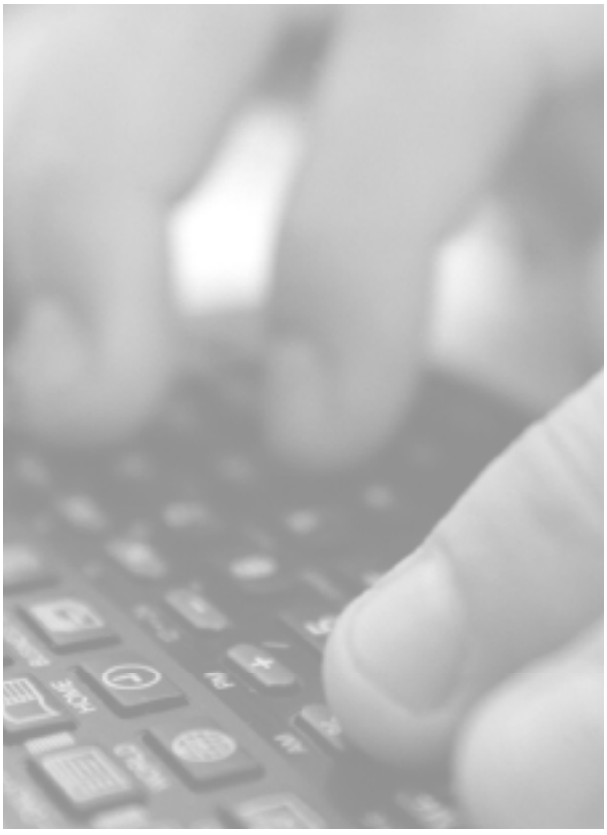
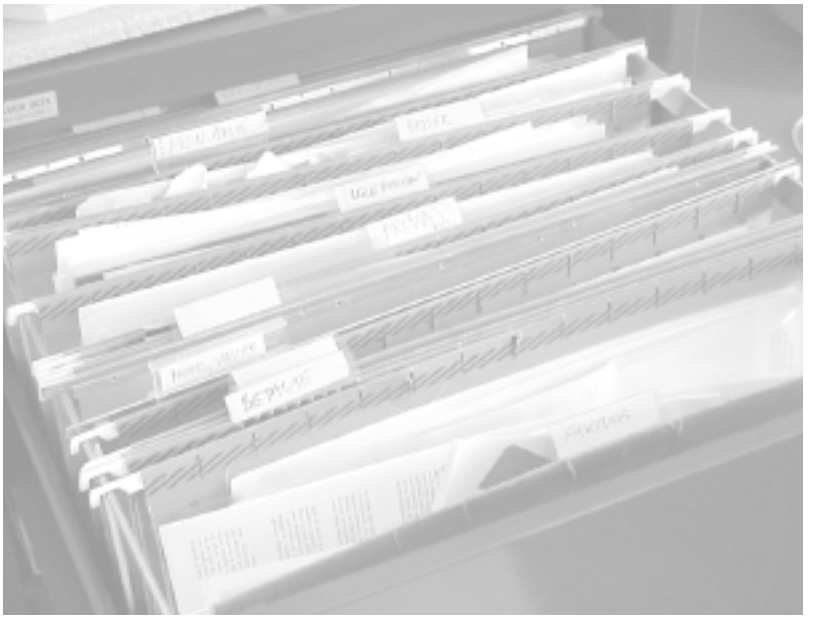


Datatilsynets årsberetning 2001

Udgiver: Datatilsynet
Design: Kontrast design
April 2002
ISSN nr: 1601-8281
ISBN nr: 87-601-9523-1



Indhold


Enter

Til Folketinget

Hermed afgiver Datatilsynet sin årsberetning for 2001.

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

Beretningen indeholder en beskrivelse af Datatilsynets aktiviteter i år 2001, herunder referater af en række principielle sager om behandling af personoplysninger.

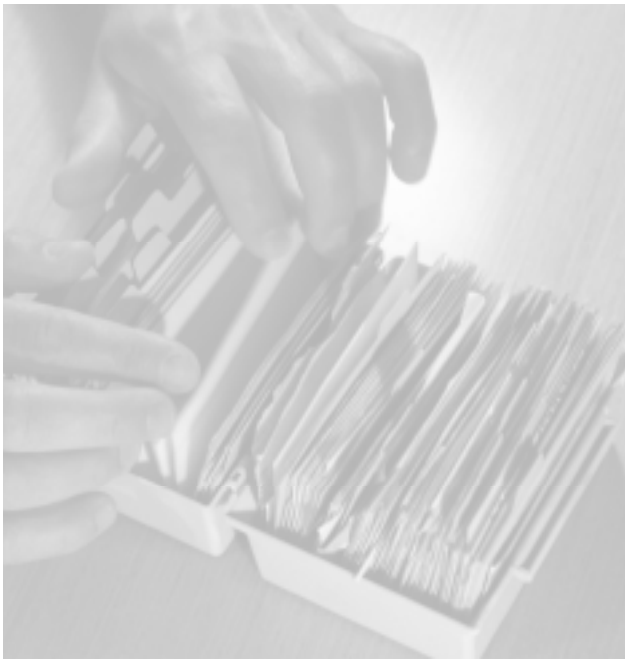
Hertil kommer et afsnit om det internationale arbejde, som Datatilsynet i årets løb har deltaget i, samt et afsnit om sikkerhedsspørgsmål, hvori de vigtigste aktiviteter på området vedrørende datasikkerhed omtales.

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

København, april 2002

Hugo Wendler Pedersen
Formand for Datarådet

Lena Andersen
Fg. Direktør



Datatilsynets virksomhed i år 2001

Datatilsynets virksomhed i 2001

Datatilsynets opgaver

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

Blandt Datatilsynets forskellige aktiviteter i 2001 kan nævnes:

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

På grund af persondatalovens overgangsordninger har sager om anmeldelser fra offentlige myndigheder og sager om tilladelse i forbindelse med anmeldelser fra private virksomheder og forskere udgjort den største del af tilsynets sagsmængde. Anmeldelserne omtales nærmere nedenfor i afsnittet "Anmeldelser fra myndigheder og virksomheder m.v.".

Datatilsynet har desuden afgivet udtalelser over udkast til bekendtgørelser, cirkulærer og lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger. Datatilsynet er også blevet hørt over lovforslag på dette område. I afsnittet "Udtalelser over lovforslag" omtales nogle af de udtalelser, tilsynet har afgivet i 2001.

Datatilsynets deltagelse i internationalt samarbejde er også et område, der har fået større og større omfang. Datatilsynet deltager blandt andet i samarbejdet i de fælles tilsynsmyndigheder nedsat i henhold til Schengen- og Europol-konventionerne, i Europarådets arbejde, og andre internationale arbejdsgrupper både på EU-niveau og verdensplan.

I løbet af 2001 kom der for alvor gang i inspektionsvirksomheden igen, idet Datatilsynet foretog i alt 76 inspektioner. Registertilsynet var på grund af den forestående lovændring tilbageholdende med inspektionerne i den sidste tid med registerlovene. Efter persondatalovens ikrafttræden den 1. juli 2000 startede Datatilsynet forsigtigt op, idet lovens overgangsordninger betød, at myndighederne m.v. endnu ikke behøvede at have alle anmeldelser efter persondataloven i orden.

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

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

Når andre myndigheder etablerer selvbetjeningssystemer på internet og lignende, yder Datatilsynet vejledning om, hvordan sikkerheden skal være for at beskytte oplysningerne. I forbindelse med en række initiativer til fremme af elektronisk borgerservice i det offentlige, har tilsynet påtaget sig opgaven som central godkendelsesinstans.

Datatilsynets organisation

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

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

Datarådet

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

Datarådets medlemmer

Pr. 31. december 2001

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

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

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

Sekretariatet

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

I forbindelse med persondatalovens gennemførelse har tilsynet ansat flere medarbejdere, blandt andet for at kunne behandle de mange anmeldelser, som Datatilsynet har modtaget. Hertil kommer nye opgaver for Datatilsynet i forbindelse med "Danmark på nettet", som omtales nedenfor.

Forøgelsen af antallet af medarbejdere havde den konsekvens, at tilsynet måtte flytte til andre lokaler, da det på sigt ikke ville være muligt at skaffe plads til alle i det gamle lejemål på Christians Brygge. Tilsynet flyttede derfor pr. 1. november 2001 til et større lejemål beliggende i Borgergade 28, 3.-6. sal, 1300 København K.

Ansatte i sekretariatet

Pr. 31. december 2001

Fg. direktør, cand. jur. Lena Andersen
Fg. kontorchef, cand. jur. Ole Hvilsom Larsen
IT-chef, civilingeniør Ib Alfred Larsen
Konsulent, cand. jur. Lotte Nyløkke Jørgensen
Konsulent, akademiingeniør Robert Hartmann Pedersen
IT-sikkerhedskonsulent Nils Rasmussen
Akademiingeniør Flemming Boysen, HD
Specialkonsulent, mag.art. Camilla Daasnes
Fuldmægtig, cand. jur. Bettina Vesterholm Agerskov
Fuldmægtig, cand. jur. Peter Rostgaard Ahleson
Fuldmægtig, cand. jur. Maiken Christensen Breüner
Fuldmægtig, cand. jur. Kira Kolby Christensen
Fuldmægtig, cand. jur. Lena B. Danvøgg
Fuldmægtig, cand. jur. Ditte Friis-Pedersen
Fuldmægtig, cand. jur. Anette Gramstrup
Fuldmægtig, cand. jur. Helene V. Grønfeldt
Fuldmægtig, cand. jur. Sameer Kohli
Fuldmægtig, cand. jur. Lene Engedal Kragelund
Fuldmægtig, cand. jur. Nana Kryger Larsen
Fuldmægtig, cand. jur. Jakob Lundsager
Fuldmægtig, cand. jur. Charlotte Edholm Mortensen (orlov)
Fuldmægtig, cand. jur. Ulla Østergaard Pedersen
Fuldmægtig, cand. jur. Lene Bang Petersen (orlov)
Fuldmægtig, cand. jur. Camilla Vinkel Voss (orlov)
Kontorfuldmægtig Kirsten Markussen
Kontorfuldmægtig Anne-Marie Müller
Kontorfuldmægtig Suzanne Stenkvist
Overassistent Pernille Jensen
Overassistent Mette Maj Leilund
Overassistent Berit Pedersen
Assistent Betina Have Krarup
Assistent Jette van der Loo
Kontorelev Irene Hesselberg
Stud. jur. Malene Lybæk Møller
Stud. jur. Maria Nymann
Stud. jur. Marie Gjesing Olesen
Stud. jur. Thomas Impgaard Sørensen

Persondataloven

Persondataloven (lov nr. 429 af 31. maj 2000) trådte i kraft den 1. juli 2000. Se Datatilsynets årsberetning 2000, side 8, om baggrunden for og forarbejderne til persondataloven.

Persondataloven er i 2001 blevet ændret ved lov nr. 280 af 25. april 2001. Lovændringen, der skete som følge af hæftestraffens afskaffelse, indebærer, at strafferammen efter lovens § 70 nu er bøde eller fængsel i indtil 4 måneder.

I tilknytning til persondataloven har Justitsministeriet udstedt en række bekendtgørelser. Herudover har Datatilsynet udsendt en række vejledninger i tilknytning til persondataloven.

Datatilsynet har i 2001 udsendt 2 nye vejledninger: Vejledning nr. 17 af 19. januar 2001 om offentlige myndigheders indberetning af skyldnere til kreditoplysningsbureauer og vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (i daglig tale kaldet sikkerhedsvejledningen).

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 også tilgængelige i elektronisk form.

Datatilsynet har også i 2001 løbende udarbejdet nye tekster og informationsmateriale, som er offentliggjort på hjemmesiden. Datatilsynet har herudover offentliggjort interessante og principielle afgørelser på hjemmesiden.

Enhver kan tegne elektronisk abonnement på Datatilsynets hjemmeside. Abonnenterne modtager automatisk en e-post, når hjemmesiden opdateres. Ved udgangen af marts 2002 var der i alt 2.408 abonnenter på Datatilsynets hjemmeside.

Anmeldelser fra myndigheder og virksomheder m.v.

Persondataloven indeholder regler om, at visse behandlinger af personoplysninger skal anmeldes til Datatilsynet. Nogle af behandlingerne skal tillige kontrolleres af Datatilsynet, inden de må sættes i værk. På Datatilsynets hjemmeside står der mere om, hvad der skal anmeldes til Datatilsynet.

Datatilsynet har udformet anmeldelsesskemaer til de forskellige typer af anmeldelser. Endvidere er der på Datatilsynets hjemmeside etableret mulighed for at indsende anmeldelser til Datatilsynet i elektronisk form.

De enkelte anmeldelser offentliggøres, når de er færdigbehandlet af Datatilsynet, i en særlig fortegnelse på hjemmesiden. Opslag i fortegnelsen kan foretages ved hjælp af enten en simpel eller en avanceret søgefunktion. Den avancerede søgefunktion giver mulighed for at søge på detaljerne i anmeldelserne, således at man f.eks. kan finde frem til alle anmeldelser, hvor der foretages kontrolsamkøring.

2001 har været præget af, at Datatilsynet har modtaget og behandlet et end- og meget betydeligt antal anmeldelser. I afsnittet "Statistiske oplysninger" findes nærmere oplysninger om antallet af Datatilsynets sager. Der er oprettet ikke mindre end 5.516 sager om anmeldelser fra offentlige myndigheder. Der er desuden modtaget anmeldelser fra den private sektor, hvor der er oprettet 1.565 sager, hvoraf 1.276 vedrører forskning og statistik. Hertil kommer ændringer til eksisterende anmeldelser, som Datatilsynet modtager stadig flere af, efterhånden som de faktiske forhold, der er beskrevet i anmeldelserne, ændrer sig.

En stor del af de anmeldelser, som tilsynet har modtaget i 2001, knytter sig til persondatalovens overgangsordninger for behandlinger, som var påbegyndt inden persondataloven trådte i kraft den 1. juli 2000. I den offentlige sektor skulle behandlinger, som var sat i værk før den 24. oktober 1998, således først opfylde anmeldelsespligten senest den 1. april 2001. Private forsknings- og statistikprojekter kunne fortsætte efter de hidtil gældende regler indtil den 1. oktober 2001, således at uafsluttede projekter først derefter skulle (gen)anmeldes til Datatilsynet.

Datatilsynet har prioriteret færdigbehandlingen af anmeldelserne højt, og dette har derfor lagt beslag på en stor del af Datatilsynets personalemæssige ressourcer. Det er i løbet af 1. kvartal 2002 lykkedes fra Datatilsynets side at få færdigbehandlet stort set alle de anmeldelser, som Datatilsynet har modtaget i 2001.

I Datatilsynets fortegnelse over anmeldte behandlinger var der ved udgangen af marts 2002 i alt 7.409 (færdigbehandlede) anmeldelser. Hertil kommer 1.089 anmeldelser, som beror på forskellige forhold, og som derfor befinder sig i tilsynets interne del af anmeldelsessystemet (backend).

Statistiske oplysninger

Oplysningerne i dette afsnit er baseret på registreringerne af nye sager i tilsynets journalsystem i 2001.

En del af tilsynets sagsbehandling er imidlertid fortsættelser til eksisterende sager. Dette er f.eks. tilfældet, når en anmeldelse ændres eller en tilladelse forlænges. Disse sager er af praktiske årsager ikke omfattet af statistikken.

Datatilsynet registrerede 8.727 nye sager i perioden 1. januar 2001 til 31. december 2001. Disse sager fordeler sig som følger:

Datatilsynets egen administration m.v.	185
Lovforberedende arbejde	66
Forespørgsler og klager vedrørende private	643
Forespørgsler og klager vedrørende offentlige myndigheder	386
Anmeldelser for den private sektor	1.565
Anmeldelser for den offentlige forvaltning	5.516
Sager på Datatilsynets eget initiativ	112
Sikkerhedsspørgsmål	50
Internationale sager	181
Kompetence i henhold til anden lovgivning	23

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

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 643 sager med forespørgsler og klager vedrørende private dataansvarlige.

Fordelingen mellem klager og forespørgsler var som følger:

Klager	ca. 64 %
Forespørgsler	ca. 36 %

Endvidere kan det oplyses, at i de afsluttede sager var ca. 43 % af klagerne berettigede, mens ca. 57 % var uberettigede.

Sagerne var fordelt på følgende virksomhedstyper:

Almindelige virksomheder	82
Den finansielle sektor	67
Fagforeninger, a-kasser, pensionskasser m.v.	20
Telesektoren	44
Foreninger og organisationer	55
Sundhedssektoren (medicinalvirksomheder, klinikker, læger m.v.)	23
Kreditoplysningsbureauer	81

Advarselsregistre	28
Stillingsbesættende virksomheder	4
Ansøgninger om tilladelser	123
Diverse	98
Sager af generel karakter	18

Forespørgsler og klager vedrørende offentlige myndigheder

Datatilsynet registrerede i alt 173 sager med forespørgsler og klager vedrørende offentlige myndigheder.

