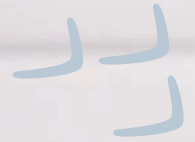




DATATILSYNET



# Datatilsynets årsberetning 2005





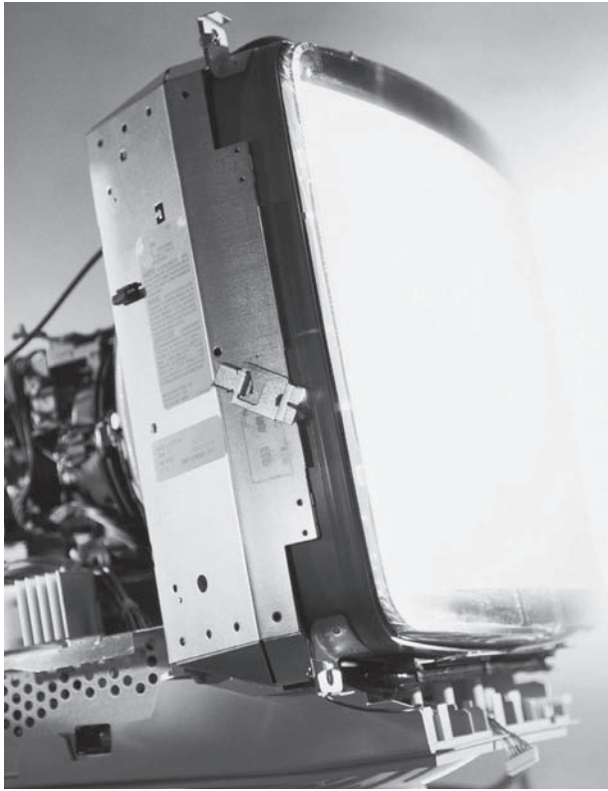
# Datatilsynets årsberetning 2005

Udgiver: Datatilsynet  
Tryk og layout: Schultz Grafisk  
Beretningen er sat med Meta  
Oplag: 400  
November 2006  
ISSN nr: 1601-5657  
ISBN nr: 87-989860-5-8



# Indhold

<i>Til Folketinget</i>	<b>5</b>
<b><i>Datatilsynets virksomhed i 2005</i></b>	<b>7</b>
Væsentlige aktiviteter	7
Datatilsynets organisation	19
Persondataloven	21
Datatilsynets hjemmeside	21
Statistiske oplysninger	22
<b><i>Udtalelser over lovforslag mv.</i></b>	<b>27</b>
Lov om registrering af køretøjer (Digital motorregistrering mv.)	27
Lov om et indkomstregister (eIndkomst)	31
Lov om ændring af lov om dagpenge ved sygdom eller fødsel	37
Lov om ændring af patentloven	40
Lov om ændring af lov om jordbrugets anvendelse af gødning og om plantedække	42
Lov om ændring af lov om omsætning af fast ejendom m.fl.	50
<b><i>Internationalt arbejde</i></b>	<b>55</b>
Indledning	55
Europarådet	56
Den Europæiske Union	56
International Konference for databeskyttelsesmyndigheder mv.	66
Nordisk Samarbejde	66
<b><i>Sikkerhedsspørgsmål</i></b>	<b>69</b>
Persondatalovens krav om datasikkerhed	69
Bibliotekssagen	69
Kommunes offentliggørelse af personoplysninger	72
Vilkår om sikkerhed ved privat anmeldelse	74
<b><i>Tilsynsvirksomhed</i></b>	<b>79</b>
Generelt om Datatilsynets inspektioner	79
Gennemførelse af inspektioner	80
Udvælgelse af dataansvarlige til inspektion i 2005	82
Datatilsynets observationer ved inspektioner i 2005	83
Oversigt over udførte inspektioner i 2005	85



# Til Folketinget

Hermed afgiver Datatilsynet sin årsberetning for 2005.

