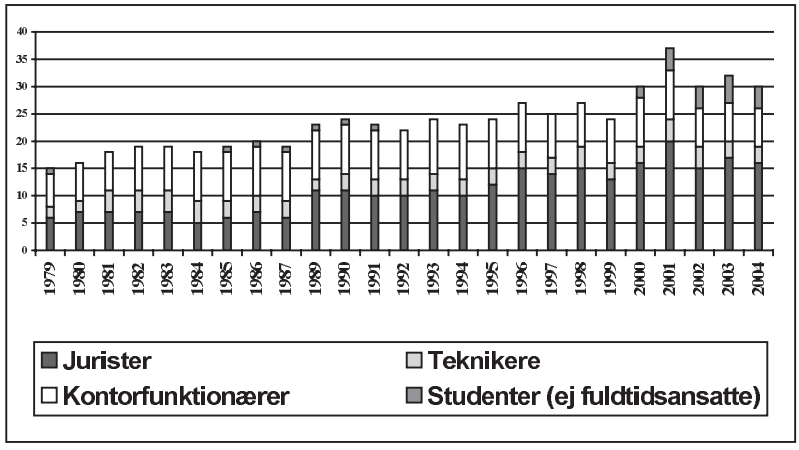
Sikkerhedsspørgsmål
Datatilsynet registrerede i alt 26 sager under kategorien sikkerhedsspørgsmål. Fordelingen af sagerne var følgende:

Sager vedrørende private	8
Sager vedrørende offentlige myndigheder	18

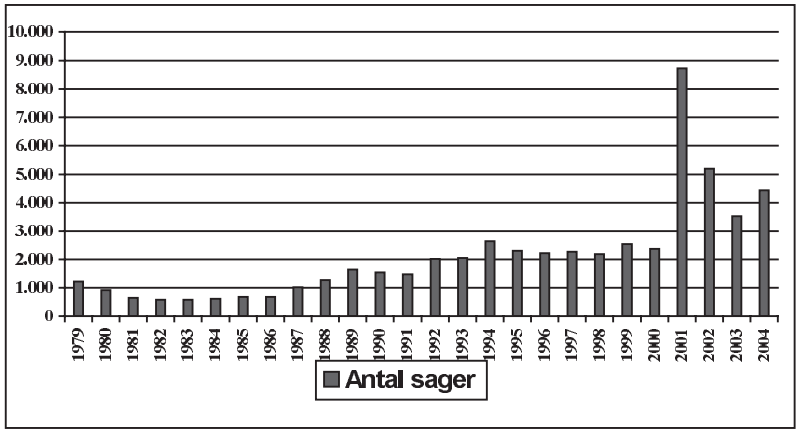
Internationale sager
Datatilsynet registrerede i alt 168 internationale sager. Fordelingen af sagerne var følgende:

Forespørgsler fra udlandet om dansk lovgivning	57
Nordisk tilsynssamarbejde	5
Europarådet	6
EU	48
Konventioner	36
Datakommissærsamarbejdet	11
OECD	0
Diverse/sager af generel karakter	5

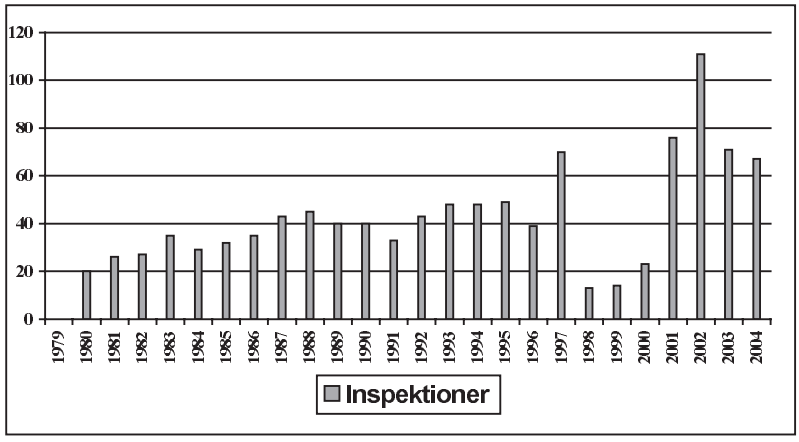
Fordelingen af de forskellige personalegrupper hen over årene



Antal sager



Antal inspektioner



Udtalelser over lovforslag mv.

Strukturkommissionens betænkning nr. 1434/2004

Indenrigs- og Sundhedsministeriet anmodede om Datatilsynets bemærkninger til Strukturkommissionens betænkning nr. 1434/2004.

Datatilsynets udtalelse, som blev afgivet efter behandling i Dataråd et, gengives i alt væsentligt nedenfor.

1. Den offentlige sektors struktur

1.1. Det fremgik af betænkningen, at kommissionen bl.a. vurderede, at der er behov for en reform af den offentlige sektors struktur. Dette begrundedes i en række identificerede svagheder ved den nuværende indretning af den offentlige sektor – og ikke mindst forventningen om, at fremtidige udfordringer vil forværre disse svagheder.

På den baggrund anbefalede kommissionen bl.a., at der gennemføres en samlet reform af den offentlige sektor, som omfatter såvel inddelingsændringer som opgaveflytninger mellem stat, amter og kommuner. Kommissionen anbefalede således, at mindstestørrelsen for forvaltningsenhederne både på lokalt og regionalt niveau øges væsentligt i forhold til i dag, og at den nuværende opgavefordeling ændres, så sammenhængende opgaver i højere grad samles i et forvaltningsled.

1.2. Inddelingsændringer og opgaveflytninger mellem stat, amter og kommuner rejser spørgsmålet om, hvorvidt der er tale om en behandling i persondatalovens forstand. I bekræftende fald kræver videregivelse af personoplysninger i forbindelse med en ressortomlægning af myndighedsopgaver selvstændig hjemmel i loven.

Ifølge persondatalovens § 1, stk. 1, gælder loven 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.

I lovens § 3, nr. 2, defineres en behandling som enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

Det var Datatilsynets opfattelse, at visse former for ressortomlægninger kan betragtes som en form for succession i behandlingen af personoplysninger, der kan finde sted, uden at behandlingsbetingelserne i persondatalovens kapitel 4 skal være opfyldt. Det var således tilsynets opfattelse, at f.eks. en sammenlægning

af 2 kommuner, hvorved samtlige kommunale aktiviteter videreføres under en ny større kommune, efter omstændighederne ikke er en behandling, som falder ind under definitionen på en behandling i persondatalovens § 3, nr. 2.

Er der derimod tale om f.eks. enkelte opgaveflytninger eller nedlæggelse af amter, hvorefter de amtslige myndighedsopgaver fordeles til f.eks. selvejende institutioner, kommuner eller statslige myndigheder, vil der efter tilsynets opfattelse være tale om en behandling i persondatalovens forstand.

I det omfang en ressortomlægning må betragtes som en behandling af personoplysninger, som er omfattet af persondataloven, var det Datatilsynets vurdering, at videregivelsen af personoplysninger må antages at kunne ske inden for rammerne af lovens kapitel 4.

1.3. Datatilsynet henledte i samme forbindelse Indenrigs- og Sundhedsministeriets opmærksomhed på reglerne om oplysningspligt i persondatalovens kapitel 8. Spørgsmålet om omfanget af oplysningspligten i forbindelse med ressortomlægning eller opgaveflytning af myndighedsopgaver må efter Datatilsynets opfattelse afgøres konkret.

2. Kontrol

2.1. Betænkningen satte i vidt omfang borgerne i centrum, herunder den offentlige sektors servicering af den enkelte borger. Særligt i relation til digital forvaltning omtaltes mulighederne for at give en bedre service til borgerne. Derimod var der kun i meget begrænset omfang taget stilling til de muligheder for kontrol, som digital forvaltning ligeledes åbner mulighed for.

I den forbindelse var det bl.a. i afsnittet om perspektiver for effektivisering anført, at digitaliserede opgaver kan samles i effektive enheder og automatiseres. Store regelbundne administrative opgaver, som kontrol af økonomiske oplysninger, indberetninger og ind- og udbetalinger, kan håndteres i samlede enheder, som vil have mulighed for at automatisere og effektivisere processer.

Det var endvidere om eksempler på nye opgavedelinger, der udnytter potentialet i digital forvaltning, anført, at håndtering af refusionsanmodninger i forbindelse med sygdom og udbetaling er 100 pct. regelstyret. Opgaven består af inddatering i it-systemer. Kontrol sker på baggrund af oplysninger fra ansøgninger og opslag i elektroniske registre. Denne opgave kan løses helt uafhængigt af fysisk lokalitet, f.eks. i en fælles enhed, som kan specialisere sig i effektiv håndtering. På sigt kan opgaven reduceres i kraft af fuld digitalisering. De oplysninger, kommunerne har behov for, kan videresendes automatisk, så de kan indgå i opfølgningen på langtidssygemeldte, og spørgsmål kan besvares lokalt.

2.2. Det var Datatilsynets vurdering, at digital forvaltning i høj grad åbner muligheder for øget kontrol, herunder sammenstilling og samkøring i kontroløjemed.

Datatilsynet forudsætter i sin praksis, at myndigheder i forbindelse med sammenstilling og samkøring i kontroløjemed bl.a. har et klart og utvetydigt retsgrundlag at arbejde på, og at de personer, der berøres af kontrolordningen, skal have forudgående information om kontrolordningen, jf. persondatalovens § 5, stk. 1.

Mulighederne for at foretage sammenstilling og samkøring i kontroløjemed svarer således til den praksis, som var gældende før persondatalovens ikrafttræden, og som er kommet til udtryk ved en tilkendegivelse fra flertallet i Retsudvalget i betænkning af 16. maj 1991 over forslag til lov om ændring af lov om offentlige myndigheders registre (L 50). Det er her forudsat, at myndighederne i forbindelse med samkøring i kontroløjemed har et klart og utvetydigt retsgrundlag at arbejde på, og at myndighederne kun lader kontrolordningen tage sigte på fremtidige forhold, medmindre særlige forhold gør sig gældende. Flertallet lagde vægt på, at de borgere, som berøres af en kontrolordning, i almindelighed gøres opmærksom på myndighedernes adgang til at foretage samkøring i kontroløjemed, inden kontrollen iværksættes, og at samkøringen så vidt muligt kun finder sted, hvis de personer, der omfattes af kontrollen, har fået meddelelse om kontrolordningen, inden de afgiver oplysninger til myndigheden.

Sammenstilling og samkøring i kontroløjemed forudsætter endvidere, at behandlingen anmeldes til Datatilsynet, jf. persondatalovens §§ 43-44, samt at tilsynets udtalelse indhentes, forinden behandlingen iværksættes, jf. § 45, stk. 1, nr. 4.

Det var i øvrigt Datatilsynets opfattelse, at antallet af sagsbehandlere, som er beskæftiget med sammenstilling og samkøring i kontroløjemed, skal begrænses mest muligt, jf. nedenfor om bl.a. autorisationer.

3. Servicecentre mv.

3.1. Strukturkommissionen pegede på, at det på enkelte områder, der lå uden for kommissionens kommissorium, kan være hensigtsmæssigt yderligere at analysere behovet for forandringer set i lyset af de gennemgåede anbefalinger til ændringer af den nuværende struktur.

Således har kommissionens analyser – særligt af de forventede udviklingstendenser, herunder af potentialerne ved en øget digitalisering af den offentlige forvaltning – peget i retning af, at der på nogle områder vil være behov for, at lovgivningen, såvel speciallovgivningen som forvaltningsloven, gennemgås med henblik på at vurdere, om eksisterende barrierer for f.eks. udveksling af oplysninger mellem forvaltninger og myndigheder kan fjernes. Der kan dog i visse

tilfælde være andre hensyn – som eksempelvis tungtvejende hensyn til fortrolighed – der taler imod.

Kommissionen vurderede, at en forudsætning for at realisere potentialet forbundet med den digitale forvaltning er, at barrierer i lovgivning mv., der hindrer udveksling af oplysninger og udførelse af borgerservice på tværs af eller mellem forskellige myndigheder, så vidt muligt ophæves.

Ophævelse af sådanne barrierer vil blandt andet understøtte mulighederne for etablering af servicecentre med en tværgående borgerbetjening. Servicecentre i kommunerne eller såkaldte kvikskranker vil muliggøre en fremskudt borgerbetjening, idet disse enheder kan betjene borgerne på vegne af flere offentlige myndigheder.

I forlængelse heraf anbefalede Strukturkommissionen, at muligheden for en fremskudt borgerbetjening tilgodeses i forbindelse med en ny offentlig struktur, f.eks. gennem etableringen af servicecentre i kommunerne.

Det fremgik endvidere af betænkningen, at med digitalisering af store borgerrettede administrationsområder i såvel kommuner og amter som stat åbnes muligheden for at etablere servicecentre i f.eks. kommunerne, som betjener et helt lokalområde i relation til flere offentlige myndigheder. Hensynet til effektivitet og brugervenlighed taler for, at disse kontaktpunkter kan håndtere alle tilgrænsende, fuldt ud digitaliserede opgaver, så borgerne kan betjenes i en samlet sagsgang.

Det anførtes i forlængelse heraf, at en kommunal borgerbetjeningsenhed – serviceskranke mv. – i dag kan varetage alle de opgaver, som en kommune lovligt kan varetage. Som udgangspunkt kan en sådan enhed således træffe afgørelse i alle typer sager, der vedrører kommunens forhold. F.eks. i sager, hvor sagsbehandlingen netop kan it-understøttes, og sager, som kan ekspederes inden for et kort tidsrum, men i praksis vil det dog nok især være i sager karakteriseret ved mange borgerhenvendelser.

3.2. På det foreliggende grundlag stod det ikke Datatilsynet klart, hvilke konkrete barrierer i lovgivningen mv. kommissionen pegede på. Hvis der med de anførte bemærkninger også sigtedes til persondataloven, henledte Datatilsynet opmærksomheden på, at persondataloven i vidt omfang er en implementering af databeskyttelsesdirektivet. Mulighederne for at fravige de direktivbestemte bestemmelser i loven er efter tilsynets opfattelse derfor meget begrænsede.

Opmærksomheden henledtes endvidere på de almindelige bemærkninger til persondataloven og på de tilkendegivelser, som i øvrigt fremkom i forbindelse med

behandlingen af loven, hvorefter der med persondataloven tilsigtedes et fortsat højt beskyttelsesniveau i forhold til den enkelte borger.

3.3. Det fremgik, at formålet med servicecentre er at sikre effektivitet og brugervenlighed, således at borgerne kan betjenes i en samlet sagsgang.

Det var imidlertid ikke klart for Datatilsynet, hvordan servicecentrene i praksis skal fungere. Tilsynet fandt i den forbindelse, at der er en række forhold, der bør afklares inden en eventuel etablering af servicecentre.

Det var tilsynets vurdering, at der bl.a. skal tages stilling til servicecentrenes organisatoriske forhold samt ske en afklaring af dataansvaret i forhold til de oplysninger, der behandles i centrene.

Endvidere skal det efter tilsynets opfattelse afklares, hvilke opgaver og kompetencer der skal tillægges servicecentre.

I den forbindelse skal der navnlig tages stilling til spørgsmålet om, hvorvidt der i servicecentrene alene skal ske sagsbehandling som led i servicering af en borger, eller om centrene ligeledes skal varetage sammenstilling og samkøring af oplysninger i kontroløjemed. Datatilsynet henledte i den forbindelse opmærksomheden på betingelserne for sammenstilling og samkøring af oplysninger i kontroløjemed.

3.4. Behandling af personoplysninger inden for en myndighed, herunder udveksling af oplysninger på tværs af forvaltningsgrene, rejser navnlig spørgsmål om, hvorvidt behandlingen tilrettelægges i overensstemmelse med persondatalovens § 5 og § 41, stk. 3, samt principperne i sikkerhedsbekendtgørelsen.

Det var Datatilsynets opfattelse, at en generel adgang til alle borgerrelaterede oplysninger er meget vidtgående og vanskelig at forene med persondatalovens § 5 og de generelle krav om datasikkerhed i lovens § 41, stk. 3, som bl.a. er udmøntet i sikkerhedsbekendtgørelsens § 11.

Forud for en eventuel etablering af servicecentre bør der således mere overordnet tages stilling til spørgsmålet om datasikkerhed, herunder autorisationer, jf. sikkerhedsbekendtgørelsens § 11.

I denne vurdering skal navnlig karakteren af behandlingen og oplysningerne tillægges betydning. F.eks. må det efter tilsynets opfattelse meget nøje overvejes, hvorvidt det er acceptabelt, at følsomme oplysninger, herunder f.eks. oplysninger i socialsager, behandles i servicecentre.

Endvidere var det Datatilsynets opfattelse, at antallet af sagsbehandlere, som er beskæftiget med sammenstilling og samkøring i kontroløjemed, skal begrænses mest muligt.

Det var i øvrigt Datatilsynets vurdering, at en eventuel videre adgang til oplysninger i servicecentre kan aktualisere behovet for at stille større krav til behandlingssikkerheden, herunder bl.a. at der sættes fokus på interne kontrolordninger samt styring af brugerrettigheder.

3.5. Udveksling af personoplysninger mellem myndigheder rejser tillige spørgsmål om eventuel behandlingshjemmel. Datatilsynet henviste til, at tilsynet tidligere har tilkendegivet, at persondatalovens begrænsninger navnlig ligger i kravet om, at offentlige myndigheder ikke må behandle eller have adgang til oplysninger, som de ikke har behov for i forbindelse med deres konkrete myndighedsudøvelse.

Almindelige ikke-følsomme oplysninger kan i vidt omfang udveksles i forbindelse med konkret udøvelse af myndighedsopgaver i medfør af persondatalovens § 6.

Udveksling af følsomme oplysninger vil ligeledes i et vist omfang kunne ske konkret i medfør af persondatalovens §§ 7 og 8. Det var imidlertid Datatilsynets umiddelbare vurdering, at navnlig de strenge betingelser i persondatalovens § 8, stk. 3, for videregivelse af oplysninger fra forvaltningsmyndigheder, der udfører opgaver inden for det sociale område, kan give anledning til vanskeligheder i forbindelse med etableringen af servicecentre.