Fordelingen mellem klager og forespørgsler var som følger:

Klager:	ca. 51 %
Forespørgsler	ca. 49 %

I de afsluttede sager var ca. 11 % af klagerne berettigede, mens ca. 89 % var uberettigede.

Sagerne var fordelt således på følgende myndigheder:

Statslige myndigheder	157
Amtskommuner	25
Kommuner	94
Ansøgning om tilladelser	88
Diverse	15
Sager af generel karakter	7

Anmeldelser for den private sektor

Datatilsynet registrerede i alt 1.565 sager om anmeldelser. Sagerne var fordelt som følger:

Forskning og statistik	1.276
Privates behandling af oplysninger om rent private forhold	214
Advarselsregistre	10
Spærrelister	1
Kreditoplysningsbureauer	5
Stillingsbesættende virksomheder	32
Edb-servicebureauer	23
Diverse/sager af generel karakter	4

Anmeldelser for den offentlige forvaltning

Datatilsynet registrerede i alt 5.516 sager om anmeldelser. Sagerne var fordelt som følger:

Fællesanmeldelser	15
Kommuner	1.231
Amtskommuner	465
Statslige myndigheder	749
Tilslutninger til fællesanmeldelser fra kommuner	2.712
Tilslutninger til fællesanmeldelser fra amtskommuner	313
Tilslutninger til fællesanmeldelser fra statslige myndigheder	25
Diverse/sager af generel karakter	6

Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 112 sager oprettet på tilsynets eget initiativ. Sagerne var fordelt på følgende sagstyper som følger:

Inspektion og kontrol vedrørende private	53
Inspektion og kontrol vedrørende offentlige myndigheder	38
Sager rejst på grundlag af presseomtale og lignende	18
Diverse/sager af generel karakter	3

Sikkerhedsspørgsmål

Datatilsynet registrerede i alt 50 sager under kategorien sikkerhedsspørgsmål. Sagerne var fordelt som følger:

Sager vedrørende private	16
Sager vedrørende offentlige myndigheder	34

Internationale sager

Datatilsynet registrerede i alt 181 internationale sager. Sagerne var fordelt som følger:

Forespørgsler fra udlandet om dansk lovgivning	53
Nordisk tilsynssamarbejde	5
Europarådet	14
EU	40
Konventioner	46
Datakommissærsamarbejdet	11
OECD	1
Diverse/sager af generel karakter	11

Besparelser som følge af bevillingsreduktioner

I december 2001 blev der udmeldt en række budgettiltag vedrørende perioden 2002-2005. Datatilsynet er berørt af både de generelle bevillingsreduktioner af midlerne til offentlige myndigheder og de særlige besparelser på råd og nævn.

I forbindelse med udmeldingen om fordelingen af besparelserne på råd og nævn på Justitsministeriets område har Datatilsynet over for Justitsministeriet anført, at tilsynet finder det mindre naturligt at medtage tilsynet i oversigten over råd og nævn m.v. Det blev anført, at Datatilsynet ganske vist består af et sekretariat og et råd, men at tilsynet i praksis fungerer som en statslig styrelse. Efter Datatilsynets opfattelse ville de udmeldte besparelser ramme helt uforholdsmæssigt hårdt. Datatilsynet anførte endvidere, at der også er knyttet en række retssikkerhedsmæssige betænkeligheder til de foreslåede besparelser. Således må det befrygtes, at tilsynet vil være nødsaget til i betydeligt omfang at begrænse sin inspektionsvirksomhed og undlade at tage sager op af egen drift. Det kan desuden vise sig meget vanskeligt at gennemføre besparelserne uden at reducere medarbejderstaben drastisk.

Tilsynets andel i besparelserne vedrørende råd og nævnt blev reduceret i forhold til den oprindelige udmelding, men der er stadig tale om betydelige begrænsninger af tilsynets bevillinger i de kommende år.

For at kunne gennemføre besparelserne er der i tilsynet taget og vil fremover blive taget en række praktiske initiativer med henblik på at nedbringe ressourceforbruget. De pålagte besparelser vil imidlertid ikke kunne gennemføres uden at reducere medarbejderstaben.

Tilsynet er ikke selv herre over, hvor mange der klager, foretager anmeldelse til tilsynet eller rejser forespørgsler over for tilsynet. Besparelserne vil med et antal af disse sager svarende til sagstallet i de seneste år blandt andet give sig udslag i en længere sagsbehandlingstid.

Besparelserne vil tillige få konsekvenser med hensyn til, hvor mange sager – herunder navnlig inspektioner – der startes på tilsynets eget initiativ. På finanslovens virksomhedsoversigt for 2002 er antallet af inspektioner nedsat i forhold til det tidligere fremsatte finanslovsforslag for 2002. Antallet reduceres således fra 125 årlige inspektioner i årene 2002-2005 til 117 inspektioner i 2002, 90 inspektioner i 2003, 65 inspektioner i 2004 og endelig faldende til 40 inspektioner i 2005. Pligtbesparelsen på råd og nævn vil kunne gøre det nødvendigt at reducere antallet af inspektioner yderligere.

Udtalelser over lovforslag

Ændring af blandt andet straffeloven og retsplejeloven

Justitsministeriet anmodede Datatilsynet om en udtalelse om udkast til forslag til lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, udleveringsloven og lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN´s Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.).

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

1. Lovforslagets § 2, nr. 3, indeholdt forslag til en ny bemyndigelsesbestemmelse for justitsministeren til ved bekendtgørelse at fastsætte regler om den registrering og opbevaring (logning) af oplysninger om internet- og teletrafik til brug for efterforskning af strafbare forhold, som internetudbydere og teleselskaber skal foretage. Det fremgik af de almindelige bemærkninger til lovforslaget, at det nærmere indhold af en kommende bekendtgørelse i vidt omfang ville komme til at svare til den regulering, der var blevet foreslået i betænkning nr. 1377/1999 om børneporno og IT-efterforskning.

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven) § 5 indeholder en række grundlæggende databeskyttelsesretlige principper for den dataansvarliges behandling af oplysninger, som altid skal iagttages, selv om der i øvrigt måtte være hjemmel i persondatalovens øvrige behandlingsregler til at foretage behandlingen. Reglerne i persondatalovens § 5 følger mere eller mindre direkte af direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

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

Disse regler førte efter Datatilsynets opfattelse til, at internetudbydere og teleselskaber kun må behandle, herunder indsamle og registrere, oplysninger, som de selv har et aktuelt behov for af hensyn til varetagelse af deres egne (civile) formål. Selskaberne må også kun opbevare oplysningerne, så længe de selv har behov for dem af hensyn til varetagelse af deres egne (civile) formål, jf. persondatalovens § 5, stk. 5.

internetudbydere og teleselskaber kan således ikke i henhold til persondatalovens regler registrere og opbevare oplysninger alene med henblik på politiets retshåndhævelse, dvs. med den begrundelse, at politiet i efterforskningsmæssig sammenhæng kan få behov for dem.

En registrering og opbevaring med henblik på politiets retshåndhævelse kræver derfor en særskilt lovhjemmel. Ud fra hensynet til privatlivets fred var det Datatilsynets opfattelse, at en særskilt hjemmel til registrering og opbevaring af oplysninger i videre omfang end, hvad der følger af persondataloven, kun burde tilvejebringes, hvis vægtige samfundsmæssige hensyn talte herfor. Datatilsynet fandt ikke at burde udtale sig om, hvorvidt dette var tilfældet.

Hvis der pålagdes internetudbydere og teleselskaber en registrerings- og opbevaringspligt som omtalt i lovforslagets almindelige bemærkninger, var det Datatilsynets opfattelse, at opbevaringstiden skulle være så kort som muligt. Dette spørgsmål ville Datatilsynet eventuelt vende tilbage til i forbindelse med udfærdigelse af en bekendtgørelse, jf. herved nedenfor vedrørende persondatalovens § 57.

Der var tale om væsentlige indgreb i privatlivets fred, som i vidt omfang var båret af den særlig situation, som var opstået i forlængelse af terrorangrebene mod USA den 11. september 2001. Datatilsynet foreslog derfor, at der blev indsat en revisionsbestemmelse i lovforslaget - vedrørende både bemyndigelsesbestemmelsen og de bestemmelser, der udstedes i medfør heraf - med henblik på, at det på et senere tidspunkt ville blive genovervejet, om de foreslåede indgreb fortsat er nødvendige.

Datatilsynet henledte endvidere opmærksomheden på, at oplysningspligten i persondatalovens § 28 og § 29 som udgangspunkt skal iagttages i forbindelse med internetudbydernes og teleselskabernes indsamling af de omhandlede oplysninger om internet- og teletrafik. Datatilsynet kunne ikke på det foreliggende grundlag afgøre, om undtagelserne i lovens § 28, stk. 2, § 29, stk. 2 og 3, eller § 30 ville kunne finde anvendelse.

Endelig henledte Datatilsynet opmærksomheden på persondatalovens § 57, hvorefter der skal indhentes en udtalelse fra Datatilsynet i forbindelse med udfærdigelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger.

2. Lovforslagets § 3, nr. 2, åbnede for, at politiet kunne få direkte (online) adgang til forsyningspligtudbyderens database vedrørende den landsdækkende nummeroplysningstjeneste, herunder oplysninger om hemmelige og udeladte numre.

Datatilsynet fandt ikke, at den foreslåede ændring af lov om konkurrence- og forbrugerforhold på telemarkedet § 34, stk. 5, giver anledning til databeskyttelsesretlige betænkeligheder.

3. Lovforslagets § 2, nr. 5, indeholdt forslag til en ny bestemmelse i retsplejeloven om dataaflæsning. Den pågældende form for dataaflæsning ville kunne indebære indsamling af oplysninger om personer, der ikke er aktuelle i forbindelse med politiets efterforskning. Datatilsynet fandt, at en sådan skjult dataindsamling uden de berørte personers vidende vil indebære en vidtgående indgriben i privatlivets fred. Tilvejebringelse af regler herom bør kun ske, hvis vægtige samfundsmæssige hensyn taler herfor. Datatilsynet fandt ikke at burde udtale sig om, hvad denne afvejning burde føre til.

Datatilsynet bemærkede i øvrigt, at personoplysninger, som er tilvejebragt gennem strafprocessuelle tvangsindgreb, skal behandles i overensstemmelse med reglerne i persondataloven, hvis oplysningerne behandles ved hjælp af elektronisk databehandling eller indgår i et manuelt register.

Ændring af udlændingeloven

Indenrigsministeriet anmodede Datatilsynet om eventuelle bemærkninger til udkast til lov om ændring af udlændingeloven (Initiativer mod terrorisme m.v. – opfølgning på FN's Sikkerhedsråds resolution nr. 1373 af 28. september 2001 om bekæmpelse af terrorisme).

Lovforslaget rejste ud fra en databeskyttelsesretlig synsvinkel navnlig 3 problemstillinger.

Med henblik på blandt andet at skabe grundlag for at intensivere samarbejdet mellem udlændingemyndighederne, efterretningstjenesterne og anklagemyndigheden m.v. foresloges der indsat en række bestemmelser om udveksling af oplysninger myndighederne imellem i udlændingeloven.

Som led i bestræbelser på at bekæmpe terrorisme foresloges der endvidere en lempelse af reglerne om politiets adgang til at søge og videregive oplysninger fra blandt andet Det Centrale Fingeraftryksregister over Asylansøgere og Uidentificerede Udlændinge m.v. (B-filen) til brug for efterforskning af strafbare forhold og til brug for besvarelse af internationale efterlysninger.

Endelig foresloges en udvidelse af udlændingelovens regler om, hvilke udlændinge der skal indberettes til Schengen-informationssystemet (SIS) som uønskede.

Datatilsynet afgav udtalelse efter at have behandlet sagen Datarådet. Udtalelsen gengives i det følgende.

1. Udveksling af oplysninger mellem udlændingemyndighederne, efterretningstjenesterne og anklagemyndigheden

De foreslåede nye bestemmelser til udlændingelovens § 45 a og § 45 c fastsatte, at Udlændingestyrelsen, Indenrigsministeriet, Flygtningenævnet, statsamterne, de to efterretningstjenester samt anklagemyndigheden kunne udveksle oplysninger om udlændinge uden samtykke, og uden at der skulle foretages en konkret vurdering af hver enkelt oplysning for sig.

For så vidt angår udlændingemyndighedernes videregivelse af oplysninger til efterretningstjenesterne var det fastsat, at videregivelse kunne ske i det omfang, videregivelse kan have betydning for efterretningstjenesternes varetagelse af sikkerhedsmæssige opgaver (§ 45 a, stk. 1). Herudover var det fastsat, at videregivelse til anklagemyndigheden kunne ske med henblik på anklagemyndighedens beslutning om, hvorvidt der skal rejses tiltale for forbrydelser begået uden for Danmark (§ 45 c).

Efterretningstjenesternes videregivelse af oplysninger til udlændingemyndighederne kunne efter lovforslaget ske i det omfang, videregivelsen kan have betydning for udlændingemyndighedernes behandling af en sag efter udlændingelovens kapitel 1, 3 eller 4 (§ 45 a, stk. 2). Endelig kunne efterretningstjenesterne også udveksle oplysninger indbyrdes (§ 45 a, stk. 3).

§ 45 a, stk. 1 (og formentlig også stk. 2), indebar en væsentlig lempelse af betingelserne for videregivelse af oplysninger som nævnt i persondatalovens § 7, stk. 1, og § 8, stk. 1 og 2, navnlig derved at det ikke længere ville være nødvendigt at foretage en konkret vurdering af hver enkelt oplysning for sig.

Det var efter Datatilsynets opfattelse et politisk spørgsmål om og i givet fald, hvor meget videregivelsesbetingelserne på dette område skulle lempes i forhold til persondatalovens regler. Betingelsen om, at oplysningerne "kan have betydning" for efterretningstjenesternes varetagelse af sikkerhedsmæssige opgaver eller for udlændingemyndighedernes behandling af en sag efter udlændingelovens kapitel 1, 3 eller 4, måtte dog give anledning til betænkeligheder. Enhver oplysning kan efter omstændighederne have betydning for henholdsvis efterretningstjenesternes sikkerhedsmæssige opgaver og udlændingemyndighedernes behandling af en sag efter udlændingelovens kapitel 1, 3 eller 4.

Datatilsynet var opmærksom på, at det efter bemærkningerne til bestemmelsen er tanken at opstille objektivt konstaterbare kriterier for udlændingemyndighedernes videregivelse af oplysning til efterretningstjenesterne. Dette ville

imidlertid også kunne ske, selv om betingelserne for videregivelse skærpedes - også uden at det ville blive nødvendigt at foretage en konkret vurdering af hver enkelt oplysning.

Efter Datatilsynets opfattelse burde det overvejes at skærpe de foreslåede videregivelsesbetingelser, f.eks. således at videregivelse betingedes af, at der er en rimelig grund til at antage, at videregivelsen kan have betydning for henholdsvis efterretningstjenesternes varetagelse af sikkerhedsmæssige opgaver og udlændingemyndighedernes behandling af en sag efter udlændingelovens kapitel 1, 3 eller 4.

Persondataloven gælder ikke for behandlinger, der udføres for (af) politiets og forsvarets efterretningstjenester, jf. persondataloven § 2, stk. 11. Datatilsynet havde derfor ikke bemærkninger til § 45 a, stk. 3.

§ 45 c, hvorefter udlændingemyndighederne kan videregive oplysninger fra en sag efter kapitel 1, 3 og 4 til anklagemyndigheden med henblik på anklagemyndighedens beslutning om, hvorvidt tiltale skal rejses for forbrydelser begået uden for Danmark, fremstod for en umiddelbar betragtning som en væsentlig lempelse af betingelserne for videregivelse af oplysninger som nævnt i persondatalovens § 7, stk. 1 og 6, og § 8, stk. 1 og 2.

Det var imidlertid Datatilsynets vurdering, at bestemmelsen ikke ville indebære en sådan afvigelse i forhold til gældende ret, hvis den administreres i overensstemmelse med de retningslinier, som var nævnt i bemærkningerne til bestemmelsen.

Den foreslåede bestemmelse til udlændingelovens § 45 b, stk. 1, fastsatte, at Indenrigsministeriet på baggrund af en indstilling fra justitsministeren skulle vurdere, om en udlænding må anses for en fare for statens sikkerhed. Denne vurdering skal lægges til grund ved udlændingemyndighedernes afgørelse af en sag om meddelelse eller inddragelse af opholdstilladelse eller om udvisning. Efter § 45 b, stk. 2, 1. pkt., kan det endvidere bestemmes, at de oplysninger, der har ført til, at udlændinge må anses for en fare for statens sikkerhed, ikke må videregives til de udlændinge, vurderingen angår.