3.6. Datatilsynet forudsatte i øvrigt, at persondatalovens bestemmelser, herunder reglerne om oplysningspligt og indsigtsret, iagttages og indarbejdes i procedurerne i forbindelse med en eventuel etablering af servicecentre.

Datatilsynet anmodede endvidere om at blive inddraget i forbindelse med de nærmere overvejelser om en eventuel etablering af servicecentre, herunder med henblik på en vurdering i forhold til persondatalovens § 41, stk. 3, og reglerne i sikkerhedsbekendtgørelsen.

4. Fælles informationsplatforme, kompetencecentre og videndeling

4.1. Det fremgik af betænkningen, at det med digital forvaltning f.eks. er teknisk muligt at etablere fælles informationsplatforme, således at forskellige myndigheder kan dele data og arbejde ud fra samme informationsgrundlag.

Udnyttelse af de tekniske muligheder for at dele information kan naturligvis kun ske under hensyn til og overholdelse af de regler om samtykke, som måtte være fastsat i lovgivningen på de forskellige områder. Udviklingen vil endvidere kræve

en vis grad af fælles mål, begreber og digital infrastruktur på tværs af myndigheder og faglige miljøer. Der vil skulle findes fælles incitamentsmodeller, der sikrer etablering af sammenhængende arbejdsgange. Arbejdet med disse spørgsmål er forankret i den fælles-offentlige Digitale Taskforce.

Etableringen af fælles informationsplatforme for forskellige myndigheder kan kræve lovændringer, især hvor informationerne vedrører følsomme oplysninger om borgerne. Det nævnes i den forbindelse, at de eventuelle begrænsninger i muligheden for udveksling af information i den nuværende lovgivning kan bunde i andre hensyn.

I betænkningen var det om faglig bæredygtighed anført, at det med digital forvaltning i fremtiden bliver lettere at understøtte det faglige arbejde og sikre, at viden deles på tværs af myndigheder – både inden for samme forvaltningsenhed og mellem forvaltningsenhederne. Den offentlige sektor kan fungere som en samlet "virtuel organisation", hvor viden og ekspertise udnyttes, hvor den findes.

Det var ligeledes anført, at det kan være relevant at etablere formelle kompetencecentre, der kan understøtte professionalisering, f.eks. hvor enhederne er meget små, eller hvor udgående medarbejdere skal dække store opgavefelter.

Formelle kompetencecentre vil kræve et tæt samarbejde mellem lokale, regionale og statslige myndigheder. På nogle områder vil ansvarsforhold skulle afklares nærmere, ligesom muligheden for at håndtere sager på vegne af andre myndigheder vil forudsætte tilpasninger i lovgivningen. Det skal i den forbindelse understreges, at der her peges på de muligheder, som den teknologiske udvikling åbner for. Der kan være konkrete hensyn, f.eks. særlige krav til fortrolighed, der taler for at bevare en vis adskillelse på et givet område.

4.2. Persondatalovens § 5 indeholder en række grundlæggende principper for den dataansvarliges behandling, herunder indsamling, ajourføring, opbevaring mv. af oplysninger. Disse krav skal altid være opfyldt.

Af persondatalovens § 5, stk. 2, følger, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål (finalité-princippet).

Det følger endvidere af § 5, stk. 3, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

I forhold til etablering af fælles informationsplatforme, kompetencecentre og videndeling var det Datatilsynets opfattelse, at persondatalovens begrænsninger navnlig ligger i kravet om, at offentlige myndigheder ikke må behandle eller have adgang til oplysninger, som de ikke har behov for i forbindelse med deres konkrete myndighedsudøvelse.

Med hensyn til spørgsmålet om genanvendelse af personoplysninger henledte Datatilsynet i øvrigt Indenrigs- og Sundhedsministeriets opmærksomhed på Artikel 29-gruppens[1] arbejdsdokument af 12. december 2003 vedrørende genanvendelse af oplysninger i offentlige myndigheders besiddelse – "Re-use of public sector information and the protection of personal data – striking the balance"[2].

Dokumentet indeholder bl.a. en drøftelse af databeskyttelsesdirektivets anvendelighed på området samt af, hvilke hensyn der skal inddrages ved en vurdering af, om f.eks. videregivelse er i overensstemmelse med finalité-princippet.

Det nævnes bl.a. i den forbindelse, at hvor oplysningerne er afgivet på baggrund af en retlig forpligtelse, skal videregivelse vurderes særligt nøje under inddragelse af hensynet til "reasonable expectations criterion", dvs. hvad der med rimelighed må kunne forventes ved afgivelsen af oplysningerne.

Behovet for at tilvejebringe tekniske foranstaltninger til sikring af, at adgang til oplysningerne er begrænset eller struktureret på en sådan måde, at uberettiget behandling undgås, herunder f.eks. masseudtræk, understreges flere steder i dokumentet.

Det er endvidere anført, at hvor genanvendelse er lovhjemlet, bør denne også indeholde mulighed for, at der kan fremsættes indsigelse mod genanvendelse allerede på tidspunktet for indsamlingen af oplysningerne. Samtidig bør der gives meddelelse om denne rettighed.

4.3. Datatilsynet henviste til, at tilsynet i en række tilfælde har taget stilling til myndigheders indsamling og videregivelse af oplysninger over internet. Tilsynet har i tilknytning hertil udarbejdet en række værd at vide-tekster, som findes på tilsynets hjemmeside: *Udveksling af oplysninger i portaler og andre digitale løsninger, Oplysningspligt ved indsamling af oplysninger på internettet, Datasikkerhed ved indsamling af oplysninger på internettet og Brugeridentifikation ved borgerservice.*

1 I henhold til artikel 29 i databeskyttelsesdirektivet er der nedsat en "gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger", den såkaldte "Artikel 29-gruppe".
2 Dokumentet "Udtalelse nr. 7/2003 om videreanvendelse af den offentlige sektors informationer og beskyttelse af personoplysninger" kan ses på Datatilsynets hjemmeside under punktet "Internationalt".

5. Selvbetjeningsløsninger og automatiserede afgørelser

5.1. Det fremgik af betænkningen, at størstedelen af den ukomplicerede administrative kontakt mellem borger/virksomhed og den offentlige sektor de kommende år vil blive omlagt til digital dialog og selvbetjening via internet og andre kanaler. Borgere og virksomheder vil anvende e-formularer til indberetninger og ansøgninger til det offentlige til at bestille serviceydelser over nettet (tidsbestilling, informationsmateriale, spørgsmål/svar mv.) og til at kommunikere digitalt med forvaltningen.

Dette vil i nogle tilfælde give mulighed for fuld selvbetjening og mere generelt mulighed for at følge sagsforløbet i den offentlige sektor og løbende være i dialog med de respektive myndigheder. Eksempelvis vil tildeling af rettighedsbestemte ydelser i forbindelse med for eksempel arbejdsløshed, studieskift, skilsmisse, flytning og fødsel kunne foregå fuldt automatisk. Personligningen er allerede automatiseret for en stor del af borgerne.

5.2. Datatilsynet henledte Indenrigs- og Sundhedsministeriets opmærksomhed på, at tilsynet ved Finansministeriets og Forskningsministeriets initiativ til fremme af elektronisk borgerservice i den offentlige forvaltning i 2000 blev central godkendelsesinstans for sikkerhedsløsninger.

Datatilsynet har i den egenskab i en række sager taget stilling til etableringen af selvbetjeningssystemer. Tilsynet henviste i den forbindelse til de generelle problemstillinger, som er omtalt ovenfor under afsnit 4.

Datatilsynet havde i øvrigt noteret sig, at Strukturkommissionen peger på, at den digitale forvaltning bl.a. giver borgerne mulighed for at følge sagsforløbet i den offentlige sektor. Tilsynet finder, at initiativer, der fremmer en øget indsigt i den offentlige sektors sagsbehandling, er i god overensstemmelse med bl.a. Den offentlige sektors strategi for digital forvaltning 2004-06 – realisering af potentialet, som er blevet til i samarbejde mellem regeringen, KL, Amtsrådsforeningen, Københavns Kommune og Frederiksberg Kommune. Heraf følger bl.a., at det skal være et indsatsområde for de kommende år at sikre, at borgerne og virksomhederne med tiden får adgang til egne data.

Datatilsynet fandt det positivt, hvis der gives borgerne digital adgang til egne sager og data. En sådan mulighed er forudset i forarbejderne til persondataloven.

6. Datatilsynet forudsatte i øvrigt, at persondatalovens bestemmelser iagttages i forbindelse med eventuelle udmøntninger af Strukturkommissionens anbefalinger.

Lov om kommunale borger-servicecentre

Indenrigs- og Sundhedsministeriet anmodede om Datatilsynets bemærkninger til forslag til lov om kommunale borgerservicecentre. Lovforslaget var et led i udmøntningen af kommunalreformen.

Datatilsynets udtalelse, som blev afgivet efter behandling i Dataråd et, gengives i alt væsentligt nedenfor.

1. Det fremgik af forslagets § 3, stk. 1, at "Et borgerservicecenter, som varetager en administrativ borgerbetjeningsopgave for en anden myndighed, kan til brug for borgerservicecenterets varetagelse af opgaven afkræve denne myndighed de oplysninger, der er fornødne til varetagelsen af opgaven."

Af § 3, stk. 2, fremgik endvidere, at "En myndighed, der til en kommunalbestyrelse har overladt en administrativ borgerbetjeningsopgave, som varetages i et borgerservicecenter, kan, i det omfang det er fornødent, til brug for myndighedens varetagelse af tilknyttede opgaver eller kontrol med borgerservicecenterets opgavevaretagelse afkræve borgerservicecenteret oplysninger, som er tilgået dette som følge af varetagelsen af opgaven."

Af de almindelige bemærkninger til lovforslaget, afsnittet om udveksling af oplysninger efter persondataloven, fremgik det, at der med lovforslaget sker en fravigelse af persondatalovens § 8, stk. 3, om behandling af følsomme personoplysninger på det sociale område.

Af persondatalovens § 2, stk. 1, følger, at regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven. Ifølge persondatalovens forarbejder følger det omvendt af bestemmelsen, at persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling. Dette gælder dog ikke, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod direktivet[3] om behandling af personoplysninger.

Datatilsynet noterede sig, at Indenrigs- og Sundhedsministeriet havde vurderet, at en fravigelse af bestemmelsen i § 8, stk. 3, ikke vil være i strid med direktivet. Datatilsynet var enig i denne vurdering.

Datatilsynet henledte imidlertid opmærksomheden på, at § 8, stk. 3, blev indsat ved fremsættelsen af det 3. lovforslag til persondataloven med henblik på at fastsætte strenge betingelser for videregivelse af personoplysninger på det sociale område.

3 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.

Det var Datatilsynets opfattelse, at lovforslaget om kommunale borgerservicecentre med sin generelle regulering muliggør udveksling af personoplysninger om sociale forhold i meget videre omfang, end det ellers ville have været tilfældet. Da der er tale om en række ikke-konkretiserede opgaver, fandt Datatilsynet, at det ikke var muligt at overskue konsekvenserne af forslaget i forhold til udveksling af oplysninger på det sociale område.

Samtidig fremgik det ikke af lovforslagets bemærkninger, hvilke hensyn der nu – 4½ år efter vedtagelsen af persondataloven – taler for, at man i så ubestemt omfang sætter bestemmelsen i persondatalovens § 8, stk. 3, ud af kraft.

Datatilsynet anbefalede derfor, at det meget nøje overvejes, om der nu er grundlag for at anlægge en anden vurdering af dette spørgsmål og fravige de strenge betingelser for videregivelse af følsomme oplysninger på det sociale område i helt generel form.

2. Det fulgte endvidere af forslaget § 3, stk. 5, at "Når arbejdsdokumenter, der i henhold til lov om offentlighed i forvaltningen og forvaltningsloven er interne, videregives i medfør af stk. 1 eller 2, mister dokumenterne ikke som følge af videregivelsen deres interne karakter."

Af de almindelige bemærkningers afsnit om gældende ret fulgte bl.a., at "Interne arbejdsdokumenter er som udgangspunkt ikke undergivet aktindsigt, jf. forvaltningslovens § 12, stk. 1, og offentlighedslovens § 7."

Det fulgte endvidere af afsnittet om Indenrigs- og Sundhedsministeriets overvejelser om den foreslåede regulering, bl.a. at "Det er efter Indenrigs- og Sundhedsministeriets opfattelse en uhensigtsmæssig barriere for borgerservicecentrenes virksomhed, at selve overladelsen af en opgave bevirker, at der skal meddeles aktindsigt i oplysninger, som ellers ville være undtaget fra aktindsigt. Efter Indenrigs- og Sundhedsministeriets opfattelse gælder dette ligeledes, hvis det ved lovgivningen er bestemt, at to myndigheder skal varetage hver sin del af et integreret sagsbehandlingsforløb i stedet for, at opgaven i overensstemmelse med en mere traditionel arbejdstilrettelæggelse var henlagt til en enkelt myndighed. Herved kan parter og udenforstående få adgang til notater og lign., som alene vedrører myndighedernes interne beslutningsproces, blot fordi der er sket en sådan særlig arbejdstilrettelæggelse, og der af denne grund er behov for at udveksle oplysningerne mellem borgerservicecenter og ansvarlig myndighed.

Der er derfor i lovforslagets § 3, stk. 5, indsat en bestemmelse om, at når arbejdsdokumenter, som efter offentlighedsloven eller forvaltningsloven er interne, videregives efter lovforslagets § 3, stk. 1, 2 og 6, mister de ikke deres interne karakter."

I tilknytning hertil bemærkede Datatilsynet, at det følger af persondatalovens § 31, at fremsætter en person begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om, 1) hvilke oplysninger der behandles, 2) behandlingens formål, 3) kategorierne af modtagere af oplysningerne og 4) tilgængelig information om, hvorfra disse oplysninger stammer.

Af lovens § 32, stk. 2, følger, at oplysninger, der behandles for den offentlige forvaltning som led i administrativ sagsbehandling, kan undtages fra indsigtsretten i samme omfang som efter reglerne i offentlighedslovens § 2 samt §§ 7-11 og 14.

På den baggrund var det Datatilsynets opfattelse, at lovforslagets § 3, stk. 1 og 2, tillige må antages at medføre en vis begrænsning i retten til indsigt i medfør af persondataloven.

Datatilsynet gik ud fra, at dette var en tilsigtet konsekvens af forslaget. Tilsynet foreslog, at dette forhold omtales i bemærkningerne til loven.

3. Af de almindelige bemærkningers afsnit om adgang til kommunens egne elektroniske systemer og til at foretage samkøring mv. fremgik bl.a., at "En adgang for en enkelt kommunal medarbejder til alle borgerrelaterede oplysninger kan efter omstændighederne være vanskelig at forene med persondatalovens § 5 og de generelle krav om datasikkerhed i lovens § 41, stk. 3, og sikkerhedsbekendtgørelsens § 11. Dette uanset, at en medarbejder med en sådan generel adgang tilsvarende varetager en lang række opgaver, som hver for sig sagligt berettiger til adgang til de enkelte oplysninger."

Datatilsynet understregede, at det som tilkendegivet i Datatilsynets høringssvar over Strukturkommissionens betænkning[4] er tilsynets opfattelse, at en generel adgang for medarbejdere til alle borgerrelaterede oplysninger er meget vidtgående, og at en sådan adgang er vanskelig at forene med persondatalovens § 5 og de generelle krav om datasikkerhed i lovens § 41, stk. 3, som bl.a. er udmøntet i sikkerhedsbekendtgørelsens § 11.

På den baggrund må adgangen til borgerrelaterede oplysninger i et servicecenter efter Datatilsynets opfattelse vurderes konkret og individuelt for den enkelte medarbejder, og det bør i denne forbindelse tilstræbes, at adgangen til navnlig følsomme oplysninger i eksempelvis sociale sager begrænses mest muligt.

Under henvisning til det anførte foreslog Datatilsynet, at formuleringen "efter omstændighederne" i de almindelige bemærkningers afsnit om adgang til kommunens egne elektroniske systemer og til at foretage samkøring mv. slettes.

4 Gengivet ovenfor.

Den pågældende brug af medarbejdere til løsning af forskellige opgaver gør det endvidere påkrævet, at der i forbindelse med servicecenterkonstruktionen og it-understøttelsen af centrene sker en forøgelse af behandlingssikkerheden, herunder med hensyn til styring af brugerrettigheder og interne kontrolordninger i forhold til medarbejdernes anvendelse af it-systemerne.

Det var i øvrigt Datatilsynets opfattelse, at etablering af servicecentre medfører, at kommunerne må styrke uddannelse og vejledning af medarbejderne om behandlingen af personoplysninger, herunder navnlig under hvilke betingelser en medarbejder lovligt kan behandle personoplysninger, som vedkommende er autoriseret til.

Datatilsynet henstillede til ministeriets overvejelse, at de nævnte aspekter om behandlingssikkerhed og uddannelse og vejledning af medarbejdere også omtales i lovforslagets bemærkninger, således at det sikres, at hensyn til persondatabeskyttelse også indgår i det videre arbejde med etablering af servicecentre.

4. Der var i de almindelige bemærkningers afsnit om udveksling af oplysninger efter persondataloven og om udveksling af oplysninger efter persondataloven henvist til persondatalovens materielle behandlingsregler i § 5, stk. 1 og 2, §§ 6 – 8 og § 11, stk. 1.

Datatilsynet fandt, at henvisningen burde omfatte § 5 i sin helhed, idet navnlig også proportionalitetsprincippet i persondatalovens § 5, stk. 3, hvoraf det fremgår, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles, er et centralt, grundlæggende princip ved behandling, herunder videregivelse, af personoplysninger.

Persondatalovens § 5 er i øvrigt en implementering af databeskyttelsesdirektivets artikel 6.

5. Datatilsynet gik i øvrigt ud fra, at persondatalovens regler iagttages i forbindelse med de kommunale borgerservicecentres behandling af personoplysninger, herunder navnlig lovens bestemmelser om behandlingshjemmel, sikkerhed og den registreredes rettigheder. I det omfang servicecentrene – som dataansvarlige myndigheder – indsamler og registrerer personoplysninger, henledte Datatilsynet særligt opmærksomheden på bestemmelserne om oplysningspligt over for den registrerede, jf. lovens kapitel 8.

.....

Datatilsynet har endvidere afgivet en udtalelse vedrørende Indenrigs- og Sundhedsministeriets udkast til forslag til lov om forpligtende kommunale

samarbejder, der ligeledes var et led i udmøntningen af kommunalreformen. I udtalelsen omtaler Datatilsynet i alt væsentligt de samme persondataretlige problemstillinger som i høringssvaret vedrørende kommunale borgerservicecentre.

.....

I forbindelse med Folketingets behandling af de to lovforslag har Datatilsynet i 2005 afgivet en udtalelse om styring af brugerrettigheder og interne kontrolordninger. Udtalelsen kan ses på Datatilsynets hjemmeside under punktet "Værd at vide", under punktet "Sikkerhed".

Lov om skatte- og ejendomsvurderingsforvaltning (skatteforvaltningsloven)

Skatteministeriet anmodede Datatilsynet om bemærkninger til udkast til forslag til lov om skatte- og ejendomsvurderingsforvaltning (skatteforvaltningsloven). Lovforslaget var et led i udmøntningen af kommunalreformen.

Datatilsynets udtalelse gengives i det væsentligste nedenfor.

1. Formålet med lovforslaget var at samle forvaltningen af lovgivning om indkomstskat, moms, punktafgifter, told, arbejdsmarkedsbidrag og lignende ydelser til det offentlige i en enhedsforvaltning i statsligt regi. Den nye enhedsforvaltning dannes gennem en fusion mellem de nuværende kommunale skatteforvaltninger og ToldSkat og organiseres som én landsdækkende forvaltningsmyndighed, der lokaliseres med filialer 30 steder landet over.

Datatilsynet bemærkede i den forbindelse, at grænserne for, hvilke behandlinger af personoplysninger den kommende told- og skatteforvaltning vil kunne foretage, findes i persondataloven. Persondatalovens behandlingsregler giver – kort fortalt – mulighed for, at told- og skatteforvaltningen må indsamle og registrere personoplysninger i det omfang, det er nødvendigt for varetagelsen af myndighedens opgaver.

2. Det fremgik af forslaget, at skatteborgerne som udgangspunkt skal kunne bruge en hvilken som helst filial som indgang til told- og skatteforvaltningen, f.eks. den filial, der ligger nærmest borgerens arbejdsplads.

I de almindelige bemærkninger til lovforslaget var bl.a. angivet, at målet er, at alle filialer af told- og skatteforvaltningen skal kunne servicere alle borgere om alle normalt forekommende skattemæssige forhold. Men en række opgaver er af sådan karakter, at administrationen heraf vil blive forankret få steder eller et enkelt sted i organisationen. Det kan f.eks. være sjældent forekommende og/eller komplicerede opgaver og opgaver af administrativ karakter, hvor der vil kunne opnås stordriftsfordele ved en koncentration.

Datatilsynet bemærkede i den forbindelse, at behandling af personoplysninger inden for den kommende told- og skattemyndighed skal tilrettelægges i overensstemmelse med persondatalovens § 5 og § 41, stk. 3, samt principperne i sikkerhedsbekendtgørelsen.

Det var Datatilsynets opfattelse, at det vil være muligt inden for rammerne af persondataloven og sikkerhedsbekendtgørelsen at give medarbejderne i filialerne adgang til de personoplysninger, der er nødvendige for at betjene borgere.

De ansatte i told- og skatteforvaltningen må imidlertid kun autoriseres til de anvendelser, som de har behov for, og kun personer beskæftiget med de formål, hvortil oplysningerne behandles, må autoriseres.

Det var i den forbindelse Datatilsynets opfattelse, at en generel adgang til alle borgerrelaterede oplysninger er meget vidtgående og vanskelig at forene med persondatalovens § 5 og de generelle krav om datasikkerhed i lovens § 41, stk. 3, som bl.a. er udmøntet i sikkerhedsbekendtgørelsens § 11.

3. Datatilsynet var bekymret for, om den nye organisationsform ville medføre, at der vil blive en videre adgang for et større antal brugere til de fortrolige og følsomme personoplysninger, som den nye told- og skatteforvaltning kommer i besiddelse af.

Det var derfor tilsynets opfattelse, at dette spørgsmål burde overvejes nærmere og beskrives i lovforslagets bemærkninger, således at også dette forhold indgår i den politiske beslutningsproces.

Det var samtidig Datatilsynets vurdering, at en sådan eventuel videre adgang til oplysninger vil aktualisere behovet for at stille større krav til behandlingssikkerheden, herunder bl.a. at der sættes fokus på interne kontrolordninger samt styring af brugerrettigheder.

Herudover kan det blive relevant at supplere adgangskontrol- og autorisationsordningen med andre løsninger. Det kunne f.eks. overvejes at gøre oplysninger om, hvem der har set oplysninger om en borger, tilgængelige for borgeren i en elektronisk selvbetjeningsløsning, ligesom det kendes fra den medicinprofil, som Lægemiddelstyrelsen er dataansvarlig for.

4. Det fremgik af lovforslagets almindelige bemærkninger, at organiseringen af told- og skatteforvaltningen som én landsdækkende forvaltningsmyndighed set fra forvaltningens side giver forvaltningen færre interne barrierer, hvilket øger mulighederne for en effektiv anvendelse af forvaltningens ressourcer, såvel med hensyn til personale som med hensyn til anvendelse af elektroniske hjælpemidler. Forvaltningen får således lettere ved at oprette enheder til at administrere

specielle sagsområder og lettere ved at kanalisere ressourceanvendelsen til områder, hvor der er et aktuelt behov.

Internt i forvaltningen vil der ske en organisering med udgangspunkt i en samlet service- og kontrolstrategi.

Datatilsynet bemærkede i tilknytning hertil, at det anførte tydede på, at der vil ske elektronisk sammenstilling eller samkøring af oplysninger i kontroløjemed.

Datatilsynet gjorde i den forbindelse opmærksom på, at tilsynet i sin praksis forudsætter, at myndigheder i forbindelse med sammenstilling og samkøring i kontroløjemed bl.a. har et klart og utvetydigt retsgrundlag at arbejde på, og at de personer, der berøres af kontrolordningen, skal have forudgående information om kontrolordningen, jf. persondatalovens § 5, stk. 1.[5]

5. Lovforslaget indeholdt en bemyndigelse til skatteministeren til at fastsætte regler, hvorefter landets kommunalforvaltninger får ret til elektronisk at trække på oplysninger, der er registreret af told- og skatteforvaltningen. Det fremgik af bemærkningerne, at baggrunden for bemyndigelsesbestemmelsen var, at kommunerne med etableringen af den foreslåede enhedsforvaltning i statsligt regi mister de informationer, der udspringer af ligningen.

I den forbindelse bemærkede Datatilsynet, at persondataloven sætter grænser for videregivelsen fra told- og skatteforvaltningen til kommunerne. Datatilsynet gik ud fra, at persondataloven, hvis regler i vidt omfang er direktivbestemte, vil skulle respekteres ved udmøntningen af bemyndigelsen.

Datatilsynet bemærkede for en god ordens skyld, at den i de almindelige bemærkninger anførte begrundelse – at kommunerne "mister" informationer, der udspringer af ligningen – ikke i sig selv synes at kunne begrunde en videregivelse. Det vil i forhold til persondatalovens regler alene være muligt at etablere adgang til videregivelse i det omfang, dette er nødvendigt for udførelsen af told- og skatteforvaltningens eller kommunernes opgaver. For så vidt angår følsomme oplysninger omfattet af persondatalovens § 7, vil der alene kunne ske videregivelse uden borgerens samtykke i det omfang, det er nødvendigt for, at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. § 7, stk. 2, nr. 4.

6. Herudover bemærkede Datatilsynet, at oplysningerne i told- og skatteforvaltningen efter tilsynets opfattelse må antages hovedsageligt at være registreret med henblik på at blive anvendt af denne myndighed til ligning mv., men ikke generelt med henblik på anvendelse hos alle offentlige myndigheder.

---

5 For nærmere om Datatilsynets praksis vedrørende sammenstilling og samkøring i kontroløjemed henvises til tilsynets høringssvar vedrørende Strukturkommissionens betænkning nr. 1434/2004, som er gengivet ovenfor.

Ved udnyttelsen af bemyndigelsen vil der således efter Datatilsynets opfattelse tillige skulle tages hensyn til persondatalovens § 5, som indeholder en række grundlæggende principper for den dataansvarliges behandling, herunder indsamling, ajourføring, opbevaring mv., af oplysninger. Disse krav skal altid være opfyldt.

I forhold til etablering af fælles informationsplatforme, kompetencecentre og videndeling er det Datatilsynets opfattelse, at persondatalovens begrænsninger navnlig ligger i kravet om, at offentlige myndigheder ikke må behandle eller have adgang til oplysninger, som de ikke har behov for i forbindelse med deres konkrete myndighedsudøvelse.

I relation til mulighederne for at genanvende told- og skatteforvaltningens oplysninger henledte Datatilsynet Skatteministeriets opmærksomhed på Artikel 29-gruppens arbejdsdokument af 12. december 2003 vedrørende genanvendelse af oplysninger i offentlige myndigheders besiddelse, "Udtalelse nr. 7/2003 om videreanvendelse af den offentlige sektors informationer og beskyttelse af personoplysninger – En passende afvejning mellem modstridende interesser"[6].

Datatilsynet fandt, at princippet om formålsbestemthed (finalité-princippet) må tages i betragtning ved udmøntningen af bemyndigelsen. Herudover vil den særlige tavshedspligt, som videreføres med lovforslagets § 16, efter Datatilsynets opfattelse skulle tages i betragtning ved vurderingen af, i hvilket omfang told- og skatteforvaltningens oplysninger kan genanvendes.

Lov om opkrævning og inddrivelse af visse fordringer

Skatteministeriet anmodede om Datatilsynets bemærkninger til udkast til forslag til lov om opkrævning og inddrivelse af visse fordringer. Lovforslaget var et led i udmøntningen af kommunalreformen.

Lovforslaget lagde op til at samle restanceinddrivelsen i staten, således at al restanceinddrivelse vedrørende offentlige fordringer overføres og samles hos én statslig myndighed, restanceinddrivelsesmyndigheden under Skatteministeriet. Samlingen vil omfatte den inddrivelse, der i dag varetages af kommunerne og amtskommunerne, politiet, domstolene, Økonomistyrelsen og af ToldSkats områder samt Inddrivelsesenheden under ToldSkat.

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

1. Lovforslaget lagde op til en omfattende videregivelse af personoplysninger, herunder følsomme oplysninger, mellem offentlige myndigheder, og det var Da-

6 Omtalt nærmere ovenfor i Datatilsynets høringssvar til Strukturkommissionens betænkning nr. 1434/2004.

tatilsynets vurdering, at dette formentlig ikke i alle tilfælde ville kunne ske inden for persondatalovens rammer.

Det var derfor Datatilsynets opfattelse, at Skatteministeriet burde beskrive forholdet til persondataloven i bemærkningerne til lovforslaget, herunder i hvilket omfang det med forslaget er tilsigtet at fravige persondataloven, jf. også de konkrete bemærkninger nedenfor under punkt 2-7.

En række af de centrale bestemmelser i lovforslaget var formuleret meget bredt og upræcist og bestod af generelle bemyndigelser til at fastsætte nærmere regler på området. Datatilsynet fandt, at flere af de omhandlede bestemmelser i deres nuværende udformning ikke levede op til de grundlæggende databeskyttelsesprincipper i persondataloven og databeskyttelsesdirektivet.

2. Det fremgik af lovforslaget, at der vil skulle ske videregivelse af oplysninger dels fra fordringshaverne til restanceinddrivelsesmyndigheden (forslagets § 2, stk. 3 og 5), dels fra andre offentlige myndigheder, pengeinstitutter og værdipapircentralen til restanceinddrivelsesmyndigheden (forslagets § 3, stk. 3) og dels fra restanceinddrivelsesmyndigheden til andre offentlige myndigheder, herunder fordringshavere (forslagets § 3, stk. 4).

Datatilsynet bemærkede i den forbindelse, at såvel indsamling og registrering af personoplysninger som videregivelse heraf udgør behandlinger omfattet af persondataloven, når det sker elektronisk. Persondataloven sondrer mellem forskellige kategorier af oplysninger – følsomme oplysninger, andre følsomme oplysninger samt fortrolige og almindelige oplysninger – og der er forskellige behandlingsregler alt afhængig af, hvilken kategori af oplysninger der er tale om.

Det fremgik af lovforslagets almindelige bemærkninger samt af bemærkningerne til § 3, at restanceinddrivelsesmyndigheden får adgang til at indhente oplysninger om skyldnerens økonomiske forhold, arbejdsmæssige forhold, boligmæssige forhold mv. Det var anført, at den overvejende del af de oplysninger, som er nødvendige for at behandle en inddrivelsessag, normalt har en sådan karakter, at de ikke kan betegnes som oplysninger om enkeltpersoners rent private forhold. Dog kunne det ikke udelukkes, at visse af de oplysninger af f.eks. social karakter, som en kommune er i besiddelse af, og som kan have betydning for behandlingen af en inddrivelsessag, må betegnes som oplysninger om enkeltpersoners private forhold.

Det fremgik endvidere af lovforslaget, at restanceinddrivelsesmyndigheden vil skulle stille oplysninger om restancer til rådighed for andre offentlige myndigheder, herunder fordringshavere, f.eks. oplysninger om skyldnerens samlede gældsforhold, indgåede og misligholdte betalingsaftaler mv.

Det var endelig i de almindelige bemærkninger til lovforslaget om konsekvensændringer bl.a. anført, at inddrivelsen af bøder, konfiskationsbeløb og sagsomkostninger under Justitsministeriets område adskiller sig fra de øvrige fordringer ved, at der enten er tale om en strafferetlig sanktion som konsekvens af en uacceptabel adfærd eller et krav, der udspringer af et strafbart forhold.

På denne baggrund var det Datatilsynets vurdering, at lovforslaget indebar behandling, herunder videregivelse, af såvel følsomme oplysninger omfattet af persondatalovens §§ 7 og 8 som fortrolige og almindelige oplysninger omfattet af persondatalovens § 6.

Datatilsynet henstillede, at forholdet til persondatalovens behandlingsregler blev overvejet, hvis ikke dette var sket i forbindelse med lovforslagets tilblivelse. Datatilsynet fandt det endvidere hensigtsmæssigt, at lovforslagets bemærkninger indeholder en beskrivelse heraf, jf. som nævnt under punkt 1.

3.1. Det fulgte af lovforslagets § 3, stk. 3, 1. punktum, at restanceinddrivelsesmyndigheden kan indhente oplysninger, der er nødvendige for restanceinddrivelsesmyndighedens opgavevaretagelse, hos andre offentlige myndigheder, hos pengeinstitutter samt hos Værdipapircentralen.

I bemærkningerne til lovforslagets § 3 omtaltes oplysninger om enkeltpersoners rent private forhold. Det var tilsyneladende hensigten, at sådanne oplysninger vil kunne indhentes af restanceinddrivelsesmyndigheden.

Som nævnt følger det af persondataloven, at der skal være hjemmel til såvel indsamlingen af oplysninger som til videregivelsen fra de myndigheder mv., hvorfra oplysningerne indhentes. Det stod ikke Datatilsynet klart, om det med bestemmelsen var tilsigtet, at videregivelsen af personoplysninger fra offentlige myndigheder mv. skal ske inden for rammerne af persondataloven, eller om der med lovforslaget var tilsigtet en fravigelse af persondataloven.

I den forbindelse gjorde tilsynet navnlig opmærksom på bestemmelserne i persondatalovens §§ 7 og 8, som regulerer adgangen til at indsamle, registrere og videregive følsomme oplysninger. Opmærksomheden henledtes særligt på, at betingelserne for at videregive oplysninger på det sociale område svarer til kravene i forvaltningslovens § 28, stk. 2, jf. herved persondatalovens § 8, stk. 3.

Af persondatalovens § 2, stk. 1, følger, at regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven. Ifølge persondatalovens forarbejder følger det omvendt af bestemmelsen, at persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling. Dette gælder dog ikke, hvis den dårligere retsstilling har

været tilsigtet og i øvrigt ikke strider mod direktivet om behandling af personoplysninger

Datatilsynets henstillede, at det præciseres i lovforslaget, om det er tilsigtet at skabe en dårligere retsstilling for de registrerede end efter persondataloven og i givet fald på hvilke områder.

Datatilsynet henstillede endvidere, at Skatteministeriet i den forbindelse foretager en vurdering af den ønskede retstilstand i forhold til databeskyttelsesdirektivet, herunder navnlig artikel 8 om de følsomme oplysninger.

Behandling af personoplysninger skal tillige ske i overensstemmelse med de grundlæggende principper, som er indeholdt i persondatalovens § 5, og som bygger på artikel 6 i databeskyttelsesdirektivet. Lovens § 5 stiller bl.a. krav om formålsbestemthed, saglighed og proportionalitet.

I den forbindelse bemærkede Datatilsynet særligt, at henvisningen til "offentlige myndigheder" i lovforslagets § 3, stk. 3, 1. punktum, var meget vidtgående og upræcis, og under henvisning til kravene i persondatalovens § 5 og databeskyttelsesdirektivets artikel 6 fandt tilsynet, at det i loven nærmere bør afgrænses, hvilke myndigheder der er tale om.

3.2. Det fulgte af lovforslagets § 3, stk. 3, 2. punktum, at restanceinddrivelsesmyndigheden fra registre, der føres af offentlige myndigheder, kan kræve de oplysninger om skyldnerens forhold, som er af betydning for inddrivelsen.

Denne formulering tydede efter Datatilsynets opfattelse på, at der dermed søgtes skabt en hjemmel til såvel indsamling af oplysninger som videregivelse heraf fra offentlige registre.

Datatilsynet henviste i den forbindelse til bemærkningerne ovenfor under punkt 2 om forholdet til persondataloven og databeskyttelsesdirektivet.

Det var Datatilsynets vurdering, at den generelle henvisning til offentlige registre var meget vidtgående. Det var derfor Datatilsynets opfattelse, at det burde præciseres, hvilke registre der er tale om, herunder om der er tale om registre, der er oprettet med henblik på specifikke formål.

Datatilsynet henledte i den forbindelse navnlig opmærksomheden på persondatalovens § 5, stk. 2, om, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål.