Det var et politisk spørgsmål, hvorledes hensyn til statens sikkerhed på dette område skal vægtes i forhold til den registreredes indsigtsret efter persondatalovens § 31 og de generelle undtagelser herfra i lovens § 32.

Datatilsynet noterede sig, at det i bemærkningerne til § 45 b udtrykkeligt var anført, at reglerne i forvaltningslovens kapital 4 om retten til aktindsigt blev fraveget, samt at persondatalovens § 29 om oplysningspligt også blev fraveget. Datatilsynet forstod det således, at bestemmelsen i persondataloven om den registreredes indsigtsret også skulle fraviges. Datatilsynet fandt herefter

ikke at burde udtale sig yderligere herom, bortset fra at når aktindsigt og oplysningspligt udtrykkeligt var omtalt, burde persondatalovens § 31 også være omtalt.

2. Oplysningspligt

Den forslåede nye bestemmelse til udlændingelovens § 40, stk. 1, 3. pkt., fastsatte, at udlændingen skal oplyses om, at de oplysninger, som udlændinge efter gældende ret allerede har pligt til at afgive efter § 40, stk. 1, 1. og 2. pkt. (dvs. til bedømmelse af, om en tilladelse i henhold til udlændingeloven kan gives, inddrages eller bortfalde, eller om udlændinge lovligt opholder sig her i landet), kan videregives til efterretningstjenesterne og anklagemyndigheden, og at oplysningerne vil kunne danne grundlag for anklagemyndighedens beslutning om, hvorvidt tiltalte skal rejses for forbrydelser begået uden for Danmark.

Efter Datatilsynets opfattelse fulgte § 40, stk. 1, 3. pkt., om oplysningspligt allerede af persondatalovens § 28 (navnlig stk. 1, nr. 3, litra a) om indsamling af oplysninger hos den registrerede selv (den pågældende udlænding), der netop tager sigte på en situation som den, der er reguleret i den foreslåede særregel om oplysningspligt. Efter persondatalovens § 28, stk. 1, nr. 3, litra a, er der pligt til at give den registrerede meddelelse om "kategorier af modtagere", hvis dette under hensyn til de særlige omstændigheder, hvorunder oplysningerne om den registrerede er indsamlet, er nødvendigt for, at den registrerede kan varetage sine interesser. I bemærkningerne til bestemmelsen anførtes det, at der er oplysningspligt, selv om den pågældende udlænding derved inkriminerer sig selv.

Datatilsynet havde således ikke isoleret set bemærkninger til § 40, stk. 1, 3. pkt.

§ 40, stk. 1, 3. pkt., regulerede imidlertid alene spørgsmålet om udlændingemyndighedernes oplysningspligt med hensyn til eventuel videregivelse til efterretningstjenesterne og anklagemyndigheden - ikke udveksling udlændingemyndighederne imellem eller anklagemyndighedens og efterretningstjenesternes oplysningspligt.

Datatilsynet henledte derfor opmærksomheden på, at persondataloven i lovens § 29 tillige indeholder regler om oplysningspligt over for den registrerede i tilfælde, hvor oplysninger indsamles hos andre end de registrerede selv. Bestemmelsen indebærer, at udlændingemyndighederne, når de modtager oplysninger om en udlænding, har pligt til at underrette de pågældende udlændinge om en række forhold. Udlændingemyndighederne kan kun undlade at underrette den pågældende udlænding, hvis en af de undtagelser, der er nævnt i persondatalovens § 29, stk. 2-3, eller § 30, finder anvendelse i det konkrete tilfælde.

Datatilsynet tilføjede, at persondatalovens regler om oplysningspligt ikke finder anvendelse på behandlinger, der foretages for politi og anklagemyndighed inden for det strafferetlige område, jf. persondatalovens § 2, stk. 4, 2. pkt. Reglerne finder heller ikke anvendelse for forsvarets og politiets efterretningstjeneste, jf. herved lovens § 2, stk. 11.

3. Søgning og videregivelse af oplysninger om udlændinges fingeraftryk og personfotografi

De foreslåede bestemmelser til udlændingelovens § 40 a, stk. 7, og § 40 b, stk. 7, lempede reglerne for, hvornår de fingeraftryk og personfotografier, som politiet optager i henhold til retsplejelovens regler, til brug for efterforskningen af et strafbart forhold manuelt eller elektronisk kan sammenholdes (samkøres) med fingeraftryk og personfotografier af asylansøgere. Lempelsen bestod i, at de gældende regler om, at der skal være tale om efterforskning af en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover, og at søgning og videregivelse kun kan ske efter forud indhentet retskendelse, ophævedes.

Forslaget til § 40 a, stk. 8, og § 40 b, stk. 8, gav mulighed for, at fingeraftryk og personfotografier, der modtages som led i en international efterlysning manuelt eller elektronisk kan sammenholdes (samkøres) med fingeraftryk og personfotografier af asylansøgere. Også her bestod lempelsen i en ophævelse af de gældende regler om, at der skal være tale om efterforskning af en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover, og at søgning og videregivelse kun kan ske efter forud indhentet retskendelse.

Om reglerne for samkøring på disse områder skal lempes, var et politisk spørgsmål, som Datatilsynet ikke fandt at burde udtale sig om. Det bemærkedes dog, at Datatilsynet - i overensstemmelse med en tilkendegivelse fra Retsudvalgets flertal i betænkning over lovforslag nr. L 50 af 16. januar 1991 - ved behandling af sager om samkøring i den offentlige forvaltning lægger vægt på, om samkøring er nødvendig for at varetage væsentlige hensyn til offentlige interesser, og om samkøring i kontroløjemed har et klart og utvetydigt retsgrundlag. Det tillagdes endvidere betydning, at en kontrolordning alene tager sigte på fremtidige forhold, medmindre særlige forhold gør sig gældende.

Efter forslaget til § 40 a, stk. 8, 2. pkt., og § 40 b, stk. 8, 2. pkt., kunne oplysninger til brug for besvarelse af en international efterlysning videregives til den udenlandske myndighed, der har udsendt efterlysningen.

Denne bestemmelse var efter Datatilsynets opfattelse meget vidtgående - også når de begrænsninger, der anføres i bemærkningerne, toges i betragtning.

Datatilsynet henstillede derfor, at det overvejes at anføre i bemærkningerne til bestemmelsen, at også andre beskyttelseshensyn over for den registrerede end de allerede nævnte, f.eks. at modtagerlandet ikke sikrer et tilstrækkeligt beskyttelsesniveau, jf. herved persondatalovens § 27, kan begrunde, at (nogle) oplysninger ikke bør videregives.

4. Indberetning til Schengen-informationssystemet

Den forslåede bestemmelse til udlændingelovens § 58 g udvidede mulighederne for indberetning af udlændinge, der ikke er statsborger i et Schengenland eller et land, der er tilsluttet De Europæiske Fællesskaber, som uønsket til Schengen-informationssystemet (SIS). Det foresloges således, at der tillige kan ske indberetning, hvis udlændingen er meddelt afslag på opholdstilladelse efter § 10, stk. 1 eller 2, nr. 1 eller 2 (forslaget til § 58 g, nr. 4), eller hvis udlændingens opholdstilladelse er inddraget i medfør af § 19, stk. 2, nr. 2 eller 3 (forslaget til § 58 g, nr. 5).

Det var anført i bemærkningerne, at det er Indenrigsministeriets vurdering, at de forslåede muligheder for indberetning følger af Schengen-konventionen artikel 96, jf. lov om Danmarks tiltrædelse af Schengen-konventionen, der omhandler optagelse af udlændinge i SIS.

§ 58 g gav ikke Datatilsynet anledning til bemærkninger.

Ekstern terminaladgang til de elektroniske tinglysningsregistre

Justitsministeriet anmodede Datatilsynet om en udtalelse om udkast til forslag til lov om ændring af tinglysningsloven.

Hovedformålet med lovforslaget var at udvide muligheden for at få ekstern terminaladgang til de elektroniske tinglysningsregistre. Det blev endvidere foreslået at ophæve tinglysningslovens særlige bestemmelser om, hvad de tinglysningsoplysninger, som indhentes via edb-terminaler, må bruges til.

Sagen blev behandlet på et møde i Datarådet. Datatilsynet udtalte herefter indledningsvis, at det lå uden for tilsynets kompetenceområde at tage stilling til spørgsmål vedrørende domstolenes behandlinger af personoplysninger, idet tilsyn med behandling af oplysninger, der foretages for domstolene, hører under Domstolsstyrelsen henholdsvis vedkommende ret, jf. reglerne i persondatalovens kapitel 17. Datatilsynets udtalelse var derfor begrænset til generelle databeskyttelsesretlige bemærkninger.

Datatilsynet fandt, at den foreslåede ændring af tinglysningslovens § 50 c, stk. 3, hvorefter det bliver muligt at videregive oplysninger til enhver via eks-

tern terminaladgang, ikke gav anledning til særlige databeskyttelsesretlige betænkeligheder. Oplysningerne i tinglysningssystemerne har altid været offentlig tilgængelige. Desuden har det siden 1992 været muligt for alle at få adgang til oplysningerne i elektronisk form, enten via publikumsterminaler på tinglysningskontorerne eller via ekstern terminaladgang.

Datatilsynet benyttede dog lejligheden til at henlede opmærksomheden på problemstillingen omkring videregivelse af borgernes eventuelle beskyttede navne- og adresseoplysninger. Ud fra databeskyttelsesretlige hensyn bør sådanne oplysninger som udgangspunkt ikke videregives.

Hvis det efter anmodning fra de pågældende borgere er muligt at undlade offentliggørelse af borgernes beskyttede navne- og adresseoplysninger (i praksis særligt oplysningen om navn), uden at dette kolliderer med tinglysningssystemets særlige formål, fandt Datatilsynet derfor, at det burde overvejes at forbedre beskyttelsen af de berørte borgeres privatliv i denne henseende.

Det var Datatilsynets opfattelse, at ophævelsen af tinglysningslovens § 50 c, stk. 7, hvorefter tinglysningsloven ikke længere vil indeholde regler, der begrænser anvendelsen af de oplysninger, som er indhentet via tinglysningsregistrene, ikke gav anledning til særlige databeskyttelsesretlige betænkeligheder.

Indsamling og efterfølgende registrering og anden form for behandling af de oplysninger, der indhentes via terminaladgang til tinglysningsregistrene, vil være reguleret af persondataloven. Datatilsynet var således enig med Justitsministeriet i, at der ikke er behov for en særskilt regulering i tinglysningsloven af anvendelse og efterfølgende behandling af oplysninger indhentet via tinglysningsregistrene.

Datatilsynet henledte opmærksomheden på, at reglerne om virksomheders uopfordrede henvendelser til bestemte aftagere i markedsføringsøjemed (opdyrkning af nye kundeforhold eller markedsføring af egne produkter m.v. over for egne, allerede eksisterende kunder) findes i markedsføringslovens § 6 a, og at dette burde præciseres i lovforslagets bemærkninger.

Sager om behandling af personoplysninger

Sager om behandling af personoplysninger

Sager om markedsføringsreglerne

Også i 2001 har de særlige regler i persondataloven om markedsføring givet anledning til en del sager. Datatilsynet har tidligere truffet principielle afgørelser på dette område. Der kan i den forbindelse henvises til årsberetningen for 2000 s. 39 ff., hvor der er gengivet 3 principielle sager.

I det følgende gengives 3 principielle sager, hvor Datatilsynet i 2001 har udtalt sig om persondatalovens regler om markedsføring.

1. Markedsføring i form af indstik i aviser og ugeblade

Indstik i aviser, ugeblade m.v. er ikke at betragte som særskilt markedsføring overfor abonnenterne og er derfor ikke omfattet af persondatalovens § 6, stk. 2-4 og § 36 (Datatilsynets j.nr. 2000-212-0004)

Sagen vedrørte en henvendelse fra Grafisk Netværk, som havde bedt om Datatilsynets fortolkning af persondataloven i relation til indstik. Spørgsmålet blev to gange drøftet i Datarådet.

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

I de tilfælde, hvor videregivelse eller anvendelse af generelle kundeoplysninger kan ske uden samtykke, skal indsigelsesreglerne i § 36 iagttages. Heraf følger, at hvis kunden ikke har fremsat indsigelse direkte over for virksomheden, skal virksomheden - hver gang den ønsker at videregive kundeoplysninger til andre virksomheder til brug for markedsføring eller anvende kundeoplysninger på vegne af en anden virksomhed - tjekke i CPR, om kunden har frabedt sig henvendelser i markedsføringsøjemed. Er dette tilfældet, må oplysningerne ikke videregives eller anvendes til dette formål.

Hvis kunden ikke gennem en markering i CPR har frabedt sig henvendelser, skal virksomheden endvidere - inden oplysningerne videregives eller anvendes - give kunden tydelig og forståelig meddelelse om indsigelsesretten. Virksomheden skal i den forbindelse give kunden en nem adgang til inden for en frist på to uger at fremsætte indsigelse mod, at videregivelse eller anvendelse finder sted. Videregivelse eller anvendelse må ikke finde sted, før det er konstateret, at forbrugeren ikke har fremsat indsigelse inden udløbet af fristen på 2 uger.

Det var Datatilsynets opfattelse, at det giver anledning til betydelig tvivl, om indstik i aviser, ugeblade m.v., der sendes til abonnenter, i relation til ovennævnte regler skal betragtes som markedsføring på vegne af de virksomheder, hvis produkter, tjenesteydelser m.v. der reklameres for.

På den ene side kan indstik betragtes som en i forhold til aviser, ugeblade m.v. uafhængig og særskilt markedsføring over for abonnenten som forbruger.

På den anden side har indstik mange lighedspunkter med almindeligt forekommende trykte annoncer i aviser, ugeblade m.v., som ikke anses for markedsføring i relation til reglerne i persondatalovens § 6, stk. 2-4, og § 36, og det ville efter Datatilsynets opfattelse i meget vidt omfang reelt umuliggøre brug af indstik over for abonnenter på aviser, ugeblade m.v., hvis den særlige indsigelsesprocedure i lovens § 36 skulle iagttages, jf. ovenfor. Denne konsekvens, der er uomtalt i lovens forarbejder, har efter Datatilsynets opfattelse næppe været tilsigtet med persondataloven.

På denne baggrund var det Datatilsynets opfattelse, at indstik i aviser, ugeblade m.v. ikke kan anses for omfattet af reglerne i persondatalovens § 6, stk. 2-4, og § 36. Den særlige indsigelsesprocedure i § 36 skal derfor ikke iagttages.

Datatilsynet forudsatte dog, at aviser, ugeblade m.v. i forbindelse med salg af indstiksplads ikke udnytter eventuelle særlige oplysninger, de måtte have om abonnenternes forbrugsvaner.

Adgangen til at reklamere gennem indstik skal herefter vurderes i forhold til reglerne i markedsføringsloven. Disse regler hører under Forbrugerombudsmandens kompetence.

2. Fortolkning af persondatalovens markedsføringsregler i forhold til den finansielle sektor

Udtalt, at der er tale om markedsføring på vegne af andre omfattet af reglerne i persondatalovens § 6, stk. 2-4, og § 36, hvis et pengeinstitut markedsfører andres, f.eks. koncernforbundne selskabers, finansielle ydelser over for pengeinstituttets kunder. Endvidere udtalt, at der kan udsendes rådgivningsmateriale til kunder uden at de særlige markedsføringsregler i persondataloven skal iagttages (Datatilsynets j.nr. 2000-213-0029)

Finansrådet rejste en række fortolkningsspørgsmål over for Datatilsynet i relation til persondatalovens § 6, stk. 2-4, og § 36, herunder særligt vedrørende rækkevidden af begrebet "anvende på vegne af en anden virksomhed i markedsføringsøjemed".

Finansrådet pegede i den forbindelse på, at reglerne i persondatalovens § 6, stk. 2-4, og § 36 medførte en række ulemper for den finansielle sektor. Som eksempel herpå henviste Finansrådet til, at pengeinstitutterne ofte fungerer som distributionskanal for en række finansielle ydelser, som produceres af underleverandører. Efter rådets opfattelse var pengeinstitutternes udbud af sådanne ydelser som hovedregel ikke markedsføring på vegne af underleverandøren, men derimod markedsføring af pengeinstituttet som udbyder og rådgiver af en vifte af finansielle ydelser.

Pengeinstitutternes skriftlige henvendelser til forbrugere, hvori underleverandørernes ydelser omtales, var derfor efter Finansrådets opfattelse ikke omfattet af begrænsningerne i persondatalovens § 6, stk. 2-4, og § 36, men alene af begrænsningerne i markedsføringslovens § 6 a.