3.3. Det fremgik af lovforslagets § 3, stk. 4, at skatteministeren kan fastsætte regler, hvorefter offentlige myndigheder, herunder fordringshavere, får elektronisk adgang til oplysninger om restancer registreret af restanceinddrivelsesmyndigheden.

Det var i bemærkningerne til lovforslaget anført, at videregivelsen vil omfatte data, der er genereret hos restanceinddrivelsesmyndigheden, som for eksempel oplysninger om skyldnerens samlede gældsforhold, indgåede og misligholdte betalingsaftaler mv.

Som anført ovenfor forudsætter videregivelse af oplysninger, dels at der er hjemmel hertil i persondataloven, dels at de almindelige betingelser i persondatalovens § 5 er opfyldt. Opmærksomheden henledtes særligt på § 5, stk. 2 og 3.

Det var Datatilsynets opfattelse, at den foreslåede bestemmelse i § 3, stk. 4, og bemærkningerne hertil indeholdt en videregivelsesadgang, der må anses for at være i strid med persondatalovens § 5 og databeskyttelsesdirektivets artikel 6.

Der burde således efter tilsynets opfattelse i selve lovforslaget ske en afgrænsning af, hvilke oplysninger der gives adgang til.

Datatilsynet forudsatte i øvrigt, at der ikke vil være adgang til at videregive oplysninger om de underliggende data, som restanceinddrivelsesmyndigheden er i besiddelse af.

4. Den nye organisationsform på inddrivelsesområdet indebar efter Datatilsynets umiddelbare opfattelse, at der vil blive en videre adgang for et større antal brugere til de fortrolige og følsomme personoplysninger, som den nye restanceinddrivelsesmyndighed kommer i besiddelse af.

Datatilsynet bemærkede i den forbindelse, at behandling af personoplysninger inden for den kommende restanceinddrivelsesmyndighed skal tilrettelægges i overensstemmelse med persondatalovens § 5 og § 41, stk. 3, samt principperne i sikkerhedsbekendtgørelsen.

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.

En udmøntning af princippet i § 41, stk. 3, er bl.a. sket i sikkerhedsbekendtgørelsens § 11, stk. 1, hvoraf det følger, at kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. Af § 11, stk. 2, følger end-

videre, at der kun må autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

Efter Datatilsynets opfattelse vil det være muligt inden for rammerne af persondataloven og sikkerhedsbekendtgørelsen at give medarbejderne i restanceinddrivelsesmyndigheden adgang til de personoplysninger, der er nødvendige.

De ansatte må imidlertid kun autoriseres til de anvendelser, som de har behov for, og kun personer beskæftiget med de formål, hvortil oplysningerne behandles, må autoriseres, jf. ovenfor om sikkerhedsbekendtgørelsens § 11, stk. 2.

5. Det fremgik af bemærkningerne til lovforslaget, at på kort og mellemlangt sigt skal restanceinddrivelsesmyndigheden benytte de eksisterende 10 it-systemer i opgavevaretagelsen. Det var anført, at dette indebærer, at dataejerskabet for oplysninger i kommunale registre for visse oplysningers vedkommende skal overgå til restanceinddrivelsesmyndigheden. Da oplysningerne i de kommunale systemer er integrerede, og adgang til oplysningerne ikke umiddelbart kan begrænses, vil det i en overgangsperiode være nødvendigt at opretholde de eksisterende adgangsmuligheder, eventuelt i form af delt dataejerskab til visse oplysningstyper.

Datatilsynet lagde til grund, at restanceinddrivelsesmyndigheden ikke derved får adgang til personoplysninger, der ikke er nødvendige for udførelsen af restanceinddrivelsen, og vice versa.

Det stod i øvrigt ikke Datatilsynet klart, hvad der mentes med begrebet "dataejerskab".

Datatilsynet henviste i den forbindelse til, at 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 henstillede, at Skatteministeriet overvejede, hvem der er dataansvarlig for de pågældende oplysninger. Det bemærkedes i den forbindelse, at der i forhold til persondataloven påhviler den dataansvarlige en række forpligtelser, bl.a. vedrørende den registreredes rettigheder, sikkerhed, anmeldelser mv.

6. Det var Datatilsynets vurdering, at der med gennemførelse af lovforslaget vil ske en omfattende behandling, herunder videregivelse, af bl.a. fortrolige og følsomme oplysninger, hvis lovlighed i henhold til persondataloven vil kunne påklages til Datatilsynet, og som i øvrigt er underlagt Datatilsynets tilsynskompetence, jf. persondatalovens § 58, stk. 1.

Ud fra Datatilsynets erfaring med behandling af klager på bl.a. kreditoplysningsområdet var det tilsynets vurdering, at antallet af klager på dette område kan tænkes at få et stigende omfang. Datatilsynet måtte derfor gøre opmærksom på, at tilsynets ressourcer er begrænsede, og at tilsynet måtte forbeholde sig at få tilført yderligere ressourcer, såfremt det viser sig nødvendigt.

Datatilsynet anmodede om, at dette aspekt indgik i Skatteministeriets videre overvejelser omkring ordningen.

DNA-profilregister

Justitsministeriet anmodede Datatilsynet om bemærkninger til forslag til lov om ændring af lov om oprettelse af et centralt DNA-profilregister og retsplejeloven.

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

1. Formålet med lovforslaget var at udvide mulighederne for at anvende DNA-profilregisteret som led i efterforskningen af kriminalitet. Dette skulle opnås ved at skabe parallelitet mellem Rigspolitichefens Centrale Fingeraftryksregister og DNA-profilregisteret. Der skulle således ifølge lovforslaget gælde lignende betingelser for de to registre, både for så vidt angår tilvejebringelse og registrering af DNA-profiler og med hensyn til reglerne om sletning fra registeret.

Som følge af ønsket om at skabe parallelitet mellem Fingeraftryksregisteret og DNA-profilregisteret indebar lovforslaget betydelige lempelser af betingelserne for registrering i DNA-profilregisteret.

Det foreliggende lovforslag rejste efter Datatilsynets opfattelse spørgsmål i forhold til de grundlæggende principper indeholdt i persondatalovens § 5. Der var således efter Datatilsynets opfattelse grund til at overveje, hvorvidt de foreslåede lempelser, der omfattede indikations-, mistanke- og kriminalitetskrav kombineret med en væsentlig begrænsning af kravene om sletning fra registeret, harmonerede med bestemmelserne i persondatalovens § 5, herunder navnlig proportionalitetsprincippet og kravet om at undgå unødig dataophobning.

Ved denne vurdering måtte det efter Datatilsynets opfattelse også tages i betragtning, at forslaget medførte en væsentligt udvidet indsamling og opbevaring

af biologisk materiale, idet dette var en forudsætning for, at de i lovforslaget forudsatte DNA-analyser kan foretages.

Det fremgår af den gældende lovs § 2, stk. 1, at der i DNA-profilregisteret kun må optages oplysninger, der er af politimæssig betydning i forbindelse med personidentifikation.

Det fremgik af lovforslagets beskrivelse af gældende ret, at det ikke er muligt at udlede følsomme oplysninger om en persons genetiske karakteristika, herunder udseende, arveanlæg, sygdomsdispositioner eller lignende, af de registrerede talprofiler.

Datatilsynet noterede sig, at det under punkt 4 i Strafferetsplejeudvalgets udtalelse var anført, at der af blod- og spytmateriale udtaget efter de foreslåede regler bl.a. kan udledes information om personers genetiske egenskaber.

Uanset at de oplysninger, som opbevares i selve DNA-profilregisteret, ikke er følsomme, ville den påtænkte udvidelse af registeret således føre til øget behandling af følsomme oplysninger, idet det biologiske materiale, der danner grundlag for DNA-profilerne, indeholder sådanne oplysninger.

Vurderingen af lovforslaget burde derfor tillige foretages i lyset af det forhold, at der er forskel på biologisk materiale og fingeraftryk.

Konsekvensen af forslaget var således, at der ville blive indsamlet og opbevaret biologisk materiale med følsomme personoplysninger i væsentligt større omfang end tidligere, samtidig med at antallet af registreringer i selve DNA-profilregisteret blev kraftigt forøget.

Datatilsynet fandt på denne baggrund, at hensynet til effektivt at kunne efterforske forbrydelser ved hjælp af en væsentlig udvidelse af DNA-profilregisteret nøje måtte afvejes i forhold til hensynet til persondatabeskyttelse, herunder til at begrænse indsamling og opbevaring af følsomme personoplysninger, og at forslaget kun bør gennemføres, hvis væsentlige samfundsmæssige hensyn findes at tale herfor.

2. I henhold til de gældende regler for DNA-profilregisteret skal en registreret person slettes af registerets persondel 10 år efter, at vedkommende er blevet frifundet, har modtaget en påtaleopgivelse eller lignende. Hvis en registreret person derimod er fundet skyldig ved dom mv., skal vedkommende slettes af registeret efter at være fyldt 70 år. Efter lovforslaget skulle alle registrerede personer først slettes, når de pågældende er fyldt 80 år – ligesom det er tilfældet i Fingeraftryks-registeret.

Denne forlængelse af registerets sletningsfrist var ifølge lovforslagets bemærkninger begrundet i ønsket om at indføre parallelitet mellem DNA-profilregisteret og Fingeraftryksregisteret og for at forbedre DNA-profilregisterets anvendelsesmuligheder.

Under henvisning til persondatalovens § 5, stk. 5, fandt Datatilsynet, at en ændring af sletningsfristen, hvorved en person, der ikke findes skyldig i et strafbart forhold, skal stå anført i registeret i en så lang periode, alene bør ske, hvis væsentlige samfundsmæssige hensyn tilsiger dette.

Datatilsynet anbefalede således, at det nøje overvejes, om en så markant ændring af sletningsreglerne er saglig og nødvendig set i forhold til de formål, man ønsker at forfølge med registreringerne.

3. Lovforslagets § 1, nr. 6, gav adgang til fortsat at opbevare DNA-profiler af visse sporfund, selv om der er sket personidentifikation. Et personidentificeret sporfund skulle således fortsat kunne registreres, hvis personen ikke var eller havde været sigtet for den pågældende forbrydelse, og vedkommende samtykkede i fortsat registrering. Var personen afgået ved døden – f.eks. et drabsoffer – krævedes der i sagens natur ikke samtykke.

I de almindelige bemærkninger til lovforslaget var bl.a. anført, at det vil være en betydelig lettelse i efterforskningsarbejdet at opbevare personidentificerede DNA-profiler fra ofre i spordelen. Formålet hermed var at gøre det muligt for politiet at benytte de automatiserede søgefunktioner i DNA-profilregisteret til hurtigt at søge nye sporfund op imod et offers DNA-profil. Denne mulighed kan have stor praktisk betydning, hvis der f.eks. findes blodpletter eller andre biologiske spor, som måske stammer fra offeret, i en mulig gerningsmands hjem.

Den foreslåede bestemmelse rejste efter Datatilsynets vurdering spørgsmål om, hvorvidt det i bestemmelsen forudsatte samtykke fra den registrerede skal leve op til persondatalovens krav til et samtykke, jf. persondatalovens § 3, nr. 8.

Datatilsynet henledte samtidig opmærksomheden på, at den registrerede til enhver tid kan tilbagekalde et samtykke i henhold til persondatalovens § 38. Tilsynet forudsatte ud fra det foreliggende, at denne bestemmelse også skal finde anvendelse i forhold til de registreringer i DNA-profilregisteret, der baserer sig på samtykke.

For så vidt angår afdøde personer, bemærkede Datatilsynet, at oplysninger om afdøde i en vis udstrækning anses for personoplysninger omfattet af persondataloven.

Det var Datatilsynets umiddelbare vurdering, at registrering (uden samtykke) – i hvert fald i en vis periode – er nødvendig for politiets varetagelse af sine opgaver på det strafferetlige område og således ligger inden for rammerne af persondatalovens § 7, stk. 6, og § 8, stk. 1.

4. I medfør af § 6 i den gældende lov om oprettelse af et centralt DNA-profilregister har en registreret person adgang til mundtligt at modtage underretning om de oplysninger, der er registreret om den pågældende. Det foreliggende lovforslag åbnede ikke op for en ændring af denne bestemmelse, men spørgsmålet om en eventuel revision af bestemmelsen blev behandlet i Strafferetsplejerådets udtalelse.

Datatilsynet henledte opmærksomheden på, at de registrerede tillige har ret til indsigt i DNA-profilregisteret efter persondatalovens § 31. Ifølge persondatalovens § 34, stk. 1, skal meddelelser i henhold til § 31, stk. 1, på begæring gives skriftligt.

Datatilsynet anbefalede, at det i forbindelse med lovforslagets behandling blev afklaret, om – og i givet fald i hvilket omfang – lovforslaget tilsigtede at fravige persondatalovens indsigtsregler.

5. I forlængelse af det under punkt 3 og 4 anførte gjorde Datatilsynet opmærksom på, at tilsynet lægger til grund, at persondatalovens regler, f.eks. om tilsyns- og inspektionsadgang, i øvrigt finder anvendelse på DNA-profilregisteret. Det blev i den forbindelse bemærket, at DNA-profilregisteret er anmeldt til Datatilsynet.

6. I de almindelige bemærkninger til lovforslaget var bl.a. anført, at DNA-profilregisteret alene indeholder de talprofiler, der er resultatet af DNA-analyse af biologisk materiale fra henholdsvis sporfund og prøver udtaget ved legemsundersøgelse i medfør af retsplejelovens kapitel 72. Registeret omfatter således ikke det bagvedliggende biologiske materiale.

Det fremgik endvidere, at Retsgenetisk Afdeling ved Retsmedicinsk Institut på Københavns Universitet i 1990 indgik en aftale med Rigspolitichefen om at udføre alle DNA-analyser til brug for straffesager. Den hidtidige praktiske ordning for håndteringen af disse prøver er beskrevet nærmere i bemærkningerne til DNA-profilregisterloven, jf. Folketingstidende 1999-2000, tillæg A, side 3047-3048. Heraf fremgår det bl.a., at det biologiske materiale fra legemsindgreb – typisk blodprøver – som analyseres på politiets anmodning, opbevares på Retsgenetisk Afdeling, der som udgangspunkt destruerer materialet 12 måneder efter analysens foretagelse. Ønsker politiet af bevismæssige årsager, at det biologiske materiale opbevares af Retsgenetisk Afdeling i længere tid, skal politiet fremsætte en begrundet anmodning herom.

Datatilsynet gentog i den forbindelse, at det er Datatilsynet vurdering, at det omtalte bagvedliggende biologiske materiale er omfattet af persondataloven som et manuelt register, jf. lovens § 1, stk. 1.

7. I lovforslaget var det oplyst, at Rigsadvokaten i 1999 nedsatte en arbejdsgruppe, der har til opgave at overveje, hvilke retningslinier der kan fastsættes for opbevaring, destruktion mv. af biologisk materiale, som er tilvejebragt ved legemsindgreb, og som kan anvendes i forbindelse med efterforskningen af straffesager. Rigsadvokatens arbejdsgruppe skal bl.a. komme med forslag til retningslinier for Retsgenetisk Afdelings opbevaring og destruktion af prøver udtaget ved legemsundersøgelse til brug for DNA-analyse. Arbejdsgruppen forventedes at afgive sin rapport med forslag til sådanne retningslinier i 2004.

Da behandlingen af det biologiske materiale som anført må anses for omfattet af persondataloven, anmodede Datatilsynet om at blive orienteret om det omtalte arbejde, og tilsynet anmodede endvidere om at blive hørt, inden retningslinierne fastsættes.

8. Datatilsynet henledte afslutningsvis opmærksomheden på, at anvendelse af det biologiske materiale til forskning kræver anmeldelse til og udtalelse fra Datatilsynet, hvis oplysninger, der er bundet i det biologiske materiale, kan henføres til enkeltpersoner.

Ny pligtafleveringslov

Kulturministeriet anmodede Datatilsynet om en udtalelse om udkast til forslag til en ny pligtafleveringslov.

Hovedformålet med lovforslaget var ifølge forarbejderne at bringe lovgivningen om pligtaflevering i overensstemmelse med den teknologiske udvikling og samle lovgivningen om pligtaflevering i én lov. Pligtafleveringsloven skulle ifølge lovforslaget omfatte film, radio- og tv-programmer og alt dansk internetmateriale.

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

1. Indledningsvis bemærkede Datatilsynet, at den bevarelse af kulturarv, som lovforslaget skulle skabe grundlag for, må betragtes som en opgave i samfundets interesse.

Med loven tilvejebringes en hjemmel til at indsamle materiale fra internetsider, der er beskyttede med adgangskoder (lukkede net-sider), i det omfang sådant materiale ud fra en fortolkning af ophavsretslovens definition i § 2, stk. 3 og 4, må anses for "gjort tilgængeligt for offentligheden". På baggrund af, at rækkevidden af dette begreb i forhold til lukkede net-sider kan give anledning til en vis

tvivl, henstillede Datatilsynet, at der i bemærkningerne til lovforslaget redegøres nærmere for, hvilke typer af private og offentlige web-sites mv. der vil blive indhøstet.

Efter Datatilsynets opfattelse skulle loven i vidt omfang varetage de samme hensyn, som varetages ved arkivlovgivningen.

Til forskel fra den foreslåede ordning indeholder arkivlovgivningen imidlertid frister for, hvornår oplysninger må gøres tilgængelige, samt retningslinier for adgangen til ikke umiddelbart tilgængelige arkivalier og for benyttelsen af arkivalierne.

Sådanne frister for tilgængelighed gør det mindre betænkeligt at opbevare navnlig følsomme oplysninger med henblik på videregivelse.

På den baggrund pegede Datatilsynet på muligheden for, at der i forhold til i hvert fald sådanne oplysninger anvendes tilgængelighedsfrister af den karakter, der findes i arkivlovgivningen

2. Herudover bemærkede Datatilsynet, at indsamlingen af materiale fra internettet vil udgøre behandling omfattet af persondataloven, i det omfang der indsamles personoplysninger.

Tilsynet understregede i den forbindelse, at der ved "personoplysninger" i persondataloven forstås enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).

Pligtafleveringsinstitutionernes videre opbevaring og videregivelse af det indsamlede materiale vil ligeledes udgøre behandlinger omfattet af persondataloven, i det omfang der indgår personoplysninger.

3. Persondataloven sondrer mellem forskellige kategorier af oplysninger. Følsomme oplysninger, andre følsomme oplysninger og almindelige oplysninger. Der er forskellige behandlingsregler alt afhængig af, hvilken kategori af oplysninger der er tale om.

Hjemlen til indsamling og registrering i de to pligtafleveringsinstitutioner

Det var Datatilsynets opfattelse, at den påtænkte indsamling og registrering vil medføre behandling af såvel følsomme oplysninger omfattet af persondatalovens §§ 7 og 8 som almindelige oplysninger omfattet af lovens § 6.

Almindelige oplysninger omfattet af persondatalovens § 6 og følsomme oplysninger omfattet af persondatalovens § 8

Det følger af persondatalovens § 6, stk. 1, nr. 5, at behandling kan ske, hvis det er nødvendigt af hensyn til udførelsen af en opgave i samfundets interesse. Af bemærkningerne til persondataloven fremgår, at der med udtrykket opgave i samfundets interesse følger, at der skal være tale om opgaver af almen interesse, dvs. opgaver, som er af betydning for en bredere kreds af personer. Dette vil bl.a. være tilfældet, for så vidt angår behandling i statistisk, historisk eller videnskabeligt øjemed.

Det følger desuden af persondatalovens § 6, stk. 1, nr. 6, at behandling kan ske, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt.

For så vidt angår oplysninger omfattet af persondatalovens § 8, følger det af bestemmelsens stk. 1, at der for den offentlige forvaltning ikke må behandles oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver.

Det var Datatilsynets opfattelse, at bevarelse af den kulturarv, som formidles i elektroniske kommunikationsnet, er en opgave i samfundets interesse og en opgave, som ved den påtænkte lovgivning henlægges til de to pligtafleveringsinstitutioner.

En indsamling og registrering af oplysninger omfattet af § 6, stk. 1, og § 8, stk. 1, som er offentliggjort, ville efter Datatilsynets opfattelse kunne ske inden for persondatalovens rammer.

Datatilsynet noterede sig i den forbindelse, at der kun indsamles offentliggjort materiale, samt at det i bemærkningerne var anført, at offentliggørelse forstås som i ophavsretsloven, jf. denne lovs § 8, stk. 1, hvorefter et værk anses for offentliggjort, når det lovligt er gjort tilgængeligt for almenheden.

Ifølge bemærkningerne til lovforslaget skelnes der mellem åbent og lukket offentliggjort materiale. Åbent materiale er ifølge bemærkningerne alt materiale, der er frit tilgængeligt for enhver bruger uden nogen form for modydelser. Lukket offentliggjort materiale er materiale, hvortil der er knyttet krav om modydelser fra brugeren, f.eks. krav om betaling eller om, at man skal identificere sig.

Datatilsynet bemærkede i tilknytning hertil, at hvis der er tale om oplysninger, der kun er tilgængelige for modtagere, der skal opfylde særlige vilkår, vil der efter Datatilsynets opfattelse ikke efter persondataloven uden videre kunne ske indsamling og registrering. F.eks. fandt Datatilsynet, at oplysninger i et kreditoplysningsbureaus registre, der kun er tilgængelige for abonnenter, som kun må

foretage opslag, hvis nærmere vilkår er opfyldt, ikke kan siges at være offentliggjort.

Datatilsynet henledte herudover opmærksomheden på, at begrænsningen af adgangen til oplysninger på lukkede net-sider i visse tilfælde er begrundet i, at persondataloven er til hinder for, at oplysningerne gøres offentligt tilgængelige.

F.eks. har Datatilsynet udtalt, at videregivelse af medlemsoplysninger fra en forening i form af offentliggørelse på det åbne internet kræver det enkelte medlems samtykke.[7] Videregivelse af medlemslister på lukkede sider på internettet er i Datatilsynets praksis blevet ligestillet med videregivelse i et foreningsblad mv. under forudsætning af, at det f.eks. ved hjælp af password eller lignende sikres, at kun medlemmer har adgang til den pågældende side.

Det var derfor Datatilsynets opfattelse, at lukkede sider, hvor adgangen er begrænset til en begrænset kreds, f.eks. til en forenings medlemmer, og som indeholder personoplysninger, der kun må være tilgængelige for denne begrænsede kreds, ikke bør anses for offentliggjort materiale.

Følsomme oplysninger omfattet af persondatalovens § 7

Efter persondatalovens § 7, stk. 1, må oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold som udgangspunkt ikke behandles.

I lovens § 7, stk. 2-7, findes der dog en række undtagelser herfra.

Behandling af de nævnte oplysninger kan således finde sted, hvis den registrerede har givet sit udtrykkelige samtykke til behandlingen, jf. § 7, stk. 2, nr. 1. Et samtykke skal opfylde de betingelser, som fremgår af persondatalovens § 3, nr. 8. Ved samtykke forstås herefter enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Efter Datatilsynets opfattelse kan den omstændighed, at oplysningerne findes på internet, ikke generelt tages som udtryk for, at der foreligger samtykke til offentliggørelsen fra de personer, der indgår oplysninger om. Tilsynet har – desværre – erfaring for, at der også offentliggøres oplysninger, herunder følsomme oplysninger, uden iagttagelse af persondatalovens samtykkekrav. En del offent-

7 Datatilsynet er af den opfattelse, at medlemskab af en forening, uanset at denne måtte være en ukontroversiel – f.eks. en sportsforening – er en privat sag. Tilsynet har yderligere lagt vægt på, at der vil være en risiko for, at medlemsoplysningerne vil blive (mis)brugt til uvedkommende formål, f.eks. markedsføring. Offentliggørelse af en oplysning om en persons medlemskab kræver derfor det enkelte medlems samtykke. Se værd at vide-tekst om "Foreningers behandling af personoplysninger" på www.datatilsynet.dk.

liggørelser er desuden fritaget fra lovens krav som følge af de undtagelser, der f.eks. gælder for medierne.

I de tilfælde, hvor der rent faktisk måtte være afgivet et samtykke til offentliggørelsen, vil dette samtykke ikke uden videre kunne antages at omfatte efterfølgende høstning, selv om personer, der indvilger i, at oplysninger om dem offentliggøres på internet, bør gøre sig klart, at oplysningerne vil kunne indsamles af søgemaskiner mv. Det var derfor Datatilsynets opfattelse, at et samtykke til indsamling og registrering i pligtafleveringsinstitutionerne skal være udtrykkeligt og specifikt, jf. herved også persondatalovens krav til et samtykke.

Det var således Datatilsynets opfattelse, at samtykke i praksis ikke vil kunne anvendes som behandlingshjemmel for pligtinstitutionernes indsamling og registrering.

Bestemmelsen i § 7, stk. 1, gælder endvidere ikke, såfremt behandlingen vedrører oplysninger, som er blevet offentliggjort af den registrerede, jf. § 7, stk. 2, nr. 3. Ifølge forarbejderne er denne bestemmelses tidsmæssige udstrækning begrænset til det tidspunkt, hvor den oplysning, der ønskes behandlet, er offentliggjort af den registrerede. Det er dermed ikke tilstrækkeligt, at den dataansvarlige er bekendt med, at visse personoplysninger er bestemt til offentliggørelse. Offentliggørelse i bestemmelsens forstand foreligger, hvis oplysningerne er bragt til kundskab hos en bredere kreds af personer. Dette vil f.eks. være tilfældet, hvis oplysningerne viderebringes gennem tv, aviser og lignende landsdækkende medier. Også andre former for videregivelse af oplysninger vil kunne anses for offentliggørelse i bestemmelsens forstand. Det er en betingelse, at oplysningerne er offentliggjort på den registreredes foranledning. Oplysninger, som andre, f.eks. pressen, af egen drift har offentliggjort, er således ikke omfattet.

Det var Datatilsynets opfattelse, at denne bestemmelse ikke vil kunne udgøre hjemlen for pligtinstitutionernes indsamling og opbevaring af oplysninger, efter at de er fjernet fra de hjemmesider, hvorfra de er indsamlet.

Hertil kommer, at der findes følsomme oplysninger på internettet, som ikke er offentliggjort af den registrerede selv, og hvor den nævnte bestemmelse ikke vil kunne være behandlingsgrundlaget.

Samlet set var det således Datatilsynets vurdering, at den omstændighed, at oplysninger er offentliggjort på internettet, ikke medfører, at man derfra kan slutte, at den registrerede selv har offentliggjort oplysningerne, jf. § 7, stk. 2, nr. 3.

Datatilsynet noterede sig også, at det fremgik af de almindelige bemærkninger i udkastet til lovfor-slaget, at det ikke kan udelukkes, at der også kan blive ind-

samlet følsomme oplysninger, (jf. persondatalovens §§ 7, stk. 1, og 8), som ikke er offentliggjort ved den registreredes foranstaltning.

Det var endvidere Datatilsynets vurdering, at der ikke i øvrigt er hjemmel i andre undtagelser i § 7 til den i lovforslaget beskrevne indsamling og registrering. Indsamling og registrering af oplysninger omfattet af persondatalovens § 7 vil således alene kunne ske, såfremt persondataloven fraviges.

Mulighederne for at fravige persondataloven

Af persondatalovens § 2, stk. 1, følger, at regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven. Ifølge persondatalovens forarbejder følger det omvendt af bestemmelsen, at persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling. Dette gælder dog ikke, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod direktivet om behandling af personoplysninger

Da lovforslaget ikke undtager følsomme oplysninger omfattet af persondatalovens § 7 fra indsamlingen og registreringen, og da dette formentlig ikke er teknisk muligt, måtte Datatilsynet gå ud fra, at det med lovforslaget var tilsigtet at skabe hjemmel til indsamling og registrering, der ikke vil kunne ske efter persondataloven.

Datatilsynets henstillede, at det præciseres i lovforslaget, om det er tilsigtet at skabe en dårligere retsstilling for de registrerede end efter persondataloven.

Datatilsynet henstillede endvidere, at Kulturministeriet foretager en vurdering af den ønskede retstilstand i forhold til databeskyttelsesdirektivet, herunder navnlig artikel 8 om de særligt følsomme oplysninger.

I den forbindelse foreslog Datatilsynet, at Kulturministeriet i lovforslagets bemærkninger beskriver, hvilke tilstrækkelige garantier der gives i forbindelse med, at der etableres en mulighed for at indsamle og registrere oplysninger i strid med det forbud, der er udgangspunktet i direktivets artikel 8, stk. 1.

Samtidig gjorde Datatilsynet opmærksom på, at undtagelser fra direktivets artikel 8, stk. 1, som omhandlet i stk. 4 skal meddeles til Kommissionen, jf. artikel 8, stk. 6.

Videregivelse

Det fremgik af lovforslagets § 19, stk. 3, at det pligtafleverede kun gøres tilgængeligt for almenheden, for så vidt adgangen til materialet ikke er begrænset i medfør af anden lovgivning. I bemærkningerne til bestemmelsen nævnes straffeloven og persondataloven som eksempler på sådan anden lovgivning.

De indsamlede oplysninger vil således alene kunne videregives, i det omfang dette er muligt efter reglerne i persondatalovens kapitel 4.

Det stod ikke Datatilsynet klart, hvordan videregivelsen vil blive tilrettelagt, så persondataloven overholdes. Datatilsynet pegede derfor på, at der i persondataloven ligger følgende begrænsninger:

For almindelige (ikke-følsomme) oplysninger vil det være persondatalovens § 6, stk. 1, nr. 1-7, der sætter grænserne.

Oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte vil kunne videregives i det omfang, en af betingelserne i persondatalovens § 8, stk. 2, er opfyldt.

Oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold må efter persondatalovens § 7, stk. 1, ikke behandles, herunder videregives.

§ 7, stk. 2-7, indeholder undtagelserne fra det generelle forbud mod videregivelse.

4. Behandling af personoplysninger skal tillige ske i overensstemmelse med de grundlæggende principper, som er indeholdt i lovens § 5.

Herudover skal den dataansvarlige efter persondatalovens § 37, stk. 1, berigtige, slette eller blokere oplysninger, der viser sig urigtige eller vildledende eller på lignende måde er behandlet i strid med lov eller bestemmelser udstedt i medfør af lov, hvis en registreret person fremsætter anmodning herom.

Formålet med indsamlingen efter det foreliggende lovforslag måtte antages at medføre, at disse regler i persondataloven næppe vil kunne anvendes på samme måde som for anden databehandling.

På den baggrund foreslog Datatilsynet, at Kulturministeriet overvejer, på hvilke måder de grundlæggende krav til databehandlingen i databeskyttelsesdirektivet

kan opfyldes. I den forbindelse henviste Datatilsynet til muligheden for at indføre tilgængelighedsfrister.

5. Det følger af persondatalovens § 29, stk. 1, at det påhviler 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 en række oplysninger, således at den registrerede kan varetage sine interesser. Det følger af bestemmelsens stk. 3, at oplysningspligten i stk. 1 ikke gælder, hvis underretning af den registrerede vil være umulig eller uforholdsmæssigt vanskelig.

Det fremgik af bemærkningerne til lovforslaget, at Kulturministeriet antog, at den foreslåede indsamling ved høstning vil være omfattet af undtagelsesbestemmelsen i § 29, stk. 3.

Datatilsynet var umiddelbart enig med Kulturministeriet i, at det ved brede høstninger af internetsider vil være uforholdsmæssigt vanskeligt for ikke at sige umuligt at informere alle de personer, der registreres oplysninger om. Imidlertid fandt Datatilsynet ikke at kunne udelukke, at der i specielle situationer kan påhvile den dataansvarlige en oplysningspligt over for personer, der behandles oplysninger om.

Herudover foreslog Datatilsynet, at brug af oplysningskampagner eller andre kompensatoriske foranstaltninger overvejes.

Datatilsynet påpegede, at persondatalovens øvrige regler om de registreredes rettigheder finder anvendelse, herunder om de registrerede personers ret til indsigt i oplysninger om dem selv.

6. Persondataloven indeholder i kapitel 12 regler om anmeldelse af behandlinger, der foretages for den offentlige forvaltning.

Som hovedregel skal enhver behandling af personoplysninger, som omfattes af loven, anmeldes til Datatilsynet, inden behandlingen iværksættes.

En række behandlinger skal dog ikke anmeldes til Datatilsynet. Dette gælder først og fremmest behandlinger, der ikke omfatter fortrolige oplysninger.

Omvendt er det en betingelse for iværksættelse af visse behandlinger, at de ikke alene anmeldes, men at Datatilsynet tillige afgiver udtalelse inden iværksættelsen. Dette gælder bl.a. for behandlinger, der omfatter følsomme oplysninger.

Det var Datatilsynets opfattelse, at den omstændighed, at oplysningerne indsamles via internet, ikke medfører, at de derved mister deres karakter af følsomme og fortrolige oplysninger.

Pligtafleveringsinstitutionerne er således omfattet af anmeldelsespligten og skal efter persondatalovens § 45, stk.1, nr. 1, indhente en udtalelse fra Datatilsynet, inden indsamlingen påbegyndes.

Det skal i den forbindelse afklares, hvem der er dataansvarlig for behandlingen. Det var Datatilsynets umiddelbare vurdering, at der vil ske behandling i begge de to pligtinstitutioner, og at disse hver især er ansvarlige for de oplysninger, som de indsamler, registrerer og i øvrigt behandler.

Pligtafleveringsinstitutionerne er som en del af den offentlige forvaltning underlagt såvel persondatalovens generelle krav om datasikkerhed i lovens kapitel 11 som de nærmere bestemmelser herom, der er fastsat i sikkerhedsbekendtgørelsen.

De anmeldelsespligtige dele af behandlingerne, det vil groft sagt sige behandlingen af de fortrolige og følsomme oplysninger, der indgår, er underlagt de skærpede sikkerhedskrav i sikkerhedsbekendtgørelsens kapitel 3. Dette betyder bl.a., at der skal ske logning som beskrevet i sikkerhedsbekendtgørelsens § 19.

Lov om indhentelse af børneattester

Kulturministeriet anmodede om Datatilsynets bemærkninger til udkast til lov om indhentelse af børneattester.

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

1. Lovforslaget indebar, at der på de enkelte områder vil blive fastsat nærmere regler om, at offentlige myndigheder og private foreninger skal foranledige, at der indhentes en såkaldt børneattest, inden der sker ansættelse mv. af personer, der som led i udførelsen af deres opgaver skal have direkte kontakt med børn under 15 år.

Indførelsen af en pligt til at indhente en børneattest inden ansættelse af personer, der som led i deres opgaver skal have direkte kontakt med børn under 15 år, måtte antages at indebære en markant stigning i antallet af indhentede børneattester.

Efter Datatilsynets opfattelse rejste lovforslaget spørgsmål i relation til såvel persondatalovens bestemmelser som databeskyttelsesdirektivet, som ligger til grund for persondataloven.

Persondatalovens § 5 og databeskyttelsesdirektivets artikel 6 indeholder grundprincipper, som skal være opfyldt ved enhver behandling af personoplysninger.

Efter Datatilsynets opfattelse gav det anledning til alvorlige overvejelser i forhold til principperne i § 5 om saglighed, rimelighed og proportionalitet at indføre en pligt til at indhente børneattester på en meget omfattende kreds af personer, uden at der i det enkelte tilfælde skal foretages en konkret vurdering af nødvendigheden heraf.

Ud fra hensynet til privatlivets fred og i lyset af databeskyttelsesretlige principper om saglighed og proportionalitet, jf. persondatalovens § 5, fandt Datatilsynet endvidere, at det måtte give anledning til bekymring, at oplysninger om alvorlige strafbare forhold spredes til et stort antal private organisationer, foreninger mv., hvorved en meget bred kreds af personer i princippet vil få adgang til disse oplysninger. Personkredsen vil ofte være uden praktisk erfaring med den måde, hvorpå fortrolige oplysninger skal behandles.

Det var derfor Datatilsynets opfattelse, at gennemførelsen af en sådan helt generel pligt til at indhente børneattester på så stor en kreds af personer kun bør ske, hvis vægtige samfundsmæssige hensyn taler herfor.

Datatilsynet fandt, at det i sidste ende må bero på en politisk vurdering af de modsatrettede hensyn, om man finder det nødvendigt at gennemføre forslaget.

Datatilsynet fandt det endvidere betænkeligt, at en betydelig mængde data videregives til og opbevares i mange foreninger mv. En sådan ophobning af data bør søges undgået. Datatilsynet henviste i den forbindelse til det grundlæggende databeskyttelsesprincip i persondatalovens § 5, stk. 3.