Finansrådet anførte, at det ville være vanskeligt for pengeinstitutterne at fortsætte som distributionskanal for ydelser produceret af underleverandører, hvis denne fremgangsmåde betragtedes som "anvendelse på vegne af andre i markedsføringsøjemed". Finansrådet henviste som begrundelse herfor til, at det ikke var praktisk muligt at indhente samtykke fra kunderne, ligesom det ikke var praktisk muligt at overholde indsigelsesproceduren i lovens § 36.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at der ikke gælder særlige regler for den finansielle sektor i forbindelse med et koncernselskabs markedsføring af et andet koncernselskabs produkter eller ydelser. Finansielle virksomheder skal derfor ligesom alle andre virksomheder iagttage de særlige regler i persondatalovens § 6, stk. 2-4, og § 36. Det gælder både i forbindelse med videregivelse og anvendelse af forbrugeroplysninger på vegne af andre i markedsføringsøjemed.

Datatilsynet udtalte endvidere, at der efter Datatilsynets opfattelse er tale om markedsføring på vegne af andre i de tilfælde, hvor pengeinstitutterne fungerer som distributionskanal for finansielle ydelser produceret af underleverandører. Når en finansiel virksomhed - eksempelvis et pengeinstitut - markedsfører en anden virksomheds finansielle ydelser, vil reglerne i persondatalovens § 6, stk. 2-4, og § 36 således skulle iagttages - uanset om markedsføringsmaterialet om underleverandørens ydelser udarbejdes og udsendes af pengeinstituttet. Dette gælder både for koncernforbundne og ikke-koncernforbundne selskaber.

Datatilsynet henviste i øvrigt til, at reglerne i persondataloven ikke er til hinder for, at et pengeinstitut - uden at iagttage reglerne i persondatalovens § 36 - markedsfører andre virksomheders produkter over for en kunde, hvis kunden har udtrykt et ønske om at blive informeret om forskellige finansielle ydelser. Det er dog en forudsætning, at kunden har udtrykt sit ønske på en sådan måde, at der er givet et gyldigt samtykke til markedsføringen.

Datatilsynet præciserede, at pengeinstitutterne naturligvis kan rådgive kunderne om forskellige finansielle ydelser, herunder ydelser produceret af andre virksomheder. En sådan rådgivning kan eksempelvis ydes i forbindelse med kundens personlige fremmøde i pengeinstituttet og ved telefoniske henvendelser, hvor kunden kan informeres om de forskellige finansielle ydelser, som pengeinstituttet tilbyder eller formidler.

Pengeinstitutterne kan endvidere udsende rådgivningsmateriale til kunderne uden at skulle iagttage reglerne i persondatalovens § 6, stk. 2-4, og § 36. Dette forudsætter imidlertid, at hovedformålet med henvendelsen til kunden er at yde kunden en neutral rådgivning om et eller flere bestemte emner med henblik på, at kunden kan varetage sine interesser. Hvis hovedformålet med henvendelsen til kunden derimod er at afsætte bestemte varer eller tjenesteydelser på andre virksomheders vegne, vil der være tale om "anvendelse på andres vegne i markedsføringsøjemed". I så fald skal reglerne i persondatalovens § 6, stk. 2-4, og § 36 iagttages.

Datatilsynet tilkendegav, at det kan være vanskeligt at afgøre, om der er tale om markedsføring eller rådgivning i forbindelse med finansielle virksomheders udsendelse af materiale, idet materialet i mange tilfælde vil indeholde elementer af såvel markedsføring som rådgivning. Det må derfor i sidste ende bero på en konkret vurdering i hvert enkelt tilfælde, om der er tale om markedsføring omfattet af de særlige regler i persondataloven, eller om der er tale om rådgivning, der falder uden for reglernes anvendelsesområde.

3. En fagforenings udsendelse af materiale til studerende

Udtalt, at uddannelsessteder ikke må videregive oplysninger om studerendes navne og adresser til en forening til brug for foreningens udsendelse af materiale til de studerende uden samtykke. Endvidere udtalt, at informationsmateriale om diverse studie- og erhvervsrelevante tiltag må udsendes til de studerende af et uddannelsessted eller et adresserings-/mailbureau på vegne af en forening uden samtykke (Datatilsynets j.nr. 2001-214-0020)

Civiløkonomerne, som er en faglig service- og interesseorganisation for ca. 15.000 medlemmer med afgangseksamen i blandt andet erhvervsøkonomi, virksomhedsledelse og tilsvarende uddannelser fra handelshøjskoler og universiteter, anmodede Datatilsynet om at vurdere, om følgende fremgangsmåder ved udsendelse af materiale til studerende på højere læreanstalter kunne iværksættes inden for rammerne af persondataloven:

a) Uddannelsesstedet udleverer labels med de studerendes navne og adresser enten til Civiløkonomerne eller til et adresserings-/mailbureau.
b) Uddannelsesstedet udsender materiale til de studerende på vegne af Civiløkonomerne.

Det materiale, som foreningen ønskede at udsende til de studerende ved brug af læreanstalternes oplysninger om de studerendes navne og adresser, havde ifølge det oplyste ikke karakter af markedsføring af foreningen som sådan. Der var derimod tale om information til de studerende om diverse studie- og erhvervsrelevante tiltag.

Meget af det informationsmateriale, som foreningen udsendte, havde efter foreningens opfattelse betydning for alle studerende og ikke kun for de studerende, som var medlem af Civiløkonomerne. Udsendelse af materiale forudsatte derfor i mange tilfælde, at læreanstalterne stillede oplysninger om de studerendes navne og adresser til rådighed.

Civiløkonomerne havde ifølge det oplyste ingen interesse i at komme i besiddelse af de studerendes navne og adresser, idet foreningen alene ønskede at sikre sig, at relevant materiale blev udsendt til de studerende. Det ville således for foreningen være tilstrækkeligt, hvis læreanstalterne eller et adresserings-/mailbureau udsendte materialet til de studerende på vegne af foreningen.

Civiløkonomerne oplyste i øvrigt, at foreningen havde et tæt samarbejde med de højere læreanstalter, og at foreningen varetog en række opgaver på disses vegne i forhold til de studerende, herunder blandt andet opgaver i forbindelse med afholdelse af virksomhedspræsentationer på uddannelsesstederne.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at uddannelsesstederne alene kunne udlevere de studerendes navne og adresser til Civiløkonomerne til brug for udsendelse af materiale, hvis der var indhentet udtrykkeligt samtykke hertil fra de studerende i overensstemmelse med persondatalovens § 6, stk. 1, nr. 1. Datatilsynet præciserede, at der skulle indhentes samtykke, uanset om der var tale om udsendelse af informationsmateriale eller markedsføringsmateriale, idet hensynet til beskyttelsen af de studerende i begge tilfælde vejede tungere end interessen i at udsende materialet.

Datatilsynet fandt dog, at udsendelse af informationsmateriale til de studerende kunne ske uden samtykke, i det omfang udsendelsen blev varetaget af uddannelsesstederne eller af et adresserings-/mailbureau på vegne af Civiløkonomerne. Datatilsynet lagde herved vægt på, at der ikke blev videregivet oplysninger om de studerendes navne og adresser til Civiløkonomerne, og at det måtte antages at være i de studerendes interesse at modtage information om diverse studierelevante tiltag.

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

Datatilsynet udtalte, at det efter tilsynets opfattelse vil være i strid med denne bestemmelse, hvis et uddannelsessted uden samtykke anvender oplysninger om de studerende til brug for udsendelse af markedsføringsmateriale på vegne af en forening - eventuelt via et adresserings-/mailbureau.

Datatilsynet understregede derfor, at uddannelsesstedernes oplysninger om de studerende alene kan anvendes på vegne af Civiløkonomerne til udsendelse af informationsmateriale om diverse studie- og erhvervsrelevante tiltag, som må antages at være af interesse for de studerende.

Datatilsynet henstillede over for Civiløkonomerne, at foreningen skulle orientere de uddannelsessteder, som stillede oplysninger om de studerende til rådighed for udsendelse af materiale, om de i denne udtalelse indeholdte begrænsninger med henblik på at sikre overholdelsen af bestemmelsen i persondatalovens § 5, stk. 2.

Due diligence

(besigtigelse ved virksomhedsoverdragelse)

Udtalt, at almindelige, ikke-følsomme oplysninger normalt kan behandles, herunder videregives, som led i en due diligence undersøgelse, jf. personda - talovens § 6, stk. 1, nr. 7. Er der derimod tale om følsomme oplysninger, jf. lovens §§ 7 og 8 vil behandlingen som hovedregel kræve de registrerede personers samtykke (Datatilsynets j.nr. 2000-210-0002)

Et advokatfirma havde i en generel forespørgsel anmodet om Datatilsynets stillingtagen til flere spørgsmål vedrørende såkaldte due diligence undersøgelser i forhold til persondataloven.

Sagen blev behandlet på et møde i Datarådet.

Datatilsynet bemærkede indledningsvis, at tilsynet lagde til grund, at i praksis vil persondataloven som oftest finde anvendelse på en udlevering af personoplysninger, der sker som led i en due diligence undersøgelse. Datatilsynet gik ud fra, at der typisk vil være tale om enten elektronisk behandling af personoplysninger eller systematiske samlinger af (papir-) sagsakter med fortrolige oplysninger om enkeltpersoner, jf. herved persondatalovens § 1, stk. 1 og 2.

Det var tilsynets opfattelse, at udleveringen af oplysninger fra sælger til den mulige købers rådgivere skal betragtes som en behandling af personoplysninger i persondatalovens forstand. Udleveringen kræver – i det omfang loven finder anvendelse, jf. § 1 – hjemmel i reglerne i lovens kapitel 4 om behandling af oplysninger.

For så vidt angår ikke-følsomme oplysninger omfattet af lovens § 6 (f.eks. almindelige id-oplysninger, lønoplysninger, oplysninger om uddannelse eller ar-

bejdsområde) var det Datatilsynets opfattelse, at udlevering af disse oplysninger til købers rådgivere i en due dilligence proces normalt kan ske med hjemmel i lovens § 6, stk. 1, nr. 7. Det følger af denne bestemmelse, at der må ske behandling af oplysninger, hvis behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

Datatilsynet lagde i denne forbindelse vægt på, at sælger og den mulige køber har en berettiget interesse i videregivelsen, samt at hensynet til den registrerede ikke taler imod, navnlig set i forhold til oplysningernes karakter. Tilsynet forudsatte i den forbindelse også, at udleveringen af oplysninger betinges af fortrolighed.

Datatilsynet pegede endvidere på, at den registreredes samtykke også kan danne baggrund for udleveringen, jf. § 6, stk. 1, nr. 1.

For så vidt angår udlevering af følsomme oplysninger omfattet at persondataloven § 7 (f.eks. helbredsoplysninger eller oplysninger om fagforeningsmæssigt tilhørsforhold) var det Datatilsynets opfattelse, at udleveringen normalt kun kan ske med de registreredes samtykke, jf. lovens § 7, stk. 2, nr. 1.

Datatilsynet udtalte endvidere, at private virksomheders videregivelse af oplysninger omfattet af lovens § 8 (f.eks. oplysninger om strafbare forhold) skal ske efter reglen i lovens § 8, stk. 5, hvorefter udgangspunktet er, at oplysningerne ikke må videregives uden den registreredes udtrykkelige samtykke. Videregivelse kan dog ske uden samtykke, når det sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.

Efter Datatilsynets opfattelse vil videregivelse af følsomme oplysninger omfattet af § 8 normalt kræve den registreredes samtykke. Der kan dog tænkes situationer, hvor videregivelse af oplysninger omfattet af § 8 vil kunne ske uden samtykke fra de registrerede. Afgørelsen heraf vil dog altid bero på en konkret vurdering i den enkelte situation.

I øvrigt anbefalede Datatilsynet, at følsomme oplysninger i videst muligt omfang anonymiseres inden udleveringen, samt at der udvises tilbageholdenhed med udleveringen af følsomme personoplysninger. I den forbindelse pegede tilsynet på lovens § 5, stk. 3, hvoraf 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.

Behandling af følsomme oplysninger om misbrugere

I forbindelse med anmeldelse af et misbrugssystem indeholdende oplysninger om stofmisbrugere og alkoholikere udtalte Datatilsynet, at behandling af følsomme oplysninger om klienter og disses pårørende som udgangspunkt bør ske på baggrund af et udtrykkeligt samtykke (Datatilsynets j.nr. 2000-53-0118)

Datatilsynet modtog en anmeldelse af et misbrugssystem fra Århus Amt vedrørende amtets behandling af oplysninger om stofmisbrugere og alkoholikere. Misbrugssystemet indeholdt særdeles følsomme oplysninger om misbrugerne selv samt om disses pårørende. Om misbrugerne blev der blandt andet behandlet helbredsoplysninger, oplysninger om sociale forhold, kriminalitet og øvrige baggrundsoplysninger af betydning for behandlingen af den pågældende. Om de pårørende blev der blandt andet behandlet oplysninger om misbrug, selvmord, selvmordsforsøg, oplysninger om psykiske problemer samt oplysninger om følelsesmæssige, fysiske og seksuelle overgreb.

Oplysningerne blev af amtet indsamlet i forbindelse med samtaler med den enkelte misbruger via et papirbaseret oplysningsskema. Disse oplysninger blev efterfølgende indtastet i amtets elektroniske klientjournal, som var tilgængelig for samtlige behandlere på amtets misbrugscenter.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at behandling af oplysninger om misbrugere bør ske på baggrund af et udtrykkeligt samtykke, jf. persondatalovens § 7, stk. 2, nr. 1, idet der var tale om behandling af meget følsomme oplysninger. Datatilsynet lagde herved blandt andet vægt på, at amtet i forvejen indhentede samtykke.

For så vidt angår behandling af oplysninger om de pårørende udtalte Datatilsynet, at tilsynet fandt det betænkeligt, at der blev behandlet så følsomme oplysninger om disse personer. Datatilsynet fandt derfor, at amtets behandling af oplysninger om de pårørende i videst muligt omfang burde ske på baggrund af et udtrykkeligt samtykke.

Datatilsynet tilkendegav dog, at oplysningerne rent undtagelsesvis kunne behandles uden samtykke efter bestemmelsen i persondatalovens § 7, stk. 2, nr. 4, hvis det måtte vise sig umuligt at indhente samtykke fra den pårørende. Det følger af bestemmelsen i § 7, stk. 2, nr. 4, at følsomme oplysninger kan behandles, hvis dette er nødvendigt for at et retskrav kan fastlægges, gøres gældende eller forsvares. Datatilsynet præciserede dog, at behandling af oplysninger om pårørende uden samtykke forudsatte, at der var iværksat de fornødne tiltag med henblik på at søge samtykke indhentet, og at det ud fra en konkret vurdering var fundet klart nødvendigt at inddrage oplysninger om klientens familiemedlemmer i behandlingsforløbet.

Datatilsynet henstillede endvidere overfor amtet, at der ved behandling af oplysninger om pårørende uden samtykke skulle gøres notat herom - eventu-

elt ved at føre en fortegnelse over de tilfælde, hvor indhentelse af samtykke havde vist sig umulig. En sådan fremgangsmåde ville gøre det muligt for Datatilsynet - eventuelt i forbindelse med en inspektion - at kunne kontrollere, at der kun rent undtagelsesvis blev behandlet oplysninger om pårørende uden et udtrykkeligt samtykke.

Datatilsynet forudsatte i øvrigt, at reglerne om oplysningspligt i persondatalovens kapitel 8 blev iagttaget i forbindelse med indsamling af oplysninger om klienterne og disses pårørende.

Offentliggørelse af oplysninger om byrådsmedlemmer på Internettet

Udtalt, at en forenings offentliggørelse af visse oplysninger om byrådsmedlemmer på internettet ikke var i strid med persondatalovens regler. Datatilsynet tog blandt andet hensynet til ytringsfriheden i betragtning (Datatilsynets j.nr. 2001-215-0050)

En kommune klagede på vegne af byrådets medlemmer til Datatilsynet over, at en forening havde offentliggjort en række oplysninger om byrådets medlemmer på en hjemmeside uden forinden at have indhentet samtykke fra de enkelte byrådsmedlemmer.

Den omhandlede hjemmeside indeholdt blandt andet billeder af de enkelte byrådsmedlemmer hentet fra kommunens hjemmeside samt oplysninger om vederlag og rejseaktiviteter og de hermed forbundne udgifter. En del af de offentliggjorte oplysninger var af foreningen indhentet hos kommunen ved begæring om aktindsigt.

Med hensyn til oplysninger om rejseaktiviteter oplyste kommunen, at det fremgår af pressen eller af kommunens hjemmeside, hvilke rejseaktiviteter byrådets medlemmer og kommunale embedsmænd deltager i. Ved begæring om aktindsigt havde foreningen fået oplyst, hvilke udgifter der var forbundet med de enkelte rejseaktiviteter. Kommunen oplyste endvidere, at det fremgår af de kommunale budgetter og regnskaber, hvordan byrådets medlemmer honoreres, og at vederlagsreglerne i øvrigt er lovbestemte. På den pågældende hjemmeside var tallene dog samlet for alle byrådets medlemmer for hver vederlagskategori. Foreningen var gennem aktindsigt mundtligt gjort bekendt med, hvordan budgetterne og regnskaberne skulle forstås. Udlægningen af oplysningerne på internettet indebar efter kommunens opfattelse en videregivelse af oplysninger, der ikke i almindelighed er tilgængelige for offentligheden, hvorfor oplysningerne burde slettes.

Kommunen havde forud for indgivelse af klage til Datatilsynet fremsat indsigelse mod offentliggørelsen over for foreningen og anmodet om, at de oplysninger, der ikke opfyldte persondatalovens bestemmelser, skulle slet-

tes fra hjemmesiden. Kommunens indsigelser blev imidlertid ikke efterkommet.

Formålet med den pågældende hjemmeside var ifølge det oplyste at give lokalpolitikerne igen med det, som de byder deres medborgere. Oplysninger om vederlag var offentliggjort med henblik på at belyse, om politikerne belønnes efter deres indsats eller mangel på samme. Foreningen var i øvrigt af den opfattelse, at byrådsmedlemmerne måtte leve med, at oplysninger om deres vederlag blev offentliggjort.

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

De billeder af byrådsmedlemmerne og de oplysninger om deres rejseaktiviteter og vederlag, der var offentliggjort på hjemmesiden, måtte efter Datatilsynets opfattelse betragtes som almindelige ikke-følsomme oplysninger omfattet af persondatalovens § 6.

I det omfang hjemmesiden indeholdt oplysninger om politiske tilhørsforhold, måtte det lægges til grund, at oplysningerne enten stammede fra offentligt tilgængelige kilder eller var offentliggjort af byrådsmedlemmerne selv. Spørgsmålet om, hvorvidt disse oplysninger måtte behandles, skulle derfor også afgøres efter lovens § 6.

I henhold til lovens § 6, stk. 1, nr. 1, må oplysninger blandt andet behandles, hvis den registrerede har givet udtrykkeligt samtykke hertil. Behandling må endvidere ske efter § 6, stk. 1, nr. 7, hvis dette er nødvendigt for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

En række af de offentliggjorte oplysninger stammede fra offentligt tilgængelige kilder eller var offentliggjort af byrådsmedlemmerne selv eller med disses samtykke. Efter Datatilsynets opfattelse måtte foreningen antages at have en berettiget interesse i at gøre disse oplysninger tilgængelige på internettet. Da oplysningerne i forvejen var tilgængelige blandt andet på kommunes hjemmeside, oversteg hensynet til byrådsmedlemmerne efter Datatilsynets opfat-

telse ikke denne interesse. Datatilsynet tog herved tillige hensynet til ytringsfriheden i betragtning.

De andre oplysninger på hjemmesiden var tilvejebragt gennem aktindsigt. Efter Datatilsynets opfattelse havde foreningen ligeledes en berettiget interesse i at offentliggøre sådanne oplysninger, som oversteg hensynet til byrådsmedlemmerne. Datatilsynet lagde herved vægt på, at der var tale om ikke-fortrolige oplysninger.

Efter Datatilsynets opfattelse var der således ikke sket en overtrædelse af persondatalovens regler i forbindelse med offentliggørelsen af oplysninger om byrådsmedlemmerne på hjemmesiden.

Datatilsynet bemærkede, at den ophavsretlige problemstilling, der knytter sig til udlægning af byrådsmedlemmernes billeder hentet fra kommunens hjemmeside, ikke henhører under tilsynets kompetenceområde.

Persondataloven indeholder i §§ 28 og 29 regler om de dataansvarliges oplysningspligt over for registrerede personer. Efter disse regler skal de dataansvarlige på eget initiativ give en række oplysninger til de registrerede i forbindelse med behandling af personoplysninger.

Hvis en dataansvarlig (f.eks. en virksomhed eller forening) indsamler personoplysninger gennem aktindsigt, skal den således være opmærksom på disse regler.

Datatilsynet gjorde foreningen opmærksom på, at persondatalovens regler om oplysningspligt skal iagttages ved indsamling af personoplysninger, f.eks. gennem aktindsigt.

Med hensyn til kommunens indsigelser mod offentliggørelsen udtalte Datatilsynet, at der ikke var anført vægtige grunde vedrørende de enkelte byrådsmedlemmers særlige situation, der talte for, at indsigelsen burde imødekommes, jf. persondatalovens § 35.

Datatilsynet fandt derfor ikke grundlag for at pålægge foreningen at slette oplysningerne om byrådsmedlemmerne fra internettet.

Indsigt i Schengen-informationssystemet

Udtalt, at en klager ikke kunne få indsigt i, hvorvidt der var indlagt oplysninger om vedkommende i Schengen-informationssystemet (SIS) i medfør af Schengen-konventionens artikel 95 og artiklerne 98-100 og i givet fald hvilke oplysninger (Datatilsynets j.nr. 2001-311-0057)

En person klagede til Datatilsynet over, at Rigspolitiet havde afslået at give den pågældende indsigt i, om der var indlagt oplysninger om vedkommende i Schengen-informationssystemet i medfør af Schengen-konventionens artikel 95 og artiklerne 98-100 og i givet fald hvilke oplysninger.

Spørgsmålet om en persons ret til at få adgang til oplysninger om sig selv i Schengen-informationssystemet er undergivet lovgivningen i den kontraherende stat, på hvis område denne ret gøres gældende, jf. Schengen-konventionens artikel 109, stk. 1. Det var således reglerne i persondatalovens kapitel 9 om indsigt, der fandt anvendelse på den pågældende klagers anmodning om indsigt.

Ifølge lovens § 31, stk. 1, skal den dataansvarlige (i dette tilfælde Rigspolitiet) efter begæring fra en person give meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

Ifølge lovens § 32, stk. 1, jf. § 30, stk. 2, gælder dette dog ikke, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser, herunder navnlig til

1) statens sikkerhed,
2) .....
3) den offentlige sikkerhed,
4) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv,
5) .....
6) .....

Efter lovens § 31, stk. 2, skal den dataansvarlige snarest besvare indsigtsbegæringer som nævnt i § 31, stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om hvornår afgørelsen kan forventes at foreligge.

Datatilsynets vurdering af klagerens ret til indsigt

Indskrænkning i den registreredes indsigtsret kan kun ske på grundlag af en konkret afvejning af de modstående interesser, som er nævnt i bestemmelsen i § 30, stk. 2, i persondataloven. Afvejningen skal foretages for hver enkelt oplysning for sig.

Formålet med indlæggelse af oplysninger i Schengen-informationssystemet i medfør af Schengen-konventionens artikel 95 og artiklerne 98-100 er: Anhol-

delse af efterlyste personer, tilvejebringelse af indstævnede personer, forkyndelse af dom eller tilsigelse, diskret overvågning eller målrettet kontrol af personer og motorkøretøjer samt tilvejebringelse af eftersøgte genstande med henblik på beslaglæggelse eller fremlæggelse som bevismiddel i en straffesag.

Henset til disse formål var det Datatilsynets opfattelse, at persondatalovens § 30, stk. 2, nr. 4, normalt må føre til, at der ikke er indsigt i oplysningerne, hvis der rent faktisk er registreret oplysninger om den pågældende. Den registrerede vil i modsat fald kunne træffe forholdsregler, der i væsentlig grad kan skade gennemførelsen af de foranstaltninger, der følger af indberetningen, jf. herved også Schengen-konventionens artikel 109, stk. 2.

For så vidt angår tilfælde, hvor en person, der ikke er registeret i Schengeninformationssystemet, anmoder om indsigt, har Datatilsynet foretaget en vurdering af, om den registrerede har adgang til at få afkræftet, at der behandles oplysninger om vedkommende i Schengen-informationssystemet.

Datatilsynet lagde ved denne vurdering afgørende vægt på, at en generel adgang til at modtage meddelelse om, at man ikke er registreret (afkræftelse), samtidig vil medføre, at de personer, som er registreret, og som ikke modtager en sådan meddelelse, ved en modsætningsslutning kan konstatere, at de er registrerede.

På dette grundlag fandt Datatilsynet ikke at kunne tilsidesætte Rigspolitiets vurdering af, at indsigt i, hvorvidt der er indlagt oplysninger i Schengen-informationssystemet i medfør af Schengen-konventionens artikel 95 samt artiklerne 98-100 - og i givet fald hvilke oplysninger - vil modvirke afgørende hensyn til kriminalitetsbekæmpelse m.v. Tilsynet var enig med Rigspolitiet i, at klagerens interesse i indsigt i Schengen-informationssystemet på disse punkter måtte vige for afgørende hensyn til offentlige interesser.

Datatilsynet fandt således, at Rigspolitiet var berettiget til at undlade at oplyse klageren om, hvorvidt der var indlagt oplysninger om vedkommende i henhold til Schengen-konventionens artikel 95 samt artiklerne 98-100.

Datatilsynets gennemgang af en eventuel registrering

I sager om indsigt i Schengen-informationssystemet anmoder Datatilsynet ved høringen af Rigspolitiet blandt andet om følgende oplysninger: Baggrunden for en eventuel registrering, hvornår denne i givet fald fandt sted, og hvornår den vil blive slettet. Tilsynet udbeder sig desuden en fuldstændig udskrift fra Schengen-informationssystemet vedrørende klageren samt kopier af de akter, der ligger til grund for en eventuel registrering.

Datatilsynet gennemgår det modtagne materiale for at sikre, at der ikke er registreringer i strid med reglerne i Schengen-konventionen.

Retsinformation

Datatilsynet har i det forløbne år stillet vilkår for offentliggørelse af administrative afgørelser på en myndigheds hjemmeside på internet eller i det statslige Retsinformation. Datatilsynet har endvidere behandlet et spørgsmål om vilkår for offentliggørelse af domme i et privat forlags retsinformationssystem.

1. Offentlige myndigheders afgørelser

Fastsættelse af vilkår for offentliggørelse af myndigheders afgørelser i retsinformationssystemer (Datatilsynets j.nr. 2000-321-0009)

Bestemmelsen i persondatalovens § 9, stk. 1, indebærer, at oplysninger, der er omfattet af § 7, stk. 1, eller § 8, kan behandles med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning. Dette vil navnlig være systemer, som er til rådighed for en bredere kreds af abonnenter for at sikre en ensartet retsanvendelse. Derimod vil en myndigheds eller virksomheds interne retsinformationssystem være underlagt de almindelige behandlingsregler.
Efter bestemmelsen skal behandlingen være nødvendig for førelsen af systemerne. Dette betyder, at bestemmelsen ikke hjemler adgang til at behandle oplysninger i et retsinformationssystem, hvis systemet kunne tjene sit formål ligeså sikkert og effektivt uden oplysninger om enkeltpersoner.
For så vidt angår almindelige oplysninger, kan behandlingen ske i henhold til lovens § 6, stk. 1, nr. 5.

Det følger af persondatalovens § 9, stk. 2, at de af stk. 1 omfattede oplysninger ikke senere må behandles i andet øjemed. Det samme gælder behandling af andre oplysninger, som alene foretages med henblik på at føre retsinformationssystemer, jf. § 6.

Datatilsynet kan efter lovens § 9, stk. 3, meddele nærmere vilkår for de i stk. 1 nævnte behandlinger. Tilsvarende gælder for de i § 6 nævnte oplysninger, som alene behandles i forbindelse med førelsen af retsinformationssystemer.

Det nævnes i bemærkningerne til § 9, stk. 3, at der f.eks. kan fastsættes vilkår om, at personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger fjernes i samme omfang, som dette skal ske efter Justitsministeriets cirkulære nr. 85 af 8. juli 1988 om indlæggelse af afgørelser i Retsinformation.

Datatilsynets vilkår

Datatilsynet har i de sager, som indtil videre har været forelagt for tilsynet, fastsat følgende vilkår for offentliggørelse af myndigheders afgørelser i retsinformationssystemer:

1. I afgørelser, som indeholder fortrolige oplysninger eller oplysninger om enkeltpersoners rent private forhold, skal de pågældende oplysninger anonymiseres i overensstemmelse med vilkår nr. 2, jf. dog vilkår nr. 3, før videregivelse må finde sted.

   I alle afgørelser skal det endvidere sikres, at der ikke videregives oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, oplysningen angår.

2. En eventuel anonymisering består i udeladelse af personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger vedrørende personer. I stedet for de udeladte oplysninger kan indsættes neutrale betegnelser. Personnumres løbenummer udelades.

3. Afgørelserne kan forsynes med sagens journalnummer, sagslistenummer m.v.

4. Hvis en afgørelse har været behandlet af en højere instans, skal dette samt udfaldet heraf fremgå af gengivelsen af sagen.

5. Det skal kontrolleres, at der ikke er fejl i gengivelsen af afgørelserne. Fejl og lignende skal rettes eller slettes.

6. Der skal etableres sikkerhed for, at der i retsinformationssystemet ikke kan tilføjes data eller manipuleres med data.

7. Datatilsynets udtalelse skal indhentes inden iværksættelse af ændringer i førelsen af retsinformationssystemet. Ændringer af mindre væsentlig betydning skal dog alene anmeldes til Datatilsynet. Anmeldelsen kan ske efterfølgende, dog senest 4 uger efter ændringen er iværksat.

I relation til begrebet "fortrolige" (ad vilkår nr. 1 og 2) har Datatilsynet uddybende anført, at fortrolige oplysninger som nævnt i vilkår nr. 1 er oplysninger, som ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller som det i øvrigt er nødvendigt at hemmeligholde for at varetage væsentlige hensyn til offentlige eller private interesser.

Følsomme oplysninger som nævnt i persondatalovens § 7, stk. 1, dvs. oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk

overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold, vil være omfattet af begrebet fortrolige oplysninger. Endvidere vil oplysninger om strafbare forhold, og væsentlige sociale problemer og andre rent private forhold, som omtalt i persondatalovens § 8, stk. 1, være fortrolige.

Herudover vil oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold efter omstændighederne kunne være fortrolige.

Endvidere skal det bemærkes, at det blotte forhold, at en borger overhovedet har en sag hos en bestemt myndighed eller har en sag af en bestemt kategori, i sig selv kan være en fortrolig oplysning.

Oplysninger som i forvejen er offentligt tilgængelige, vil som hovedregel ikke være at betragte som fortrolige oplysninger.

Private foreningers eller selskabers interesse i at beskytte oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, vil også kunne føre til, at oplysningerne må anses for at være fortrolige, når væsentlige hensyn til de pågældendes økonomiske interesser tilsiger, at oplysningerne ikke videregives til uvedkommende.

Med hensyn til begrebet fortrolig kan i øvrigt henvises til punkt 2.1.3. "Behandlinger, der er undtaget fra anmeldelse" i Datatilsynets vejledning nr. 125 af 10 juli 2000 om anmeldelse i henhold til kapitel 12 i lov om behandling af personoplysninger.

2. Domme

Vilkår for retsinformationssystemer med videregivelse af domme (Datatilsynets j.nr. 2001-219-0080 og 2001-42-0287)

Forlaget Thomson A/S havde søgt om tilladelse til førelse af forlagets retsinformationssystemer. Anmeldelsen var sket i forlængelse af drøftelser mellem repræsentanter for Datatilsynet og forlaget, herunder for Ugeskrift for Retsvæsen.

I det omfang en dom indeholder følsomme personoplysninger omfattet af persondatalovens §§ 7 og 8, kom Forlaget Thomson A/S med forslag til retningslinjer for, i hvilke tilfælde der skal ske anonymisering.

Sagen blev behandlet i Datarådet, hvorefter Datatilsynet udtalte følgende:

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

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

Et register er i persondatalovens § 3, stk. 1, nr. 3, defineret som "enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på funktionsbestemt eller geografisk grundlag".

Datatilsynet lagde vægt på, at formålet med en domssamling som Ugeskrift for Retsvæsen ikke er at kunne finde frem til oplysninger om bestemte personer, og det indeholder ikke fortegnelser over personnavne eller i øvrigt søgeredskaber, der gør det muligt at foretage målrettet søgning efter oplysninger om bestemte personer. Formålet er alene at formidle domme.

Der var derfor Datatilsynets opfattelse, at papirudgaven af ugeskriftet ikke er at betragte som et register i persondatalovens forstand.

Persondatalovens § 1, stk. 2, om anden ikke-elektronisk behandling indeholder et krav om, at den manuelle behandling skal være systematisk. Dette betyder ifølge bemærkningerne til bestemmelsen, at bestemmelsen ikke omhandler enkeltstående eller mere tilfældige manuelle behandlinger af personoplysninger.

Spørgsmålet om, hvorvidt den manuelle udgave af Ugeskrift for Retsvæsen udgjorde systematisk behandling som beskrevet i lovens § 1, stk. 2, kunne efter Datatilsynets opfattelse give anledning til nogen tvivl.