2. Vedrørende indhentelse af børneattesterne noterede Datatilsynet sig, at det fremgik af lovforslaget, at indhentelse af børneattester sker på grundlag af et skriftligt samtykke.

Datatilsynet forudsatte, at samtykket lever op til kravene i persondatalovens § 3, nr. 8.

Datatilsynet påpegede i den forbindelse vigtigheden af, at samtykket indeholder udførlig information om, hvilke oplysninger der indhentes fra Kriminalregisteret, herunder at oplysninger indhentes fra Kriminalregisterets efterforskningsdel, at oplysningerne videregives til den rekvirerende myndighed, forening mv., og at den registrerede kan få meddelelse om, hvilke oplysninger der er videregivet.

Datatilsynet bemærkede, at tilsynet i overensstemmelse med sin hidtidige praksis ikke fandt, at det forhold, at der alene kan opnås ansættelse, hvis den

registrerede giver samtykke til indhentelse af børneattest, i sig selv medfører, at samtykket ikke kan anses for frivilligt.

3. Som ovenfor anført fandt Datatilsynet, at lovforslaget måtte antages at indebære en markant stigning i antallet af indhentede børneattester og en stor spredning af oplysningerne. Dette rejste efter tilsynets opfattelse væsentlige spørgsmål vedrørende modtagerens behandling af oplysningerne.

Datatilsynet gik ikke ud fra, at lovforslaget tilsigtede at regulere modtagerens behandling af eventuelle oplysninger om strafbare forhold[8], som den pågældende har fået gennem indhentelse af børneattester.

Datatilsynet måtte gå ud fra, at den enkelte modtager normalt opbevarer svarene fra Rigspolitichefen systematisk. Datatilsynet gik desuden ud fra, at svarene, også i de tilfælde, hvor der ikke er tilførsler på børneattesten, indeholder oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden. Der indgår således bl.a. oplysninger om personnummer.

Såfremt svarene opbevares i ringbind, der er systematiserede, f.eks. efter dato eller navn, vil der efter Datatilsynets umiddelbare opfattelse være tale om et manuelt register omfattet af persondatalovens § 1, stk. 1.

Modtagernes behandling, herunder opbevaring og eventuelle videre brug af de børneattester, som de modtager, skal således ske under iagttagelse af persondataloven.

Persondatalovens kapitel 4, herunder dels de generelle betingelser i lovens § 5, jf. ovenfor, dels de specifikke regler for forskellige typer af oplysninger, skal tages i betragtning.

I forbindelse med indhentelse af børneattester vil der blive behandlet oplysninger om seksuelle forhold omfattet af persondatalovens § 7, om strafbare forhold omfattet af persondatalovens § 8, om personnumre omfattet af lovens § 11 og almindelige (ikke-følsomme) personoplysninger omfattet af lovens § 6.

Oplysning om, at der ikke er registreringer på børneattesten, er omfattet af persondatalovens § 6 om almindelige (ikke-følsomme) oplysninger. Behandling af denne oplysning skal ske under iagttagelse af persondatalovens § 6, stk. 1, nr. 1-7.

I de tilfælde, hvor der er pligt til at indhente en børneattest, vil modtagelsen af attesten være nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, jf. § 6, stk. 1, nr. 3. Til dokumentation af, at forpligtelsen

8 Datatilsynet har efterfølgende præciseret, at der også er tale om behandling af oplysninger om seksuelle forhold.

er opfyldt, vil den dataansvarlige tillige efter § 6, stk. 1, nr. 3, kunne opbevare (registrere) Rigspolitichefens svar i en periode, som dog ikke må være længere, end hvad der er nødvendigt formålet med opbevaringen taget i betragtning, jf. persondatalovens § 5, stk. 5.

Offentlige myndigheder kan i henhold til persondatalovens § 11, stk. 1, behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer.

Af persondatalovens § 11, stk. 2, følger, at private må behandle oplysninger om personnummer, når det følger af lov eller bestemmelser fastsat i henhold til lov, den registrerede har givet sit udtrykkelige samtykke hertil, eller behandlingen alene finder sted til videnskabelige eller statistiske formål, eller hvis der er tale om videregivelse af oplysninger om personnummer, når videregivelsen er et naturligt led i den normale drift af virksomheder mv. af den pågældende art, og når videregivelsen er af afgørende betydning for at sikre en entydig identifikation af den registrerede, eller videregivelsen kræves af en offentlig myndighed.

Efter Datatilsynets opfattelse vil de *private foreninger mv.* i forbindelse med indhentelse af børneattester alene kunne indhente og registrere oplysninger om personnumre, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Samtykket skal opfylde kravene i persondatalovens § 3, nr. 8.

Efter Datatilsynets opfattelse vil en *offentlig myndighed* kunne behandle, herunder opbevare, Rigspolitichefens svar i medfør af persondatalovens § 8, stk. 1.

For så vidt *angår private* dataansvarlige fandt Datatilsynet, at der ved indhentelse af samtykket til at indhente børneattesten bør anvendes en samtykkeerklæring, der også omfatter den videre opbevaring.

4. Vedrørende anmeldelsespligten udtalte Datatilsynet, at efter tilsynets opfattelse indhentes børneattester med henblik på at behandle oplysninger om seksuelle og strafbare forhold. Der vil således efter tilsynets opfattelse ikke være tale om, at følsomme oplysninger af tilfældige årsager optræder.

Det var derfor Datatilsynets opfattelse, at *offentlige myndigheder*, der indhenter børneattester og opbevarer svarene i et manuelt register, f.eks. i et ringbind, efter persondatalovens kapitel 12 har pligt til at foretage anmeldelse til Datatilsynet samt pligt til at indhente tilsynets forudgående udtalelse efter § 45, stk. 1, nr. 1.

De *private modtageres* indsamling og opbevaring af redegørelserne fra Rigspolitichefen om tilførsler omfattet af § 36 vil indebære behandling af følsomme oplysninger. Det var Datatilsynets opfattelse, at private dataansvarlige, der

indhenter børneattester, må siges at *have til hensigt* at foretage behandling af oplysninger om seksuelle og strafbare forhold.

Det var således Datatilsynets opfattelse, at de *private modtagere* vil være omfattet af persondatalovens pligt til at foretage anmeldelse til og indhente forudgående tilladelse fra Datatilsynet, jf. persondatalovens § 50, stk. 1, nr. 1.

Navnlig under hensyn til, at det må antages at blive i et meget lille antal tilfælde, at der rent faktisk videregives oplysninger om strafbare forhold som følge af ordningen, overvejede Datatilsynet, om ordningen kan omfattes af en af undtagelserne fra anmeldelses- og tilladelseskravet, som er fastsat i persondatalovens § 49 og bekendtgørelsen om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig[9]. Datatilsynet fandt imidlertid ikke, at der er mulighed herfor.

Datatilsynet gjorde samtidig opmærksom på, at anmeldelser fra et så stort antal private organisationer, foreninger mv., som lovforslaget omfatter, vil medføre en sådan ekstraordinær belastning for Datatilsynet, at tilsynet ikke vil kunne overkomme opgaven inden for de nuværende ressourcemæssige rammer. Datatilsynet fandt det endvidere klart uholdbart, hvis anmeldelsespligten ikke i et rimeligt omfang kan følges op af inspektioner. Datatilsynet måtte derfor tage forbehold for at stille krav om tilførsel af yderligere ressourcer som følge af lovforslaget. Det var således ikke rigtigt, når Kulturministeriet om de negative økonomiske konsekvenser alene anførte, at "der vil være begrænsede udgifter forbundet med at indhente børneattester".

Hvis Kulturministeriet ønskede at overveje muligheden for at undtage modtagernes behandling helt eller delvist fra anmeldelsesordningen, gjorde Datatilsynet opmærksom på bestemmelserne i databeskyttelsesdirektivets artikel 8, stk. 5, artikel 18 samt artikel 20, som må tages i betragtning.

I forhold til Kulturministeriets vurdering heraf understregede Datatilsynet vigtigheden af, at der etableres sikkerhedsgarantier for at imødegå de særlige risici, som Datatilsynet fandt, at der er ved den påtænkte ordning.

Efter afgivelsen af høringssvaret anmodede Kulturministeriet om Datatilsynets bemærkninger til et revideret udkast til forslag til lov om indhentelse af børneattester.

Datatilsynets udtalelse hertil gengives i alt væsentligt nedenfor.

9 Bekendtgørelse nr. 543 af 15. juni 2000.

1. Datatilsynet noterede sig det anførte om forholdet til persondataloven, herunder Kulturministeriets overvejelser om baggrunden for at fastsætte en konkret undtagelse til persondatalovens regler om anmeldelsespligt.

Sammenholdt med det anførte i de specielle bemærkninger til forslaget, herunder navnlig forudsætningerne om, at der ved den nærmere udmøntning af ordningen tages særlige forholdsregler med henblik på at sikre, at indhentede oplysninger ikke behandles i strid med persondataloven, havde Datatilsynet ikke grundlag for at antage, at den påtænkte ordning vil være i strid med databeskyttelsesdirektivet.

2. Det var i de almindelige bemærkninger anført, at: "*Datatilsynet har fået forelagt et revideret lovudkast på basis af ovenstående betragtninger samt lovforslagets § 4 og bemærkningerne hertil og har givet sin tilslutning til forslaget*."

Datatilsynet anmodede om, at formuleringen om Datatilsynets tilslutning til forslaget udgik. Datatilsynet henviste i den forbindelse til, at tilsynet efter persondatalovens § 57 alene afgiver en udtalelse om forholdet til persondatabeskyttelseslovgivningen. Det må imidlertid bero på en politisk vurdering, om der foreligger sådanne tungtvejende samfundsmæssige interesser, at den påtænkte ordning bør gennemføres. Datatilsynet henviste til sin første udtalelse og fandt ikke at burde udtale sig nærmere herom.

3. Af udkastet fremgik, at myndigheder og private fysiske og juridiske personer, som indhenter børneattester på grundlag af regler udstedt i medfør af § 2, stk. 1 og 2, ikke af denne grund skal foretage anmeldelse til eller indhente udtalelse fra Datatilsynet i henhold til persondatalovens kapitel 12 eller 13.

Det var Datatilsynets opfattelse, at det bør præciseres, at der, for så vidt angår private dataansvarlige, er tale om en egentlig tilladelsesordning, jf. persondatalovens § 50.

4. Datatilsynet noterede sig endvidere, at det af de særlige bemærkninger til lovforslagets § 4 fremgik, at "*Under hensyntagen til databeskyttelsesdirektivet, navnlig art. 8, stk. 5, og artikel 18 og 20 forudsættes, at lovændringen følges op af mere præcis information i form af en vejledning fra Rigspolitiet til modtagerne, når positive børneattester udstedes. Vejledningen udarbejdes af Datatilsynet og vedlægges børneattesterne. Det skal fremgå af vejledningen, at attesten straks efter modtagelsen bør destrueres, medmindre andre regler, fx på det ansættelses- og forvaltningsretlige område, kræver opbevaring af attesten, og i så fald kun i det omfang, sådanne regler kræver det. Når det gælder private foreninger mv., skal attesten som hovedregel destrueres straks. Vejledningen skal også omhandle den videre opbevaring af børneattester med henblik på at sikre, at attesterne ikke behandles i strid med persondataloven. Når der udstedes en positiv*

børneattest, skal Rigspolitiet anmode den modtagende myndighed, institution, forening mv. om at udpege en person, der har ansvaret for beskyttelsen af personoplysningerne i børneattesten inden for rammerne af persondataloven og databeskyttelsesdirektivet."

Datatilsynet anførte, at det ikke er muligt for Datatilsynet at påtage sig at udarbejde den omtalte vejledning. Formuleringen herom henstilledes derfor ændret. Tilsynet anmodede imidlertid om at få forelagt et udkast til vejledning, jf. persondatalovens § 57.

5. Det fremgik ligeledes af de særlige bemærkninger til forslaget, at "*Datatilsynet i medfør af persondatalovens § 55, stk. 1, kan føre tilsyn med, at behandlingen af børneattester sker i overensstemmelse med persondataloven. Det kan eksempelvis ske i form af stikprøvekontrol*".

Datatilsynet bemærkede hertil, at når Kulturministeriet ønsker at fravige anmeldelsesordningen i henhold til persondatalovens kapitel 12 og 13, vil dette være ensbetydende med, at Datatilsynet ikke har kompetence til at foretage inspektion. På den baggrund anmodede Datatilsynet om, at passagen i de særlige bemærkninger om Datatilsynets inspektionsmulighed udgik af forslaget.

Internationalt arbejde

Indledning

Som beskrevet i tidligere årsberetninger, senest i Datatilsynets Årsberetning for 2003, 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 links 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 OECD's 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 omfattede 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 2004. 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 180).

Ikrafttræden: Den 1. februar 1990 i Danmark.

Efter sammenlægningen i 2003 af Den Rådgivende Komité T-PD (Consultative Committee T-PD) og Databeskyttelsesekspertgruppen (CJ-PD) på grund af manglende økonomiske ressourcer har T-PD fortsat CJ-PD's arbejde med behandling af personoplysninger ved brug af biometriske data. T-PD's drøftelser vedrørende biometri er beskrevet i en statusrapport (progress report), som kan ses på Europarådets hjemmeside. T-PD har i 2004 endvidere beskæftiget sig med spørgsmålet om "Application of Data Protection Principles to the Internet". Drøftelserne skal danne grundlag for T-PD's fremtidige arbejde i relation til behandling af personoplysninger på internet.

T-PD 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 2004 har 28 lande underskrevet tillægsprotokollen, heraf har 8 lande ratificeret protokollen.

Europarådets hjemmeside kan findes via et 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 tidspunk-

tet for lovens ikrafttræden. Ved bekendtgørelse nr. 508 af 23. juni 1999 er det fastsat, at loven træder i kraft den 1. juli 1999. Loven er senere ændret ved lov nr. 1435 af 22. december 2004.

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 2004 afholdt 4 møder, hvor man bl.a. har behandlet spørgsmål, som vedrører oprettelse af nye analysedatabaser (se konventionens artikel 10 og artikel 12) og relationerne til Europol.

Det Fælles Klageudvalg har i 2004 afholdt 5 møder. Klageudvalget afgjorde bl.a. sin tredje klagesag i september og modtog i september 2 nye klager.

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. opfyl-

des 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. Loven er senere ændret ved lov nr. 227 af 2. april 2003 og lov nr. 448 af 9 september 2004.

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 2004 afholdt 5 møder. Tilsynsmyndigheden har bl.a. fortsat drøftelserne om myndighedens fremtidige arbejde set i lyset af et kommende SIS II-system. I den forbindelse har Den Fælles Tilsynsmyndighed afgivet en udtalelse angående SIS II. Udtalelsen "Opinion on SIS II Developments" kan findes på Datatilsynets hjemmeside samt på Den Fælles Tilsynsmyndigheds hjemmeside, http://www.schengen-JSA.dataprotection.org. Tilsynsmyndighedens hjemmeside er endnu ikke tilgængelig på dansk.

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 2004 blev der afholdt 3 møder i den fælles tilsynsmyndighed, hvor man bl.a. drøftede den fælles tilsynsmyndigheds arbejdsopgaver og 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.

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 overensstem-

melse med Rådets afgørelse begyndte sekretariatet sit virke i september 2001. Sekretariatet ledes af en jurist med stor erfaring inden for databeskyttelse.

Fællesmøde for de fælles tilsyns/kontrolmyndigheder
I anledning af en anmodning fra det engelske House of Lords om en udtalelse angående EU anti-terror aktiviteter afholdt de fælles tilsyns/kontrolmyndigheder i 2004 for første gang fælles møder. Der blev i alt afholdt 3 fælles møder, hvor bl.a. anmodningen fra House of Lords blev drøftet. Møderne resulterede i vedtagelsen af en fælles udtalelse om databeskyttelse. House of Lords' rapport angående EU antiterror aktiviteter kan ses på det engelske parlaments hjemmeside, www.parliament.uk, eller ved at bruge følgende link: http://www.publications.parliament.uk/pa/ld200405/ldselect/ldeucom/53/53.pdf. Det forventes, at der vil blive afholdt flere fælles møder med henblik på at drøfte spørgsmål af tværgående interesse.

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 ophævedes 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 anvendelse af Dublin-konventionen (EF-Tidende Nr. L 316 af 15/12/2000, s. 1), vedtaget af EU-Rådet den 11. december 2000.

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

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

Formålet med Eurodac-forordningen er at fastlægge regler for oprettelse af en elektronisk database af fingeraftryk af asylansøgere og visse andre personer for at lette anvendelsen af Dublin-konventionen, 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 Eurodac-forordningens 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 den pågældende medlemsstats nationale ret overvåger, at den pågældende medlemsstats behandling af personoplysninger i overensstemmelse med Eurodac-forordningen, 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 Eurodac-forordningen.

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 [10]) er sekretariat for gruppen.

Artikel 29-gruppen har i 2004 afholdt 5 to dages-møder og 1 endagsmøde. Datatilsynet har endvidere deltaget i en underarbejdsgruppe, "Internet Task Force", som særligt arbejder med beskyttelse af personoplysninger i forbindelse med anvendelse af internet og anden ny teknologi.

Artikel 29-gruppen har i 2004 vedtaget en række henstillinger, udtalelser mv.

Der er således vedtaget dokumenter om følgende:

- Udtalelse nr. 1/2004 om beskyttelsesniveauet i Australien i forbindelse med luftfartsselskabers overførsel af passageroplysninger (PNR) (WP 85)

- Arbejdsdokument om Trusted Computing Platforms og særligt om arbejdet udført af Trusted Computing Group (TCG group) (WP 86)

- Udtalelse nr. 2/2004 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger, der er indeholdt i flypassagerers PNR, som overføres til USA's told- og grænsekontrolmyndighed (Bureau of Customs and Border Protection (CBP)) (WP 87)

- Udtalelse nr. 3/2004 om tilstrækkeligheden af beskyttelsesniveauet i Canada i forbindelse med overførslen af Passenger Name Records og Advanced Passenger Information fra flyselskaber (WP 88)

- Udtalelse nr. 4/2004 om behandlingen af personoplysninger ved brug af videoovervågning (WP 89)

- Udtalelse nr. 5/2004 om uanmodet kommunikation med henblik på markedsføring, jf. artikel 13 i direktiv 2002/58/EF (WP 90)

- Arbejdsdokument om genetiske oplysninger (WP 91)

10 Ansvaret for området er i 2005 overført til GD Frihed, Sikkerhed og Retfærdighed.

- Artikel 29-gruppens arbejdsprogram for 2004 (WP 92)

- Fælles Erklæring som reaktion på terrorangrebene i Madrid (WP 93)

- Syvende årsberetning om situationen vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger og beskyttelse af privatlivets fred i Den Europæiske Union og i tredjelande for årene 2002 og 2003

- Udtalelse nr. 6/2004 om implementeringen af Kommissionens afgørelse af 14-V-2004 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger indeholdt i Passenger Name Records vedrørende flypassagerer, der overføres til USA's Bureau of Customs and Border Protection, og vedrørende aftalen mellem Det Europæiske Fællesskab og USA om behandlingen og overførslen af PNR-data af flyselskaber til USA's Department of Homeland Security, Bureau of Customs and Border Protection (WP 95)

- Udtalelse nr. 7/2004 om anvendelsen af biometriske elementer i opholdstilladelser og visum i lyset af oprettelsen af det Europæiske Visuminformationssystem (VIS) (WP 96)

- Udtalelse nr. 8/2004 om information til passagerer om overførsel af PNR-oplysninger vedrørende flyvninger mellem EU og USA (WP 97)

- Strategi-dokument (WP 98)

- Udtalelse nr. 9/2004 vedrørende udkast til rammeafgørelse om opbevaring af data behandlet og tilbageholdt med henblik på at yde elektroniske offentlige kommunikationsydelser eller data tilgængelige i offentlige kommunikationsnetværk med henblik på forebyggelse, efterforskning, opklaring og forfølgning af strafbare forhold, herunder terrorisme (WP 99)

- Udtalelse om mere harmoniserede bestemmelser om oplysningspligt (WP 100)

- Erklæring fra artikel 29-gruppen om retshåndhævelse (WP 101)

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" (EDPS) 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.

Datatilsynets hjemmeside indeholder en henvisning til hjemmesiden for den europæiske tilsynsførende for databeskyttelse, hvor dennes udtalelser mv. offentliggøres.

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. Forretningsordenen for Den Fælles Kontrolinstans blev vedtaget i 2004, og instansen har efterfølgende løbende afholdt møder.

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 2004 blev den årlige EU-datatilsynskonference afholdt i Rotterdam af det hollandske datatilsyn (College Bescherming Persoonsgegevens). På konferencen drøftedes en række spørgsmål af fælles interesse, bl.a. håndhævelse af databeskyttelseslovgivningen, forbedring af kommunikationen med omverdenen og problemstillinger vedrørende EU-samarbejdet inden for tredje søjle.

International konference for databeskyttelsesmyndigheder mv.

Det 26. årlige internationale møde for datatilsynsmyndighederne blev i september 2004 afholdt i Wroclaw, Polen, arrangeret af det polske datatilsyn. På konferencen blev der behandlet en række emner af fælles interesse, herunder bl.a. problemstillinger vedrørende automatisk softwareopdatering og et udkast fra ISO (International Organisation for Standardisation) til en databeskyttelsesstandard.

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 2004 stod det danske 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 håndhævelse og kontrol i forhold til persondatalovgivningen, rammerne for de nordiske tilsyns samarbejde, retten til anonym færdsel og offentlige myndigheders offentliggørelse af personoplysninger på hjemmesider.

I 2004 blev der endvidere afholdt Nordisk Teknikermøde i Helsinki og Nordisk Sagsbehandlermøde i Reykjavik. I Helsinki blev bl.a. spørgsmålene om RFID-teknologi, spyware, digitale signaturer, digital forvaltning, kontrol af medarbejdere, biometri og anonym færdsel i forhold til brug af mobiltelefoner diskuteret, mens der på det Nordiske Sagsbehandlermøde bl.a. blev drøftet fællesnordiske inspektioner, retten til anonym færdsel, kravene til et gyldigt samtykke, rammerne for det nordiske samarbejde og persondatalovens forhold til henholdsvis offentligheds-, forvaltnings- og arkivloven.

Sikkerhedsspørgsmål

Persondatalovens krav om datasikkerhed

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

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

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

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

OCES certifikater

Datatilsynet har igen i 2004 taget stilling til en række spørgsmål vedrørende OCES certifikater, herunder om sikkerhed ved OCES digital signatur, om netbank kunders erhvervelse af OCES digital signatur, om OCES signaturkataloget samt om ændring af OCES certifikatpolitik og alternative registreringsprocedurer. Nedenfor gengives enkelte af Datatilsynets udtalelser.

Sikkerhed ved OCES digital signatur

Datatilsynet blev via pressens omtale opmærksom på en sikkerhedsfejl ved den digitale signatur i forbindelse med flytning af et certifikat fra en pc til en anden og udbad sig derfor en redegørelse fra Videnskabsministeriet.

Videnskabsministeriet oplyste over for Datatilsynet, at brugere, der flyttede et certifikat uden at følge de givne vejledninger, kunne risikere at importere et certifikat, der ikke var beskyttet af en adgangskode.

Ministeriet oplyste endvidere, at TDC efter offentliggørelsen af sikkerhedsbristen havde iværksat en række afhjælpende foranstaltninger, herunder orientering af

alle brugere, vejledning i check af adgangskode på flyttede signaturer og endelig en teknisk opdatering af signaturer med sikring mod den pågældende fejl.

Datatilsynet udtalte bl.a., at det forhold, at en bruger kan kompromittere det sikkerhedsniveau, som er fastlagt i den samlede systemløsning, ved ikke at følge en given instruks, efter Datatilsynets opfattelse forringer sikkerheden ved anvendelsen af certifikatet. Der forelå derfor efter Datatilsynets opfattelse en sikkerhedsbrist, og risikoen ved og eventuelle konsekvenser heraf burde følgelig vurderes.

I den foreliggende situation opstod sikkerhedsbristen ved, at brugeren ikke fulgte den givne vejledning. Brugeren kunne selv konstatere et eventuelt problem ved den første anvendelse af en digital signatur efter en forkert flytning af denne, idet der i så fald ikke krævedes adgangskode ved aktivering af den digitale signatur.

Det var imidlertid Datatilsynets holdning, at det i en sådan situation bør overvejes, om sikkerheden kan øges ved teknisk at gennemtvinge, at brugerne følger en given vejledning.

Datatilsynet noterede sig, at der i dette tilfælde fandtes en teknisk mulighed for at øge sikkerheden, og at TDC nu havde implementeret denne. (Datatilsynets j.nr. 2004-632-0071)

Netbank kunders erhvervelse af OCES digital signatur

IT- og Telestyrelsen anmodede Datatilsynet om en udtalelse vedrørende et oplæg til registreringsprocedure i forbindelse med netbank kunders erhvervelse af OCES digital signatur.

Datatilsynet vurderede, at den beskrevne procedure opfyldte samme sikkerhedsniveau som de allerede godkendte verifikationsprocedurer i forbindelse med udstedelse af OCES certifikater. (Datatilsynets j.nr. 2004-721-0030)

OCES signaturkataloget

Datatilsynet blev via pressens omtale opmærksom på, at uvedkommende havde nem adgang til at høste e-post-adresser fra OCES signaturkataloget. Endvidere fremgik det af presseomtalen, at brugere, som havde bestilt et OCES certifikat, ikke var blevet gjort opmærksomme på, at deres navn og e-post-adresse ville blive offentliggjort i OCES signaturkataloget.

TDC oplyste over for Datatilsynet, at optagelsen i det offentligt tilgængelige katalog var en standardindstilling, som dog kunne fravælges. På grund af den offentlige debat omkring dette spørgsmål havde TDC foretaget ændringer i bestillingsformularen, således at det nu tydeligt fremgik, at brugerens accept også omfatter optagelse i en offentlig digital telefonbog med navn og e-mail-adresse, såfremt dette ikke fravælges under avancerede indstillinger.

Endvidere oplyste TDC, at der var gennemført en række tekniske foranstaltninger for at forhindre høst af e-post-adresser i signaturkataloget.

Datatilsynet tog denne redegørelse til efterretning med en konstatering af, at de gennemførte foranstaltninger gav væsentligt forbedret sikkerhed mod misbrug. (Datatilsynets j.nr. 2004-215-0182)

Alternative registrerings-procedurer

IT- og Telestyrelsen anmodede om Datatilsynets bemærkninger til et forslag til alternative registreringsprocedurer, hvorefter et medarbejdercertifikat og en centralt genereret nøgle udsendes på CD-kort til en ledelsesperson i en række virksomheder.

Datatilsynet foreslog yderligere sikkerhedsprocedurer, som efterfølgende er implementeret i den konkrete løsning. (Datatilsynets j.nr. 2004-321-0337)

Afgørelser vedrørende logning

I en række sager er Datatilsynet blevet stillet over for problemstillinger og fortolkningsspørgsmål i forhold til det krav om logning, som følger af sikkerhedsbekendtgørelsens § 19, og de mulige undtagelser hertil (Datatilsynets j.nr. 2004-329-0015).

Logning af e-post
Et e-post-system må kun indeholde følsomme eller fortrolige oplysninger, hvis adgang til sådanne oplysninger er begrænset til de brugere, som er autoriseret dertil.

Behandling af personoplysninger i e-mail systemer falder ind under undtagelsesbestemmelsen i § 19, stk. 2, i sikkerhedsbekendtgørelsen. Der skal således ikke foretages logning, hvis oplysningerne slettes efter en vis kortere periode, der generelt bør være af en størrelsesorden på højst en måned.

E-post-meddelelser kan gemmes i længere tid, hvis dette sker i et system, der opfylder logningskravet.

Logning af elektroniske kalendersystemer
Et kalendersystem må kun indeholde følsomme eller fortrolige oplysninger, hvis adgang til sådanne oplysninger er begrænset til de brugere, som er autoriseret dertil.

Behandling af personoplysninger i kalendersystemer falder ind under undtagelsesbestemmelsen i § 19, stk. 2, i sikkerhedsbekendtgørelsen. Der skal således ikke foretages logning, hvis oplysningerne slettes efter en vis kortere periode, der generelt bør være af en størrelsesorden på højst en måned efter gennemførelsen af den pågældende aktivitet.

Hvornår skal en "nærmere fastsat kortere frist" i § 19, stk. 2, regnes fra?
Den af den dataansvarlige myndighed nærmere fastsatte frist, som ifølge sikkerhedsvejledningen generelt bør være af en størrelsesorden på højst en måned, skal regnes fra det tidspunkt, hvor dokumentet er sendt til modtageren.

Opbevaring af personoplysninger på flytbare medier
Opbevaring af personoplysninger i digital form er en behandling og dermed omfattet af persondataloven.

En offentlig myndigheds opbevaring af personoplysninger på et flytbart medie er således underlagt sikkerhedsbekendtgørelsens bestemmelser. Imidlertid vil ikke alle bestemmelserne være meningsfyldte f.eks. vil autorisation og adgangskontrol i praksis være ensbetydende med fysisk sikring af lagringsmediet, hvilket der må tages højde for ved fastsættelsen af sikkerhedsforanstaltninger.

Såfremt et dokument, der foreligger i endelig form på diskette eller andet flytbart medie, genindlæses, påbegyndes der ikke i kraft af genindlæsningen en ny kortere periode, i hvilken dokumentet ikke er omfattet af et eventuelt logningskrav i henhold til persondataloven § 19, stk. 2. Dokumentet vil heller ikke kunne genindlæses og ajourføres under påberåbelse af, at det igen overgår til en status som et dokument, der ikke foreligger i endelig form.

Såfremt det færdige dokument indeholder følsomme eller fortrolige oplysninger, er mediet underlagt kapitel 1-3 i sikkerhedsbekendtgørelsen, og dokumentet må efter lagring på et flytbart medium og efter udløbet af den nærmere fastsatte kortere frist kun genindlæses i et system, som er i stand til at logge.

Logning af log
I visse situationer kræver Datatilsynet anmeldelse af systemer, som er baseret på en systemlog. Dette gælder f.eks. ved overvågning af medarbejderes brug af internet, der typisk er baseret på en log, som er en standardfunktion i en firewall. Det er i disse tilfælde ikke muligt at logge brugen af denne log, og Datatilsynet vil ikke kræve log af brugen af en systemlog, som normalt aktiveres af drifts- eller sikkerhedsmæssige grunde.

Det er Datatilsynets generelle holdning, at der ikke kan kræves logning af en log, eller mere populært sagt, at tilsynet ikke kræver kontrol af kontrollen. Adgangsret til en log vil endvidere normalt altid være forbeholdt en systemadministrator.

Kommunes offentliggørelse af personoplysninger

Udtalt, at en kommune ved en fejlagtig offentliggørelse af personoplysninger på kommunens hjemmeside ikke havde udvist den fornødne omhu, og at kommunen dermed ikke havde overholdt sikkerhedskravene i persondatalovens § 41, stk. 3 (Datatilsynets j.nr. 2004-632-0073)

Datatilsynet blev gennem omtale i dagspressen opmærksom på, at Sundsøre Kommune ved en fejl havde offentliggjort personoplysninger på kommunens hjemmeside, og anmodede derfor kommunen om en udtalelse.

Det fremgik af sagen, at der i august 2001 ved en menneskelig fejl på Sundsøre Kommunes hjemmeside blev offentliggjort oplysninger fra en lukket dagsorden i kommunens Personudvalg. Dagsordenen indeholdt oplysninger om afslag på kontanthjælp, revalidering og tvangsfjernelse af børn.

Som sagen var oplyst for Datatilsynet blev kommunen opmærksom på, at de pågældende oplysninger var offentligt tilgængelige i forbindelse med, at en borger – som i øvrigt var omtalt i dagsordenen – rettede henvendelse til kommunen.

Sundsøre Kommune fjernede herefter den pågældende dagsorden fra sin hjemmeside og i perioden fra den 19. til den 25. august 2004 forsøgte kommunen gentagne gange at få slettet cache-filer med dokumentet, således at dette ikke kunne findes ved en Google-søgning. Den 25. august 2004 meddelte "Google Team" Sundsøre Kommune, at hjemmesiden med den pågældende dagsorden kunne fjernes fra deres søgeresultater inden for en periode af 3 til 4 dage.

Sundsøre Kommune oplyste bl.a. over for Datatilsynet, at kommunen ville ændre dagsordensystemet således, at der ved fremtidige oprettelser af dagsordenspunkter skal tages stilling til, om et punkt er lukket eller åbent – med udgangspunkt i, at det er lukket. Derved sikres systemet mod bl.a. menneskelige fejl.

Datatilsynet udtalte, 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.

Bestemmelsen i persondatalovens § 41, stk. 3, indeholder således en forpligtelse for den dataansvarlige til at beskytte såvel følsomme oplysninger som fortrolige og almindelige ikke-følsomme oplysninger, ligesom den dataansvarlige skal sikre sig, at myndighedens systemer, organisation og arbejdsgange indrettes således, at kravene i § 41, stk. 3, efterleves.

En nærmere udmøntning af § 41, stk. 3, er bl.a. sket i sikkerhedsbekendtgørelsens § 6, hvoraf det følger, at den dataansvarlige myndighed skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne.

Det var Datatilsynet opfattelse, at en sikring af, at personoplysninger ikke uberettiget offentliggøres på en hjemmeside, er omfattet af den dataansvarliges forpligtelse efter lovens § 41, stk. 3.

Det var endvidere Datatilsynet opfattelse, at der navnlig i situationer, hvor der er en potentiel risiko for offentliggørelse af fortrolige og/eller følsomme personoplysninger, skal udvises særlig påpasselighed, både for så vidt angår tilrettelæggelsen af arbejdsgange, og for så vidt angår indretningen af myndighedens systemer.

I det konkrete tilfælde, hvor følsomme personoplysninger blev offentliggjort, fandt Datatilsynet ikke, at Sundsøre Kommune havde udvist den fornødne omhu, og kommunen havde dermed ikke overholdt kravene i persondatalovens § 41, stk. 3. Datatilsynet fandt det skete meget beklageligt. Tilsynet noterede sig imidlertid, at der var tale om en enkeltstående fejl, og at Sundsøre Kommune straks havde iværksat tiltag med henblik på at forebygge lignende fejl, herunder en ændring af kommunens dagsordensystem.

Datatilsynet noterede sig endvidere, at Sundsøre Kommune beklagede det passerede dybt, og at kommunen med det samme tog initiativ til at få slettet cachefiler med de pågældende oplysninger.

3 kommuners udlevering af skatteoplysninger

Udtalt, at kommuners udlevering af personoplysninger til uvedkommende alene på baggrund af oplysninger om personnumre er en overtrædelse af persondatalovens § 41, stk. 3 (Datatilsynets j.nr. 2004-632-0067, 2004-632-0068 og 2004-632-0069)

Datatilsynet blev gennem medieomtale opmærksom på, at 3 kommuner havde udleveret udskrifter af skatteoplysninger (R 75-oplysninger) til en journalist på baggrund af journalistens oplysning om en kollegas personnummer. Journalisten blev ikke afkrævet yderligere legitimation.

Datatilsynet anmodede de 3 kommuner om en udtalelse. Kommunerne bekræftede, at der var blevet udleveret personoplysninger som beskrevet, og oplyste, at der efterfølgende var blevet iværksat en række initiativer med henblik på at skærpe sikkerheden.

Datatilsynet henviste til, at persondatalovens § 41, stk. 3, stiller krav om, 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.

Nærmere regler om de i § 41, stk. 3, anførte sikkerhedsforanstaltninger er fastsat i Justitsministeriets sikkerhedsbekendtgørelse, som i § 5 stiller krav om, at den dataansvarlige myndighed skal fastsætte interne bestemmelser om sikkerhedsforanstaltninger i myndigheden. Af § 6 følger, at den dataansvarlige myndighed skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne.

Datatilsynet henviste endvidere til vejledningen til sikkerhedsbekendtgørelsen og til, at tilsynet har offentliggjort en række tekster om, hvad man må og ikke må, under punktet "Værd at vide", herunder "Sikkerhed ved udlevering af oplysninger", på tilsynets hjemmeside.