Imidlertid vil de behandlinger, der ved hjælp af edb foretages med henblik på udgivelsen af den trykte udgave, under alle omstændigheder være omfattet af loven. Dette vil navnlig være tilfældet med hensyn til tekstbehandling af de afsagte domme. Desuden er den elektroniske udgave også under alle omstændigheder omfattet af loven.

Private retsinformationssystemer skal have tilladelse fra Datatilsynet, i det omfang behandlingen er omfattet af anmeldelsespligten i lovens § 48 efter persondatalovens § 50, stk. 1, nr. 5. I den forbindelse kan Datatilsynet efter lovens § 50, stk. 5, fastsætte nærmere vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv.

Retsinformationssystemer som f.eks. Ugeskrift for Retsvæsens retsinformationssystemer er efter Datatilsynets opfattelse af væsentlig samfundsmæssig betydning. Spørgsmålet var således ikke, om Forlaget Thomson A/S skulle have tilladelse eller ej, men alene om på hvilke vilkår tilladelse skulle gives.

Det var Datatilsynets opfattelse, at udgangspunktet måtte være, at der ikke må videregives oplysninger om enkeltpersoners rent private forhold, dvs. følsomme oplysninger omfattet af lovens §§ 7 og 8. Det var dog Datatilsynets opfattelse, at i sager, hvor en fagforening er repræsentant (mandatar) for et medlem af fagforeningen, vil denne oplysning i sig selv ikke kræve, at der skal ske anonymisering.

Med hensyn til de ikke-følsomme oplysninger burde hovedlinien efter Datatilsynets opfattelse være, om der er tale om fortrolige oplysninger. Det må accepteres, at der offentliggøres ikke-fortrolige oplysninger uden nogen form for anonymisering, jf. persondataloven § 6, stk. 1, nr. 5 og 7. Dette svarer til Datatilsynets vilkår vedrørende offentliggørelse af myndigheders afgørelser.

Tilbage stod spørgsmålet om de "fortrolige" oplysninger, hvor der efter Datatilsynets opfattelse i visse tilfælde vil skulle ske anonymisering.

I de af forlaget foreslåede retningslinjer var der ikke taget særligt hensyn til vidner og andre bipersoner. Det var Datatilsynets opfattelse, at også vidner skal nyde beskyttelse i f.eks. straffesager. Tilsynet fandt derfor, at der generelt skulle ske anonymisering i de af Forlaget Thomson A/S foreslåede kategorier, og ikke som foreslået af Forlaget Thomson A/S kun for bestemte grupper inden for disse kategorier. Endvidere burde en kategori med sager om erstatning for uberettiget varetægtsfængsling udvides til at omfatte enhver form for strafferetlig forfølgning.

Datatilsynet fandt endvidere anledning til at medtage et vilkår om, at der yderligere skal ske anonymisering, hvis forholdene særligt tilsiger dette. Datatilsynet ønskede hermed at sikre, at der sker anonymisering af fortrolige oplysninger i de tilfælde, som ikke omfattes af de øvrige vilkår, og hvor videregivelse uden anonymisering ikke kan ske inden for rammerne af lovens § 6, stk. 1, og § 9, stk. 1.

Datatilsynet tilkendegav over for Forlaget Thomson A/S, at tilladelse ville blive givet på følgende vilkår:

1. Der skal ske anonymisering i følgende sager:
   a) I straffesager skal der ske anonymisering. Endvidere skal der ske anonymisering i sager om erstatning i anledning af strafferetlig forfølgning.

b) I ægteskabssager, det vil sige sager om separation, skilsmisse, forældremyndighed og bidragspligt, og i faderskabssager skal der ske anonymisering.
c) I sager om administrativ frihedsberøvelse, i sager om prøvelse af tvangsindlæggelse på en psykiatrisk hospitalsafdeling, i værgemålssager og i sager om anbringelse af børn uden for hjemmet i henhold til bistandsloven skal der ske anonymisering.
d) I fogedsager, sager om konkurser mod enkeltpersoner, i gældssaneringssager og ved ægtefællers fællesbodelinger skal der ske anonymisering.
e) I skattesager, hvor sagen indeholder oplysninger om den pågældende samlede indtægts- eller formueforhold skal der ske anonymisering.
f) I ansættelsessager om bortvisning, hvor bortvisningen eksempelvis er begrundet i strafbare eller lignende forhold hos den ansatte, der er egnet til at nedsætte den ansattes almindelige omdømme skal der ske anonymisering.
g) I erstatningssager, hvor der findes beskrivelse af hændelsesforløb, helbred eller andre personlige forhold, f.eks. diagnoser og sygdomsprognoser skal der ske anonymisering.
h) I lejesager f.eks. sager om ophævelse af lejemål på grund af lejerens adfærd skal der ske anonymisering.
i) I alle sager, der indeholder fortrolige oplysninger, skal der ske anonymisering, hvis særlige forhold tilsiger dette. Dette gælder dog ikke oplysninger om, at en fagforening er repræsentant (mandater) for et medlem af fagforeningen.

2. En eventuel anonymisering består i udeladelse af personnavne, præcise adresseangivelser og eventuelt andre identifikationsoplysninger vedrørende personer. I stedet for de udeladte oplysninger kan der indsættes neutrale betegnelser. Personnumres løbenummer udelades.

3. Domme kan forsynes med sagens journalnummer, sagslistenummer m.v.

4. Der skal etableres sikkerhed for, at der ikke kan tilføjes eller manipuleres med data.

5. Hvis en dom har været behandlet af en højere instans, skal dette samt udfaldet heraf fremgå af gengivelsen af sagen.

6. Det skal kontrolleres, at der ikke er fejl i gengivelsen af dommene. Fejl og lignende skal rettes eller slettes.

7. Datatilsynet skal have underretning om væsentlige ændringer i eller ophør af førelsen af retsinformationssystemet.

Datatilsynet gjorde opmærksom på, at vilkårene er supplerende i forhold til reglerne i persondataloven samt i visse tilfælde udtryk for en præcisering af lovens regler. Det blev derfor understreget, at reglerne i persondataloven finder anvendelse i det omfang, at der er tale om forhold, som ikke er reguleret i de ovenstående vilkår.

Endvidere gjorde tilsynet opmærksom på, at persondataloven finder anvendelse også på den behandling der finder sted forud for offentliggørelsen. Persondataloven finder f.eks. anvendelse på elektronisk behandling, der sker ved redigering og anonymisering af dommene, og hvor persondatalovens sikkerhedsregler, herunder § 41, skal iagttages.

Datatilsynet gjorde afslutningsvis opmærksom på, at persondataloven - med undtagelse af nogle få områder - kun omfatter behandling af personoplysninger. Vilkårene for retsinformationssystemer er derfor kun gældende for behandling af personoplysninger.

Sagen er ikke afsluttet ved redaktionens slutning.

Internationalt arbejde

Internationalt arbejde

Indledning

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

Som beskrevet nærmere i tidligere årsberetninger, senest Datatilsynets Årsberetning for 2000, har der siden 1979 - men især fra 1989 - udviklet sig et omfattende regelsæt på databeskyttelsesområdet, som har fået stadig større betydning for Datatilsynets arbejde. På Datatilsynets hjemmeside er de regelsæt, som nærmere vil blive omtalt, tilgængelige via link under Internationalt.

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

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

Særligt afgørende har dog været udviklingen inden for EU med vedtagelse af direktiver gældende for det indre marked (søjle I-området), blandt andet 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 er omfattet af Amsterdam-traktatens afsnit VI om politisamarbejde og retligt samarbejde i kriminalsager (søjle III-området). Disse konventioner indeholder specifikke regler om persondatabeskyttelse og om tilsyn med overholdelse af disse regler.

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

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

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

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende.

2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører ham/hende, og til berigtigelse heraf.

3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.

Også i 2001 har der været et stort antal internationale sager, blandt andet mange henvendelser om information om dansk lovgivning. Til støtte herfor er lov om behandling af personoplysninger oversat til engelsk. Oversættelsen er tilgængelig på Datatilsynets hjemmeside.

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 2001. Desuden omtales også det mere uformelle, internationale samarbejde, som har udviklet sig gennem årene.

Europarådet

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

Ikrafttræden: Den 1. februar 1990 i Danmark.

I 2001 var det 20 år siden, konventionen blev åbnet for underskrivelse. Dette blev fejret ved afholdelse af en konference i et samarbejde mellem Europarådet og det polske tilsyn (Biuro Generalnego Inspektora Ochrony Danych Osobowych). Konferencens tema var "Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future". På konferencen blev blandt andet behandlet emner om databeskyttelse specielt i de central- og østeuropæiske lande, konventionens relevans i dag specielt i forhold til informationsteknologien, overførsel af oplysninger til tredjelande og den enkelte persons mulighed for at beskytte egne data i en globaliseret verden.

Konferencen var blevet forberedt gennem længere tid af Den rådgivende Komité (Consultative Committee T-PD), som er nedsat i henhold til konventio-

nens artikel 18. Foruden denne opgave har T-PD i 2001 beskæftiget sig med en analyse af konventionsteksten i lyset af de seneste tendenser på databeskyttelsesområdet med henblik på en evaluering af konventionen. Desuden har man behandlet spørgsmålet om overførsel af oplysninger til tredjelande.

Den rådgivende Komité vedtog i 2000 et forslag til tillægsprotokoltekst til konventionen, som vedrører oprettelse af databeskyttelsesmyndigheder og forholdet til tredjelande. Tillægsprotokollen blev i 2001 vedtaget af Ministerkomitéen, og efterfølgende fremlagt til underskrivelse. De 15 lande har i slutningen af 2001 underskrevet tillægsprotokollen.

Ministerkomiteen har i øvrigt den 15. juni 1999 på grundlag af T-PDs forberedelse vedtaget en ændring af konventionen, som gør det muligt for De europæiske Fællesskaber at tiltræde konventionen. Dette er endnu ikke sket.

Databeskyttelsesekspertgruppen (CJ-PD) har blandt andet behandlet problemet med den omsiggribende overvågning af personer og behovet for at opstille retningslinjer for anvendelsen af videoovervågning. Dette er sket på baggrund af en ekspertrapport, der er blevet offentliggjort på Europarådets hjemmeside indeholdende et forslag til "Guiding Principles for the protection of individuals with regard to the collection and processing of personal data by means of video surveillance."

CJ-PD bliver ofte anmodet om at være andre ekspertgrupper i Europarådet behjælpelig med at vurdere, hvorledes reglerne om persondatabeskyttelse bør anvendes. I 2001 drejede det sig blandt andet om arbejdet med et udkast til rekommandation om "Access to official information". Desuden har man på baggrund af vedtagelsen af udkastet til konvention om cybercrime i Den europæiske komite om strafferetlige problemer overvejet, i hvilket omfang der i udkastet er tilstrækkelig beskyttelse af personoplysninger. Konventionen om cyberkriminalitet er i øvrigt efter vedtagelse i Ministerkomiteen i november 2001 fremlagt til underskrivelse.

På grund af manglende økonomiske ressourcer har Europarådet i nogen tid måttet foretage indskrænkninger i mødeaktiviteterne for både T-PD og CJ-PD, således at der kun har kunnet afholdes plenarmøder en gang årligt. Dette har haft væsentlig indflydelse på den effektivitet, hvormed der har kunnet arbejdes. På denne baggrund har T-PD og CJ-PD i 2001 afholdt et fælles møde, hvor man har drøftet mulighederne for omstrukturering af de to organers arbejdsform og ændringer i beslutningskompetence. Arbejdet hermed vil blive fortsat.

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

Europol-konventionen

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

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

Formål: Gennem oprettelse af en europæisk politienhed med en national enhed i hver EU-medlemsstat at forbedre effektiviteten hos medlemsstaternes kompetente myndigheder og disses samarbejde om forebyggelse og bekæmpelse af blandt andet 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 2001 afholdt 7 møder, hvor man blandt andet har behandlet spørgsmål, som vedrører oprettelse af analysedatabaser, se konventionens artikel 10 og artikel 12, og relationerne til Europol. Desuden er arbejdet i en række arbejdsgrupper, hvori deltager 3-5 af kontrolinstansens medlemmer, fortsat. I disse arbejdsgrupper behandles spørgsmål, som kræver grundig forberedelse forud for plenarmøderne. Datatilsynet deltager i en arbejdsgruppe, som beskæftiger sig med regel- og procedurespørgsmål. Her har man også i 2001 forberedt udkast til kontrolinstansens udtalelser vedrørende forberedelse af de aftaler, som Europol efter EU-Rådets bemyndigelse skal indgå med tredjelande og internationale organisationer, se konventionens artikel 18.

Derudover har Den Fælles Kontrolinstans godkendt en undergruppes inspektionsrapport vedrørende Den fælles Kontrolinstans' inspektion af Europol i november 2000. Af særlige spørgsmål der har været drøftet i årets løb skal især nævnes spørgsmålet om medlemsstaternes operationelle projekter, der gennemføres på mellemstatsligt niveau med bistand fra Europol. Som følge af terrorangrebene mod USA den 11. september 2001 har spørgsmålet om Euro-

pols samarbejde med USA været genstand for drøftelse i Den fælles Kontrolinstans.

Det Fælles Klageudvalg har i år 2001 afholdt en række møder, hvor man blandt andet har behandlet to klagesager fra fysiske personer. De pågældende personer har klaget over, at de ikke har kunnet få oplyst, hvorvidt Europol har registreret oplysninger om dem. Ved redaktionens slutning var ingen af disse sager endeligt afgjort.

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 blandt andet opfyldes ved hjælp af udveksling af oplysninger og erfaringer til brug for de enkelte landes bekæmpelse af kriminalitet.

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

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

Ikrafttræden: Folketinget bemyndigede ved lov nr. 418 af 10. juni 1997 om Danmarks tiltrædelse af Schengen-konventionen regeringen til at ratificere til-

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

Arbejdsopgaver: I henhold til konventionens artikel 115 er der nedsat en fælles tilsynsmyndighed, der blandt andet 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 Schengensamarbejdet har Danmark deltaget i møderne som medlem.

Der er i 2001 afholdt 4 møder. Den fælles Tilsynsmyndighed har i januar 2002 afgivet sin 5. aktivitetsrapport for perioden marts 2000 til december 2001. Rapporten er tilgængelig på Datatilsynets hjemmeside. I øvrigt har Den fælles Tilsynsmyndighed i år 2001 udarbejdet en rettighedshåndbog, beskæftiget sig med spørgsmål vedrørende udviklingen af SIS II samt forberedt en inspektion af den centrale SIS støttedatabase (C.SIS) i Strasbourg. Det forventes, at inspektionen kan afholdes i 2002.

Registertilsynet - nu Datatilsynet - er udpeget som tilsynsmyndighed efter konventionens artikel 114 og 128, jf. gennemførelseslovens § 2, stk. 3, hvilket blandt andet 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 told området

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 midlertidig 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 år 2001 blev der afholdt et møde i den fælles tilsynsmyndighed, hvor man vedtog en foreløbig forretningsorden. Det forventes, at det egentlige arbejde i myndigheden kan starte i løbet af år 2002.

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

Sekretariatet for de fælles tilsynsmyndigheder

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

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

Ved afgørelsen har de fælles tilsynsmyndigheder fået mulighed for at fungere mere effektivt, og samtidig kan det opnås at nedbringe omkostningerne. Det er udtrykkeligt fastslået, at databeskyttelsessekretariatet skal være uafhængigt, idet det ved udførelsen af sine opgaver kun er bundet af instrukser fra de fælles tilsynsmyndigheder. Af praktiske grunde er databeskyttelsessekretariatets administration dog tæt knyttet til Generalsekretariatet for Rådet.

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

Napoli II-konventionen

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

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

Ikrafttræden: Konventionen blev undertegnet den 18. december 1997. Ved udgangen af år 2001 havde 6 lande ratificeret konventionen. Danmark har endnu ikke ratificeret konventionen. Napoli II-konventionen erstatter konventionen af 7. september 1967 om gensidig bistand mellem EU-landenes toldforvaltninger (Napoli I-konventionen), der blev tiltrådt af Danmark i forbindelse med indtrædelsen i EF i 1973. Napoli I-konventionen ophæves ved ikrafttrædelsen af Napoli II-konventionen.

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

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

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

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

Eurodac-systemet

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

Registertilsynet afgav allerede i 1999 en udtalelse til Udlændingestyrelsen om et forslag fra Kommissionen til en Rådsforordning om oprettelse af Eurodac. Arbejdet med oprettelse af Eurodac-systemet går imidlertid helt tilbage til marts 1996, hvor EU's medlemsstater indledte forhandlinger om en konvention om oprettelse af et definitivt identifikationssystem baseret på sammenligning af asylansøgeres fingeraftryk. Dette arbejde blev formelt set afsluttet i december 1998, hvor man i Rådet nåede til enighed om at "fastfryse" teksten, indtil Amsterdam-traktaten var trådt i kraft.

Medlemsstaterne udarbejdede desuden et udkast til protokol, som skulle lette anvendelsen af Dublin-konventionen yderligere ved at fastsætte bestemmelser om indsamling af fingeraftryksoplysninger om personer, der pågribes i forbindelse med ulovlig overskridelse af en ydre grænse. Rådet nåede ligeledes til enighed om udkastet til protokollen og blev i marts 1999 enige om også at "fastfryse" denne tekst.

Det område, som de fastfrosne tekster omfatter, nemlig asylspørgsmålet, hører nu ind under artikel 63, nr.1, litra a) i traktaten om oprettelse af Det Europæiske Fællesskab (søjle I). I forbindelse med Rådets fastfrysning af de ovenfor nævnte tekster fik Kommissionen mandat til efter Amsterdam-traktatens ikrafttræden at fremsætte forslag til en fællesskabsretsakt omfattende disse tekster.

Af særlig interesse kan nævnes, at det i forordningen er bestemt, at der midlertidigt skal oprettes en uafhængig fælles tilsynsmyndighed, som skal kontrollere den centrale enheds behandling af personoplysninger, indtil den uaf-

hængige kontrolinstans, der er omhandlet i EU-traktatens artikel 286, er blevet oprettet, se herom nedenfor.

Datatilsynet må forventes at blive udpeget som den nationale tilsynsmyndighed.

Det generelle databeskyttelsesdirektiv

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

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

Art. 29-gruppen har i 2001 afholdt 5 to-dagsmøder. Gruppen har også i 2001 vedtaget en række henstillinger, udtalelser m.v. Der er således vedtaget dokumenter om standardkontraktbestemmelser for overførsel af personoplysninger til dataansvarlige og databehandlere etableret i tredjelande. Gruppen har vedtaget dokumenter om cyberkriminalitet (WP 41 og WP 51) og behandling af personoplysninger i ansættelsesforhold (WP 48).

Endvidere har gruppen vedtaget dokumenter om beskyttelsesniveauet af persondata i Canada (WP 39) og Australien (WP 40) og om visse minimumskrav til onlineindsamling af personoplysninger i EU (WP 43).

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

Som en konsekvens af vedtagelsen af det generelle databeskyttelsesdirektiv gennemføres i øvrigt i EU-Rådets økonomigruppe (Databeskyttelse) koordine-

ring af medlemsstaternes holdninger forud for behandling af spørgsmål i Europarådet, som falder inden for direktivets område. Datatilsynet er rådgiver i denne sammenhæng og har i visse tilfælde deltaget i møderne.

Databeskyttelse internt i EU-/EF-institutionerne

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

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

Formålet: Hensigten med forordningen er, at regler svarende til det generelle databeskyttelsesdirektiv og til direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren skal gælde for fællesskabets institutioner og organer i lighed med de nationale gennemførselsbestemmelser for medlemsstaterne. Forordningen indeholder tillige bestemmelser om oprettelse af en uafhængig kontrolmyndighed.

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

Europa-Parlamentet og Rådet udnævner efter fælles aftale den europæiske tilsynsførende for en periode på fem år på grundlag af en liste, Kommissionen opstiller efter et offentligt stillingsopslag.

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 årligt afholdte internationale konference. Sekretariatsfunktionen varetages af det land, der sidst har afholdt den årlige konference.

I 2001 afholdt man den årlige EU-datatilsynskonference i Athen, arrangeret af det græske tilsyn (Hellenic Data Protection Authority). På konferencen drøftedes en række spørgsmål af fælles interesse, blandt andet beskyttelse af ansatte, udveksling af oplysninger med tredjelande, databeskyttelse i telekommunikationssektoren, elektronisk handel og samtykke som hjemmel til behandling af personoplysninger.

Konferencen afgav desuden - lige som sidste år - en særlig udtalelse vedrørende "Retention of Traffic Data by Internet Service Providers (ISPs)". I udtalelsen er udtrykt bekymring for, at ISPs rutinemæssigt skal opbevare trafikdata ud over nødvendige formål for at kunne give mulig adgang hertil for retshåndhævende myndigheder. Konferencen afgav endvidere en udtalelse vedrørende artikel 8 af the EU Charter of Fundamental Rights. I udtalelsen er udtrykt tilfredshed med indførelsen af artikel 8, hvormed databeskyttelse er blevet en grundlæggende menneskeret.

International konference for datatilsynsmyndigheder

Det 23. årlige internationale møde for datatilsynsmyndighederne blev i september 2001 afholdt i Paris, arrangeret af det franske tilsyn (Commission Nationale de l´Informatique et des Libertés). På konferencen beskæftigede man sig med en række emner af fælles interesse, herunder blandt andet biometrics og ansigtsgenkendelse, teknikker til positionsbestemmelse, cyberkriminalitet og e-handel.

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 Akteneinsicht). Ar-

bejdsgruppen 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. På møderne vedtages blandt andet en række fælles holdninger (Common Positions) til emner, som er taget op til behandling efter ønske fra et eller flere af medlemmerne. Disse fælles holdninger kan anvendes i det videre konkrete arbejde med lovgivning eller fastlæggelse af praksis, som behandles internationalt eller nationalt.

Gruppens rapporter og publikationer er tilgængelige på tysk eller engelsk på Berlins Datatilsyns hjemmeside (http://www.datenschutzberlin.de/doc/int/iwgdpt/index.htm). Gruppen og dens dokumenter beskrives nærmere på Datatilsynets hjemmeside under menupunktet Internationalt.

Nordisk samarbejde

Det nordiske samarbejde mellem datatilsynsmyndighederne i Danmark, Finland, Island, Norge og Sverige er blevet fortsat, og i 2001 stod det islandske Datatilsyn for afholdelse af det fællesnordiske datachefmøde.

På mødet udvekslede deltagerne oplysninger om såvel generelle som konkrete afgørelser. Blandt andet diskuterede deltagerne særlige spørgsmål i tilknytning til det generelle direktivs gennemførelse i de nordiske lande, blandt andet lovenes anvendelsesområde og anmeldelsesordninger i de forskellige lande.


WRITE ENABLE
WRITE PROTECT

Sikkerhedsspørgsmål

Sikkerhedsspørgsmål

Persondatalovens krav om datasikkerhed

Af persondatalovens § 41, stk. 3, fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

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

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

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

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

Konklusionen har været, at de beskrevne sikkerhedskrav bør følges, både når den dataansvarlige er en offentlig myndighed, og når der er tale om en privat virksomhed m.v. Det er således Datatilsynets opfattelse, at persondatalovens § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i private virksomheder m.v. som i den offentlige forvaltning. Eksempelvis gælder dette ved transmission af personoplysninger over det åbne internet. Efter Datatilsynets opfattelse bør der ved transmission af oplysninger om personnumre over det åbne internet som minimum foretages kryptering. Der bør også foretages kryptering, hvis andre oplysninger, som må betragtes som fortrolige (f.eks. oplysninger om økonomiske forhold og lignende), transmitteres.

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

I det følgende omtales 2 sager, hvor navnlig spørgsmål om opfyldelse af lovens sikkerhedskrav har været behandlet.

Sletning af oplysninger lagret på en harddisk

Udtalt, at Datatilsynet fandt det yderst kritisabelt, at der alene var udført en formatering af en række harddiske, inden disse blev videresolgt til udlandet, idet dette ikke kunne betragtes som en effektiv sletning af de personoplysninger, der var lagret på diskene (Datatilsynets j.nr. 2000-631-0057 og 2001-631-0062)

Datatilsynet blev i slutningen af december 2000 gennem pressen opmærksom på, at harddiske som tidligere havde tilhørt en række danske virksomheder og foreninger, tilsyneladende var dukket op i handelen i udlandet, uden at oplysningerne på harddiskene var blevet effektivt slettet.

De pågældende virksomheder m.v. havde overladt det til et firma (en databehandler) at foretage sletning af de afleverede harddiske og indgået kontrakter, der forpligtede det databehandlende firma til at foretage en effektiv sletning af harddiskene, inden disse blev videresolgt.

Efter en nærmere undersøgelse af sagen kunne Datatilsynet konstatere, at oplysninger var kommet til uvedkommendes kendskab i strid med persondataloven, idet de harddiske, hvorpå oplysningerne var lagret, ikke var blevet effektivt slettet inden de blev videresolgt.

Dette skyldtes i det væsentligste det databehandlende firmas forhold, idet firmaet ikke havde sørget for at foretage den nødvendige sletning og derved handlet i strid med de instrukser, som de afleverende virksomheder m.v. havde givet, jf. herved persondatalovens § 41, stk. 1. Det databehandlende firma havde heller ikke truffet de sikkerhedsforanstaltninger, som de i henhold til persondatalovens § 41, stk. 3, var selvstændigt forpligtede til at træffe. Datatilsynet fandt dette yderst kritisabelt.

Sagen rejste endvidere spørgsmål om det ansvar, man som dataansvarlig i medfør af lovens § 42, stk. 1, har til at føre kontrol med de behandlinger, som man overlader til en databehandler. Datatilsynet udtalte, at den praktiske udførelse og omfanget af en sådan kontrol i sidste ende beroede på en konkret vurdering af den behandling, som er overladt til databehandleren. Sagens hændelsesforløb viste, at det havde været rigtigst, om der fra den dataansvarliges side var blevet udført en vis kontrol med sletningen, f.eks. i form af stikprøver.

Endelig rejste sagen spørgsmål om overførsel af oplysninger til tredjelande, idet det databehandlende firma overførte harddiskene til Litauen, inden sletning blev foretaget. Datatilsynet fandt, at det var en forudsætning for den konkrete overførsel, at Litauen i denne sammenhæng kunne betragtes som et sikkert tredjeland i persondatalovens forstand. Det databehandlende firma skulle derfor være opmærksom på, at overførslen ikke måtte medføre en væsentlig forringelse af den beskyttelse af de registrerede, som persondataloven tilsigter at give.

Sikkerhedskrav til elektronisk signatur

Udtalt, at der som udgangspunkt i tilfælde, hvor elektroniske certifikater er påkrævet, må kræves kvalificerede certifikater. I konkrete tilfælde vil dette dog kunne fraviges, idet der til et konkret afgrænset sagsområde også vil kunne anvendes dedikerede certifikater, som - i forhold til persondatalovens krav - må anses for tilstrækkeligt sikre (Datatilsynets j.nr. 2001-232-0066)

Dafolo A/S rettede på vegne af tre nordjyske kommuner henvendelse til Datatilsynet for at få belyst tilsynets holdning til, hvilke typer af certifikater man anser for tilstrækkeligt sikre til en konkret anvendelse.

Det var planen at etablere to former for elektronisk selvbetjening via de tre nordjyske kommuners hjemmesider. Disse ville udgøre dels selvbetjening via elektroniske blanketter dels direkte adgang til egne data/dokumenter, hvor borgere og virksomheder skulle kunne følge en sags gang gennem det offentlige system. Projektet ville fra begyndelsen rumme data vedrørende tre sagsområder, hvoraf det ene ville indeholde en række følsomme oplysninger.

Det følger af lov om behandling af personoplysninger (persondataloven) § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Ifølge bekendtgørelse nr. 528 af 15. juni 2000 (sikkerhedsbekendtgørelsen) må der kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger, jf. § 14.

I forbindelse med selvbetjeningsløsninger skal der samlet set være den fornødne sikkerhed for, at personoplysninger ikke kommer uvedkommende i hænde, og at personoplysninger ikke forringes eller tilintetgøres.

Datatilsynet har tidligere givet udtryk for den generelle holdning, at der i forbindelse med den registreredes indsendelse af fortrolige oplysninger som minimum skal anvendes brugerid og adgangskode. Ved indsendelse af følsomme oplysninger ville det afhænge af de nærmere omstændigheder i det konkrete tilfælde, hvorvidt anvendelse af certifikat/digital signatur anbefales.

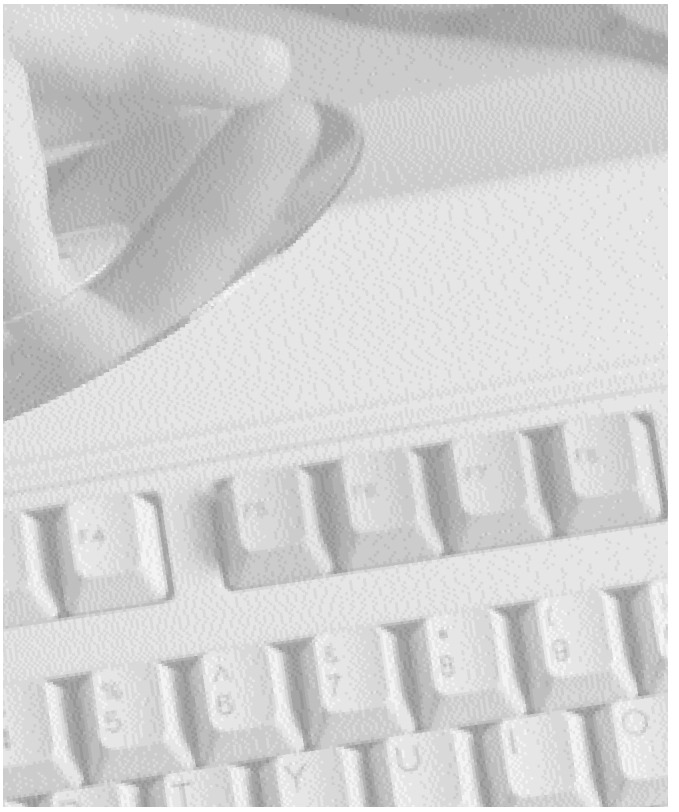
Når det drejer sig om adgang til oplysninger - det enten være sig i form af den registreredes indsigt i oplysninger om sig selv eller videregivelse af oplysninger til tredjemand - vil anvendelse af brugerid og adgangskode normalt være tilstrækkeligt. Ved adgang til følsomme oplysninger vil det afhænge af de nærmere omstændigheder i det konkrete tilfælde, hvorvidt anvendelse af certifikat/digital signatur anbefales.

Sagen blev behandlet på et møde i Datarådet, og Datatilsynets udtalte, at der efter Datatilsynets opfattelse i tilfælde, hvor certifikater er påkrævet, som udgangspunkt må kræves kvalificerede certifikater. I konkrete tilfælde kan dette dog fraviges.

Datatilsynet fandt, at det certifikat, som de tre kommuner påtænker at anvende - i forhold til persondatalovens krav - må anses for tilstrækkeligt sikkert for anvendelse i de tre konkrete sagsområder under forudsætning af, at certifikaterne er fremstillet efter samme retningslinjer som kvalificerede certifikater, dog bortset fra kravet om underskriverens (rekvirentens) fremmøde i forbindelse med identitetskontrol ved udstedelsen. Identitetskontrollen skal dog indebære andre foranstaltninger til sikring af underskriverens identitet, f.eks. at udsteder kontrollerer, at den adresse, hvortil PIN-koder m.v., som skal anvendes til aktivering af certifikatet, sendes, er identisk med den pågældende persons folkeregisteradresse.

.....

Datatilsynet har siden i forbindelse med en forespørgsel fra Ministeriet for Videnskab, Teknologi og Udvikling udtalt, at et såkaldt OCES certifikatet - i relation til persondataloven - generelt vil kunne benyttes ved borgernes indsendelse af oplysninger til myndighederne. Sagen er beskrevet på tilsynets hjemmeside.



Tilsynsvirksomhed

Tilsynsvirksomhed

Generelt om Datatilsynets inspektioner

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

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

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

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

Datatilsynets har mulighed for at gennemføre uanmeldte inspektioner. I praksis varsles inspektionerne 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 omfat-

tet af tilladelseskravet i lovens § 50 samt til edb-servicevirksomheder omfattet af anmeldelsespligten i lovens § 53. Se evt. nærmere i afsnittet "Inspektioner hos private virksomheder" nedenfor.

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

I de følgende afsnit omtales indberetninger om overtrædelser af loven samt forskellige typer af inspektioner. I sidste afsnit findes en samlet oversigt over udførte inspektioner i 2001.

Indberetninger om overtrædelser af loven

I 2001 fandt Datatilsynet i et enkelt tilfælde anledning til at afgive indberetning til en kommunalbestyrelse om overtrædelser af persondataloven. Indberetningen blev foretaget på baggrund af en inspektion udført i år 2000. Inden redaktionens slutning har Datatilsynet desuden foretaget indberetning til Rigspolitichefen på baggrund af en inspektion hos Kalundborg Politi afholdt i december måned 2001. De to sager gengives nedenfor. I øvrigt var alle sager vedrørende inspektioner afholdt i 2001 endnu ikke afsluttet ved redaktionens slutning.