Spørgsmålet er desuden omtalt i Datatilsynets Vejledning om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger. Det fremgår således af vejledningens punkt 1.3., at den dataansvarlige – og en eventuel databehandler – skal sikre sig, at den, der meddeles oplysninger til, er rette person, så oplysninger om den registrerede ikke kommer til uvedkommendes kendskab. Der må kun udleveres oplysninger, når vedkommende har legitimeret sig behørigt, eller når der på anden måde er skabt sikkerhed for, at den, der f.eks. fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører.

Der gælder ikke specifikke regler for, hvorledes dette skal sikres, men sædvanlige legitimationspapirer, så som pas, kørekort eller ID-kort mv., vil kunne kræves forevist. Navnlig i forbindelse med udlevering af fortrolige oplysninger, herunder særligt oplysninger om rent private forhold (f.eks. oplysninger om strafbare forhold samt oplysninger om helbredsforhold og væsentlige sociale problemer), er det vigtigt at sikre, at oplysningerne ikke udleveres til uvedkommende.

Kravet om legitimation kan fraviges, når der på anden måde er skabt sikkerhed for, at den person, som f.eks. fremsætter en begæring om indsigt, er identisk med den person, oplysningerne vedrører. Herved tænkes navnlig på den situation, at den medarbejder hos den dataansvarlige, som modtager begæringen, i forvejen kender den person, der fremsætter begæringen.

Det er ikke tilstrækkelig legitimation, at en person ved personligt fremmøde eller ved telefonisk henvendelse er i stand til at oplyse en registreret persons personnummer. Her skal det på anden måde sikres, at den pågældende er identisk med den registrerede eller på andet grundlag, f.eks. en fuldmagt, har lovlig adkomst til oplysningerne. Det gælder med andre ord, at hverken offentlige myndigheder

eller private virksomheder mv. må basere sin datasikkerhed på personnummeret som en form for adgangskode (password).

Datatilsynet fandt, at kommunerne ved at udlevere personoplysninger til uvedkommende alene på baggrund af oplysninger om personnumre ikke i fornødent omfang havde sikret sig, at den, der meddeles oplysninger til, er rette person. Kommunerne havde derved overtrådt persondatalovens § 41, stk. 3, hvilket tilsynet fandt kritisabelt.

Da der efter Datatilsynets opfattelse var tale om en væsentlig overtrædelse af persondataloven, orienterede tilsynet de pågældende kommunalbestyrelser om sagen.

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 behandlinger administreres, eller oplysninger 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.

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

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

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

meldelsespligten 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.

Gennemførsel 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, drøftes.

Herefter gennemgås en række emner af generel karakter samt emner, som vurderes at være særligt 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
- TV-overvågning
- Kontrol af medarbejderes brug af internet og e-mail
- Elektronisk borgerbetjening og transmission af oplysninger via hjemmeside
- Hjemmearbejdspladser og mobile arbejdspladser
- Trådløse netværk

I efteråret 2004 valgte Datatilsynet i forbindelse med inspektioner hos offentlige myndigheder at lægge særlig vægt på et mere afgrænset antal af emner. Herved blev der tid til en mere grundig gennemgang og drøftelse af de enkelte emner. Følgende emner var valgt

- Den registreredes rettigheder
- Kontrol af logfiler
- Autorisationer – særligt i relation til ændringer som følge af kommunalreformen og brug af ESDH-systemer
- Sikkerhed – dokumentation og praksis

Efter gennemgang af relevante emner gennemgås ved de inspektioner hos offentlige myndigheder, hvor en af Datatilsynets teknikere deltager, 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 giver 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. Ved inspektioner, hvor der ikke deltager en tekniker, gives en mere summarisk feedback på de uddybende sikkerhedsregler, og der fokuseres i højere grad på andre emner end de rent teknisk-sikkerhedsmæssige.

Før en inspektion afsluttes, foretages en besigtigelse af lokaler, hvor personoplysninger behandles. Herunder kan der foretages diverse stikprøver i den dataansvarliges systemer. Den fysiske indretning gennemgås, og relevante spørgsmål drøftes med de medarbejdere, der behandler personoplysninger eller administrerer edb-udstyr.

Formålet med at foretage stikprøver og stille spørgsmål til konkrete medarbejdere er at undersøge, hvordan de regler og procedurer, som tilsynet har fået præsenteret mundtligt eller skriftligt, efterleves i praksis. Dette gøres f.eks. ved at undersøge automatiske funktioner, som styrer passwordkvalitet og udskiftningsfrekvens for passwords i edb-systemerne, og ved at undersøge dokumentation for administration af adgangskontrolsystemer og periodisk kontrol af autorisationer. Datatilsynet kan endvidere undersøge, om der findes tekstbehandlingsdokumenter o.l., som efter reglerne burde være slettet, ligesom man oftest gennemgår praksis for behandling af kasserede udskrifter og datamedier indeholdende personoplysninger.

Det har i forbindelse med inspektioner hos private dataansvarlige i flere år været praksis at afslutte inspektionssagen på stedet, når der under inspektionen ikke blev observeret forhold, der skulle undersøges nærmere eller bringes i orden, før sagen kunne afsluttes. Indtil efteråret 2004 har det været tilsynets praksis ved inspektioner hos offentlige myndigheder, at selve inspektionssagen først blev afsluttet formelt med et efterfølgende brev fra Datatilsynet til den dataansvarlige, også i tilfælde, hvor tilsynet ikke fandt noget at bemærke ved gennemførslen af inspektionen.

I efteråret 2004 benyttede tilsynet ved kommuneinspektioner forsøgsvis en procedure, som gør det muligt at afslutte en inspektion hos en offentlig myndighed på samme måde som hos private.

Efter den nye procedure gennemgår Datatilsynet mere indgående end hidtil sine observationer med den dataansvarlige myndighed, inden tilsynets repræsentan-

ter forlader stedet, og den dataansvarlige får udleveret en kopi af tilsynets noter. Selv om sagen ikke kan sluttes på stedet, kan udlevering af noterne bidrage til, at myndigheden med det samme kan få et bedre overblik over tilsynets observationer, og herunder hvilke forhold der skal undersøges nærmere eller bringes i orden.

Uanset at den nye procedure kun i en enkelt kommune – Sydthy Kommune – resulterede i, at inspektionen kunne afsluttes på stedet, er erfaringerne med den nye procedure lovende. Det er i den forbindelse Datatilsynets opfattelse, at muligheden for på stedet at afslutte en inspektionssag bl.a. bidrager til at reducere omfanget af – ikke kun Datatilsynets, men også den pågældende myndigheds – administration knyttet til en inspektion, hvilket er en klar ressourcemæssig fordel. Det er samtidig indtrykket, at effekten ved en inspektion forøges ved, at den inspicerede myndighed får tilsynets umiddelbare respons. Tilsynet planlægger derfor indtil videre at benytte den nye procedure over for kommuner og eventuelt også at tage samme praksis i brug over for andre offentlige myndigheder.

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.

Fokus på et geografisk område

Ved planlægningen af Datatilsynets inspektioner i 2004 fandt tilsynet, at området omkring Salling og Mors i forhold til landet som helhed havde haft et relativt lavt antal inspektioner siden persondatalovens ikrafttræden. Der blev derfor iværksat en koncentreret indsats i denne region.

Indsatsen bestod i, at tilsynet udstationerede seks medarbejdere på Mors i fire dage. Der blev i løbet af de fire dage gennemført inspektioner i 10 kommuner i området, hos Viborg Amtskommune, i 3 politikredse, ved 2 sygehuse samt hos en stillingsbesættende virksomhed – 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 og 2004 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.

Datatilsynets observationer ved inspektioner i 2004

Datatilsynets inspektioner har igen i 2004 været bredt fordelt over forskellige typer af private og offentlige dataansvarlige: Kommuner og amter, offentlige sygehuse, politiet, staten i øvrigt, private forskere, og øvrige private virksomheder – herunder private virksomheders personaleadministration, forsikringsselskaber og stillingsbesættende virksomheder (headhuntere). Tilsynet har endvidere foretaget inspektion hos en biobank og hos en virksomhed, der har anmeldt et advarselsregister.

I det følgende beskrives i store træk de observationer, som Datatilsynet har gjort i forbindelse med inspektionerne i 2004. 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 2004 er fortsat, at de dataansvarlige generelt 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.

Som omtalt i afsnittet om Datatilsynets virksomhed måtte tilsynet imidlertid i 2004 konstatere, at en særlig gruppe af dataansvarlige ikke har været tilstrækkeligt opmærksom på anmeldelsespligten, nemlig virksomheder, der driver erhvervsmæssig stillingsbesættende virksomhed.

Datatilsynet anmoder rutinemæssigt forud for en inspektion den dataansvarlige myndighed om at få tilsendt en oversigt over behandlinger af personoplysninger, som myndigheden har vurderet ikke at være anmeldelsespligtige. Formålet hermed er bl.a., at en sådan oversigt er velegnet som udgangspunkt for en drøftelse/vurdering af den dataansvarliges egen vurdering af de konkrete behandlinger. Oversigten kan endvidere være et nyttigt redskab for den dataansvarlige i tilfælde, hvor en registreret person anmoder om indsigt i de oplysninger, den dataansvarlige behandler om den pågældende. Som eksempler på behandlinger i denne kategori kan nævnes forskellige typer ventelister, udlånslister, visiteringslister, telefonlister, vagtplaner, fordelingslister o.l. Det er Datatilsynets erfaring, at en del dataansvarlige har vanskeligt ved at udarbejde en sådan oversigt.

På det private forskningsområde ses der eksempler på, at den dataansvarlige benytter en databehandler, som ikke er anført i anmeldelsen. En databehandler, som den ansvarlige forsker ofte overser, er Danmarks Statistik.

Opfyldelse af logningskrav og sletning af data

Tilsynet udførte under inspektionerne i 2004 en række kontroller af opslag i kriminalregisteret på politiets område og i systemer hos Told og Skat på det

kommunale område. Formålet var at undersøge baggrunden for de opslag, som brugerne havde foretaget i de centrale systemer. Tilsynet fandt herved ikke eksempler på opslag, som der ikke var en saglig og tjenstlig begrundelse for.

Datatilsynet måtte i en del tilfælde fremhæve kravet om at slette tekstbehandlingsdokumenter o.l., som indeholder fortrolige personoplysninger. Sådanne dokumenter skal slettes efter en vis kortere periode, såfremt de behandles i et system, som ikke er i stand til at logge efter sikkerhedsbekendtgørelsens regler herom. Tilsynet stødte jævnligt på eksempler på, at tekstbehandlingsdokumenter o.l. ikke var slettet i overensstemmelse med reglerne. Manglende sletning af tekstbehandlingsdokumenter ses på flere områder, men synes særligt at være et problem på sygehusområdet.

Oplysningspligt og indsigtsret
De fleste offentlige myndigheder er opmærksomme på reglerne på disse områder. På sygehusområdet er der dog fortsat 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.

Elektronisk borgerbetjening
De dataansvarlige myndigheder er tilsyneladende generelt opmærksomme på reglerne for transmission af personoplysninger over internettet. Det er endvidere tilsynets indtryk, at de løsninger, der benyttes til elektronisk borgerbetjening, ofte er leveret af leverandører, som er godt bekendt med reglerne på området.

Datatilsynet kræver, at der foretages kryptering ved transmission af personnumre og andre fortrolige oplysninger over internet. 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.

Uddybende sikkerhedsregler
Ved tilsynets inspektioner er det typiske billede fortsat, at de dataansvarlige følger god praksis i forhold til it-sikkerhed. Tilsynet kunne dog også i 2004 i flere tilfælde konstatere 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 sikker-

hedsregler skal således beskrive eller referere til beskrivelser af ansvarsforhold, etablerede sikkerhedsforanstaltninger, arbejdsgange osv.

Reglerne skal revideres mindst en gang om året for at sikre, at de er tidssvarende og i overensstemmelse med de faktiske forhold. Datatilsynet ser det som en stor fordel, at det af reglerne fremgår, hvem der har ansvar for denne gennemgang, hvilke terminer der er fastsat for gennemgangen, og at det endvidere tydeligt fremgår, hvornår reglerne senest er revideret.

Besigtigelse af fysisk sikkerhed
I Datatilsynets inspektioner indgår som regel altid en besigtigelse af publikumsområder, serverrum og arkiver, hvor der behandles eller opbevares 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 stadig eksempler på, 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.

På det private forskningsområde ses der i nogle tilfælde at være problemer omkring opbevaring af manuelt materiale i arkiver og lignende, hvor uvedkommende i forhold til projektet også har adgang. Uvedkommende i forhold til et projekt kan være øvrige ansatte på en sygehusafdeling, som huser et privat forskningsprojekt, der udføres af en ansat på afdelingen.

Inspektioner hos politiet

Som nævnt i Datatilsynets årsberetning for 2003, side 167, orienterede Datatilsynet i 2003 Rigspolitichefen om konstaterede problemer med manglende sletning af tekstbehandlingsdokumenter i en række kredse, hvor Datatilsynet havde konstateret, at der 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 i den forbindelse bl.a. peget på problemer forbundet med anvendelsen af POLSAS (Politiets Sagsbehandlingssystem).

Rigspolitichefen har efterfølgende iværksat løsninger på de tekniske problemer, som betingede behandling af oplysninger uden for POLSAS.

Det er tilsynets umiddelbare indtryk, at de iværksatte løsninger og øget opmærksomhed omkring reglerne på området i løbet af 2004 har afhjulpet de problemer

vedrørende behandling af tekstbehandlingsdokumenter, som tilsynet påpegede over for politiet i 2003.

I forbindelse med Datatilsynets gennemførelse af inspektioner ved to politikredse i 2003 drøftede tilsynet spørgsmål om behandling af data på flytbare medier og overholdelse af sikkerhedsbekendtgørelsens § 19, stk. 1.

Datatilsynet har i forbindelse med afslutningen af inspektionssagerne udtalt, at det er tilsynets vurdering, at elektronisk opbevaring af data på eksempelvis en cd-rom i sig selv er en behandling. Der er således i princippet ikke forskel på opbevaring af oplysninger på en harddisk (som ofte også er flytbar) eller på en diskette. Det er derfor Datatilsynets opfattelse, at behandling af personoplysninger også er omfattet af persondataloven, når oplysningerne er lagret på et flytbart medie, og at en offentlig myndigheds opbevaring af personoplysninger på et flytbart medie således skal opfylde sikkerhedsbekendtgørelsens bestemmelser.

Tilsynet udtalte endvidere, at det er Datatilsynets holdning, at der ikke i kraft af genindlæsning af et dokument, som foreligger i endelig form på diskette eller andet flytbart medie, påbegyndes en ny kortere periode, jf. sikkerhedsbekendtgørelsens § 19, stk. 2, i hvilken dokumentet er undtaget fra logningskravet i bekendtgørelsens stk. 1. Hvis det færdige dokument indeholder følsomme eller fortrolige oplysninger, er det Datatilsynets holdning, at mediet er underlagt kapitel 1-3 i sikkerhedsbekendtgørelsen, og dokumentet må efter lagring på et flytbart medium og efter udløbet af den nærmere fastsatte kortere frist kun genindlæses i et system, som er i stand til at foretage logning i overensstemmelse med sikkerhedsbekendtgørelsens § 19.

Datatilsynet har gjort Rigspolitichefen opmærksom på denne problemstilling og oplyst, at tilsynet vil drøfte problemstillingen i forbindelse med inspektionerne i 2005 i politikredsene.

Oversigt over udførte inspektioner i 2004

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 inspektion. Enkelte inspektionssager er endnu ikke færdigbehandlet.

Staten
AMU-center København
Teknisk Erhvervsskole Center
Ministeriet for Flygtninge, Indvandrere og Integration – departementet
Statsministeriets departement
Udenrigsministeriets departement
Undervisningsministeriets departement
Finansministeriets departement

Politimesteren i Glostrup
Politimesteren i Holbæk
Retsmedicinsk Institut
ATP
Politimesteren i Frederikssund
Rigspolitiet, Europol
Politimesteren i Løgstør
Politimesteren i Thisted
Politimesteren i Skive

Kommuner og amter

i Vordingborg Kommune
Maribo Kommune
Roskilde Amts institution Udsigten
Stevns Kommune
Gentofte Kommune
Allerød Kommune
Hvalsø Kommune
i Tølløse Kommune
i Fakse Kommune
Thisted Kommune
Møldrup Kommune
Aalestrup Kommune
Morsø Kommune
Løgstør Kommune
Sundsøre Kommune
Struer Kommune
Viborg Amtskommune
Sydthy Kommune
Lemvig Kommune
Thyholm Kommune

Offentlige Sygehuse

i Vestsjællands Amt
Sygehus Slagelse
Sygehus Kalundborg

i Frederiksborg Amt
Lemvig Sygehus
Sygehus Nord, Nykøbing-Thisted

Private forskere

Niels Thomas Hertel, Odense Universitetshospital/Syddansk Universitet
Christian Færgeman, Odense Universitetshospital/Syddansk Universitet

Ole Mogensen, Odense Universitetshospital/Syddansk Universitet
Niels Obel, Odense Universitetshospital/Syddansk Universitet
Inger Stenstrøm, Odense Universitetshospital/Syddansk Universitet
Annette Skærp Nielsen, Hvidovre
Signe Wildt, Hvidovre
Ulla Pallesen, Københavns Universitet
Hans Hvenegaard, CASA København
Pernille Harden, PLS Rambøll, København
Martin Krakhauer, Rigshospitalet
Peter Johannesen, Rigshospitalet
Mikkel Aastrup Nørreslet, Danmarks Farmaceutiske Universitet
Jill Mehlbye, AKF Amternes og kommunernes forskningsinstitut
Niels Tommerup, Panum Instituttet
Camilla Kragelund, Tandlægekolen, København

Øvrige private
E-boks
Industriens pensionsforsikring
PFA Forsikringsadministration
Russel Reynolds
Nykredit Livsforsikring
Skandia Livsforsikring A/S
Novo Nordisk A/S
Carlsberg Breweries A/S
Cryos ApS
Executec Consulting ApS
CV Management

Datatilsynet
Borgergade 28, 5.
1300 København K
Telefon: 3319 3200
Telefax: 3319 3218
Epost: dt@datatilsynet.dk
Hjemmeside: www.datatilsynet.dk