Indberettet Bogense Kommune for ikke at have fastsat forskrifter for to konkrete systemer i henhold til den tidligere gældende lov om offentlige myndigheders registre og for ikke at have foretaget anmeldelse af de pågældende systemer efter reglerne i lov om behandling af personoplysninger kapitel 12. Endvidere udtalt, at kommunens længerevarende manglende iagttagelse af kravet om logning var særdeles kritisabel (Datatilsynets j.nr. 2000-623-0003)

Under en inspektion i Bogense Kommune blev det blandt andet oplyst, at kommunens social- og sundhedsforvaltning gennem mere end 11 år havde anvendt et journalsystem indeholdende detaljerede følsomme personoplysninger. I systemet var det ikke muligt at foretage logning, ligesom der ikke havde været fastsat registerforskrifter for systemet i henhold til den tidligere gældende lov om offentlige myndigheders registre. I øvrigt var systemet heller ikke anmeldt efter reglerne i kapitel 12 i lov om behandling af personoplysninger.

Endvidere blev det oplyst, at kommunen i ca. 10 år i tilknytning til hjemmeplejen havde anvendt et system, for hvilket der ikke var fastsat registerforskrifter eller foretaget anmeldelse i henhold til lov om behandling af personoplysninger.

Bogense Kommune oplyste overfor Datatilsynet, at den manglende fastsættelse af forskrifter i henhold til lov om offentlige myndigheders registre skyldtes manglende agtpågivenhed.

Kommunen oplyste endvidere, at der var truffet foranstaltninger til implementering af nye systemer på de pågældende områder, samt at kommunens it-sikkerhedspolitik var godkendt af byrådet i marts 2001.

Datatilsynet foretog på den baggrund indberetning til Kommunalbestyrelsen i Bogense Kommune af de konstaterede overtrædelser og udtalte i den forbindelse kritik af Bogense Kommunes manglende opfyldelse af reglerne i såvel reglerne i lov om behandling af personoplysninger kapitel 12 som den tidligere lov om offentlige myndigheders registre. Samtidig fandt Datatilsynet, at kommunens undladelse af at træffe de fornødne sikkerhedsforanstaltninger var særdeles kritisabel.

Bogense Kommune har efterfølgende foretaget anmeldelse i overensstemmelse med kapitel 12 i lov om behandling af personoplysninger af to systemer i henholdsvis social- og sundhedsforvaltningens og hjemmeplejens regi. I forbindelse med anmeldelserne har kommunen oplyst, at de to systemer opfylder kravene i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Datatilsynet har taget anmeldelserne til efterretning og afventer nu, at Bogense Kommune foretager de resterende anmeldelser i forhold til lov om behandling af personoplysninger kapitel 12.

Indberettet Kalundborg Politi til Rigspolitichefen for at have registreret oplysninger om strafbare forhold i forbindelse med bandekriminalitet, uden at der var foretaget logning (Datatilsynets j.nr. 2001-621-0016)

Under en inspektion hos Kalundborg Politi konstaterede Datatilsynet blandt andet, at Kalundborg Politi i de sidste ca. 2 1/2 år havde registreret oplysninger i et dokument benævnt "Bandekriminalitet", uden at foretage en logning, der opfylder de tidligere gældende krav i lov om offentlige myndigheders registres § 12 samt de gældende regler i sikkerhedsbekendtgørelsens (bekendtgørelse nr. 528 af 15. juni 2000) § 19, stk. 1.

Datatilsynet konstaterede endvidere i forbindelse med behandling af anmeldelser i henhold til persondatalovens § 45, stk. 1, nr. 1, jf. § 43, fra Esbjerg og Assens Politi tilsvarende overtrædelser af sikkerhedsbekendtgørelsens § 19, stk. 1.

Da disse overtrædelser af persondatalovens og sikkerhedsbekendtgørelsens regler var af en vis alvor, fandt Datatilsynet anledning til at give Rigspolitiet meddelelse herom.

Datatilsynet meddelte Rigspolitiet, at de omhandlede sager efter Datatilsynets opfattelse gav indtryk af, at der er behov for større viden i politikredsene om persondatalovens og sikkerhedsbekendtgørelsens krav, særligt i forbindelse med kredsenes etablering af egne "systemer" i almindelige tekstbehandlingsdokumenter, intranet o.lign.

Datatilsynet har anmodet om underretning om, hvad Rigspolitiet vil gøre i anledning af de konstaterede overtrædelser af persondataloven. Sagen var ikke afsluttet ved redaktionens slutning.

Inspektioner hos offentlige myndigheder

En inspektion hos en offentlig myndighed gennemføres ved en samtale med myndighedens repræsentanter med udgangspunkt i myndighedens anmeldelser samt myndighedens beskrivelse af uddybende sikkerhedsforanstaltninger. Datatilsynets repræsentanter inspicerer desuden de fysiske faciliteter, der danner ramme for myndighedens behandling af personoplysninger. I forbindelse med samtalen får myndigheden lejlighed til at stille spørgsmål til Datatilsynets repræsentanter. Datatilsynet lægger vægt på også at benytte inspektionerne til at komme i dialog med myndighederne. Inspektionen afsluttes med, at Datatilsynet sender et brev til myndigheden, hvori resultatet af inspektionen meddeles.

Datatilsynet har i årets løb blandt andet konstateret og påtalt følgende forhold:

- Der er ikke blevet foretaget anmeldelser i henhold til persondatalovens kapitel 12
- Printere og skærme står tilgængelige for publikum, således at udskrevet materiale samt oplysninger på skærmbilledet kan læses af uvedkommende
- Kapitel 3 i sikkerhedsbekendtgørelsen er ikke opfyldt, idet der ikke kan logges eller betingelserne for undtagelse fra logningskravet ikke er opfyldt
- Dokumenter med personoplysninger i papirkurve er tilgængelige for besøgende

Det har været et gennemgående træk ved årets inspektioner hos offentlige myndigheder, at myndighedernes nye "Uddybende sikkerhedsregler" har givet Datatilsynet anledning til bemærkninger. Sikkerhedsreglerne har ofte været udformet således, at de nærmest antager karakter som bestemmelserne i sikkerhedsbekendtgørelsen, i stedet for, som det klart fremgår af sikkerhedsbekendtgørelsens § 5, at uddybe bekendtgørelsens bestemmelser.

Hovedformålet med den dataansvarlige myndigheds uddybende sikkerhedsregler er at dokumentere, hvorledes sikkerhedsbekendtgørelsens enkelte bestemmelser er opfyldt netop hos denne myndighed. Det kan tilføjes, at der ikke er krav om, at denne dokumentation skal foreligge i form af et enkelt, samlet dokument, men kan meget vel bestå af et overordnet dokument med referencer til andre, eksisterende dokumenter såsom beskrivelser, instrukser m.v.

I de pågældende tilfælde har Datatilsynet ved inspektionen givet en vejledning herom og har i den efterfølgende udtalelse henstillet, at myndigheden snarest udfærdiger de uddybende sikkerhedsregler i overensstemmelse med loven.

Inspektioner hos private virksomheder

Datatilsynets inspektionskompetence i forhold til private virksomheder er begrænset til de tilfælde, hvor der er sker behandling omfattet af tilladelseskravet i lovens § 50 samt til edb-servicevirksomheder omfattet af anmeldelsespligten i lovens § 53.

Kort fortalt betyder dette, at Datatilsynet har inspektionsadgang hos private virksomheder m.v. og forskere i følgende tilfælde

- Dataansvarlige der behandler følsomme oplysninger omfattet af lovens § 7 eller § 8 (f.eks. forsikringsselskaber, kontaktbureauer og private forskere)
- Advarselsregistre, herunder også såkaldte spærrelister i forbindelse med betalingskort
- Kreditoplysningsbureauer
- Stillingsbesættende virksomheder (headhuntere)
- Retsinformationssystemer
- Edb-servicebureauer

Datatilsynet har i 2001 primært foretaget inspektioner af kontaktbureauer, kreditoplysningsbureauer og private forskere (se evt. næste afsnit om "Inspektioner af private forskningsprojekter"). Datatilsynet har herudover foretaget inspektioner hos forskellige andre private virksomheder. Der er således foretaget inspektioner af enkelte forsikringsselskaber, stillingsbesættende virksomheder, virksomheder der fører en spærreliste og enkelte konsulentvirksomheder, som behandler følsomme oplysninger omfattet af persondatalovens § 7 og § 8.

En inspektion i en privat virksomhed gennemføres ved en samtale med virksomhedens repræsentanter baseret på et spørgeskema udarbejdet på baggrund af den behandling, den pågældende virksomhed foretager. Datatilsynet inspicerer også de fysiske faciliteter, der danner ramme for behandlingen. I

forbindelse med samtalen får virksomheden lejlighed til at stille spørgsmål til Datatilsynets repræsentanter. Inspektionen indebærer derfor både tilsyn med virksomhedens behandling og rådgivning og vejledning af virksomheden i, hvorledes behandling af personoplysninger bedst kan ske i overensstemmelse med persondatalovens regler.

Det er Datatilsynets erfaring, at virksomhederne i de fleste tilfælde har en egen interesse i at behandle personoplysninger i overensstemmelse med persondataloven. Dette skyldes, at virksomhederne lægger stor vægt på, at aktuelle og potentielle kunder kan have tillid til virksomhedens behandlinger. Særligt i forbindelse med anskaffelse og opsætning af diverse tekniske sikkerhedsforanstaltninger, er de private virksomheder således ofte ganske langt fremme.

Datatilsynet har derfor ikke i forbindelse med de inspektioner hos private virksomheder, som tilsynet har foretaget i 2001, fundet anledning til at udtale alvorlig kritik. Alle inspektioner med undtagelse af én er endvidere afholdt planmæssigt. I det ene tilfælde, hvor Datatilsynet var blevet oplyst en forkert adresse, har Datatilsynet udtalt, at det var beklageligt, at Datatilsynet ikke havde mulighed for at foretage den planlagte inspektion af den pågældende virksomhed. Inspektionen er dog planlagt gennemført i 2002.

Inspektioner af private forskningsprojekter

Private forskningsprojekter er anmeldelsespligtige og skal have Datatilsynets tilladelse, hvis der behandles følsomme oplysninger - f.eks. helbredsoplysninger - om deltagerne, og hvis disse kan identificeres.

Datatilsynet fastsætter en række vilkår for tilladelsen, og formålet med inspektionerne er således at undersøge, hvorvidt de dataansvarliges behandlinger af personoplysninger udføres i overensstemmelse med persondataloven og med de vilkår, som Datatilsynet har fastsat for behandlingerne.

Kontrollen gennemføres som konkrete inspektioner af udvalgte projekter. En inspektion finder sted på den adresse, hvor oplysningerne opbevares og behandles. Datatilsynet inspicerer således projekter på hospitaler, universiteter, højskoler m.v., og projekter, der gennemføres i private hjem.

Datatilsynet gennemførte de første inspektioner hos private forskere i efteråret 2000, og har i løbet af 2001 foretaget 27 inspektioner hos private forskere.

Datatilsynet har ved planlægningen af årets inspektioner tilstræbt, at der er sket en vis geografisk variation, ligesom det er tilstræbt, at der er besøgt en variation af private forskere, dvs. lige fra erfarne forskere til studerende til

private virksomheder. Tilsynet har således aflagt besøg blandt andet i Århus, Ålborg, Randers, Næstved, Køge, Humlebæk, Hvidovre samt på en række steder i Københavnsområdet.

Inspektionerne er tillige blevet afholdt dels på arbejdspladser på offentlige sygehuse dels hos private virksomheder og i private boliger.

På grundlag af de gennemførte inspektioner er det tilsynets erfaring, at forskerne - i det store og hele - overholder de fastsatte vilkår og lever op til vilkårenes intentioner. Det er desuden tilsynets klare opfattelse, at forskernes holdning til datasikkerhed er meget god, og at der i forbindelse med håndtering af data generelt udvises stor agtpågivenhed.

Datatilsynet har indtil nu ikke fundet anledning til udtale alvorlig kritik i forbindelse med inspektionerne. Også gennemførelsen af inspektioner i private hjem er forløbet planmæssigt og har ikke givet anledning til bemærkninger eller påtale af alvorlig karakter.

Datatilsynet har ved enkelte inspektioner, navnlig hos hospitalsansatte forskere, påtalt forskernes manglende adgang til separat aflåselige arkivrum, kontorer eller tilsvarende faciliteter til opbevaring af manuelt projektmateriale med personoplysninger.

Det skal i den forbindelse understreges, at en opbevaring af projektmateriale under tilsvarende forhold som f.eks. afdelingens patientjournaler, ikke nødvendigvis sikrer overholdelse af Datatilsynets krav til datasikkerheden i projektet. Her stilles der krav om, at manuelt projektmateriale med personoplysninger skal opbevares "forsvarligt aflåst og på en sådan måde at uvedkommende ikke kan gøre sig bekendt med indholdet". Med uvedkommende menes personer, der ikke deltager i gennemførelsen af det konkrete projekt. Afdelingens personale, kontorfæller eller kolleger, som man tilfældigvis deler skab med, vil i den sammenhæng være uvedkommende personer, såfremt de ikke deltager i det konkrete projekt.

Datatilsynet har ved enkelte inspektioner måttet præcisere, at det er af afgørende betydning for inspektionens gennemførelse, at den ansvarlige for projektet er tilstede og kan redegøre for de faktiske forhold i projektet.

Oversigt over udførte inspektioner i 2001

Datatilsynet har i år 2001 foretaget i alt 76 inspektioner, heraf 15 hos statslige myndigheder, 18 i kommuner, 16 hos forskellige private virksomheder og 27 vedrørende privat forskning.

Inspektioner hos offentlige myndigheder

Staten:
Arbejdsskadestyrelsen
Indenrigsministeriet, CPR-kontoret
Indenrigsministeriets Departement
Kulturministeriets Departement
Politimesteren i Glostrup
Politimesteren i Kalundborg
Politimesteren i Slagelse
Politimesteren i Tårnby
Rigspolitiet, SIRENE kontoret (NSIS)
Socialministeriets Departement
Statsamtet København
Statsamtet Roskilde
Trafikministeriets Departement
Udlændingestyrelsen
Økonomiministeriets Departement

Kommuner:
Blåbjerg
Fuglebjerg
Herlev
Holmsland
Hvidovre
Hvorslev
Hårby
Lunderskov
Lyngby-Tårbæk
Purhus
Randers
Tårnby
Vallensbæk
Vamdrup
Vejle
Ølgod
Årup
Åskov

Inspektioner i private virksomheder m.v.

Advarselsregistre og spærrelister:
Danske Biludlejere (advarselsregister)
Kuwait Petroleum A/S, Q8 (spærreliste)

Kreditoplysningsbureauer:
Dansk Kreditorservice
Dun & Bradstreet Danmark A/S
RKI Kredit Information A/S

Kontaktbureauer:
bompi.dk (kontaktbureau)
Kontaktnet (kontaktbureau)
Scor.dk (kontaktbureau)
Webdate (kontaktbureau)

Stillingsbesættende virksomheder:
Access Personel A/S
Master Management Danmark

Andre:
Dansk Mental Hygiejnecenter
Lærerstandens Forsikring
Netdoktor
Roche A/S
Trekroner forsikring

Privat Forskning:
Konsulent Jytte Therkildsen
Overlæge Asbjørn Mohr Drewes, Aalborg Sygehus
Overlæge Conni Fensbo, Aalborg Psykiatrisk Sygehus
Læge Peter Vestergaard, Århus Amtssygehus
Sygeplejerske Henriette Vind Hansen, Århus Amtssygehus
Tandplejechef Dorte Blume Møbak
Læge Jens Peter Bonde, Århus Kommunehospital
Afdelingslæge Grethe Schmidt, Rigshospitalet
Forskningsadjunkt Susanne Bügel, Forskningsinstitut for Human Ernæring
Overlæge Preben Philip, Næstved Centralsygehus
Adm. Overlæge Jette Jansen, Næstved Centralsygehus
Læge, ph.d. studerende Mette Hitz, Roskilde Amtssygehus Køge
Ole Raaschou-Nielsen, Kræftens Bekæmpelse, Forskningsafdelingen
Videnskabelig medarbejder Johnni Hansen, Kræftens Bekæmpelse, Forskningsafdelingen
Overlæge Jørgen H. Olsen, Kræftens Bekæmpelse, Forskningsafdelingen
Læge Niels Patrick Gosden, Retspsykiatrisk Klinik
Læge Ulrik Dixen, Hvidovre Hospital
Læge Morten Bay-Nielsen, Hvidovre Hospital
Klinisk koordinator Helene Bergman, Coloplast
Klinisk koordinator Claus Bøgebjerg, Coloplast
Klinisk koordinator Pernille W. Larsen, Coloplast

Læge Celeste Porsbjerg, Bispebjerg Hospital
Læge Finn Molke Borgbjerg, Bispebjerg Hospital
Professor Jens Chr. Djurhuus, Skejby Sygehus
Læge Ulrik Kesmodel, Skejby Sygehus
Professor Niels Jørgen Secher, Skejby Sygehus
Læge Karen Markussen Linnet, Skejby Sygehus