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

Beretningen indeholder en beskrivelse af Datatilsynets aktiviteter i 2005 og gengiver Datatilsynets udtalelser til nogle af de lovforslag mv., som tilsynet har fået i høring i 2005.

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

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

Siden 2004 har Datatilsynet løbende offentliggjort udtalelser og afgørelser i sager, som vurderes at være af generel interesse, på tilsynets hjemmeside [www.datatilsynet.dk](http://www.datatilsynet.dk). Årsberetningen indeholder derfor ikke referater af konkrete sager om behandling af personoplysninger.

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

København, november 2006

Asbjørn Jensen  
*Formand for Datarådet*

Janni Christoffersen  
*Direktør*



# Datatilsynets virksomhed i 2005

## Væsentlige aktiviteter

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

Blandt Datatilsynets forskellige aktiviteter i 2005 kan nævnes:

- Vejledning og rådgivning over for offentlige myndigheder, private personer og virksomheder
- Behandling af klager fra personer over f.eks. registrering, videregivelse eller manglende indsigt
- Udtalelser om lovforslag og bekendtgørelser mv.
- Strukturreformen
- Udtalelser om anmeldelser fra offentlige myndigheder
- Udtalelser om internationale retsakter
- Bidrag til besvarelser af Folketingsspørgsmål
- Tilladelser i forbindelse med anmeldelser fra private virksomheder og forskere
- Forskellige former for tilladelser til offentlige myndigheder og virksomheder mv.
- Sager på tilsynets eget initiativ, herunder inspektioner hos offentlige myndigheder samt hos en række private virksomheder og forskere
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsynsmyndigheder
- Schengen-evaluering
- Afholdelse af Nordisk Sagsbehandlermøde
- Deltagelse i arbejdsgrupper, udvalg o.l.

- Deltagelse i Personalestyrelsens konference om persondataloven i relation til personaleadministration

Datatilsynet har i 2005 registreret 4.585 nye sager, hvilket er en stigning på 3 % i forhold til 2004, hvor der blev registreret 4.441 nye sager. De forskellige kategorier af sager fremgår af oversigten i afsnittet "Statistiske oplysninger". De væsentligste stigninger i antallet af nye sager ses i kategorierne forespørgsler og klager vedrørende private dataansvarlige samt private anmeldelser.

### ***Rådgivning og vejledning***

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

Et vigtigt område for rådgivning og vejledning har igen i 2005 været digital forvaltning og forberedelserne til den kommende strukturreform, jf. nærmere nedenfor.

### ***Klagesagsbehandling***

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

Tilsynet har igen i 2005 registeret en relativt stor stigning i antallet af nye sager (klager og forespørgsler) vedrørende private dataansvarlige (fra 571 i 2004 til 692 i 2005). I forhold til offentlige myndigheder er der i 2005 registeret en lille stigning (fra 394 i 2004 til 408 i 2005) i antallet af nye sager.

Ud over de henvendelser, der bliver registreret som nye sager, modtager Datatilsynet et meget stort antal telefoniske henvendelser. De telefoniske henvendelser

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

Datatilsynet har siden midten af 2004 forsøgsvis gennemført kvartalsmæssige stikprøvetællinger af antallet af telefoniske henvendelser til tilsynet. Baseret på optællingerne anslås antallet af telefoniske henvendelser til tilsynet at ligge på ca. 17.000 i 2005, hvilket svarer til niveauet i 2004.

### *Høring over lovforslag mv.*

Datatilsynet skal efter persondataloven høres over udkast til bekendtgørelser, cirkulærer og lignende generelle retsfor skrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger. Tilsynet bliver også hørt over lovforslag, direktivforslag og betænkninger mv. på dette område.

Datatilsynets udtalelser over lovforslag mv. giver bl.a. Folketinget viden om, hvilke konsekvenser for databeskyttelsen et lovforslag har. Tilsynets høringssvar udgør således et bidrag til grundlaget for den politiske beslutningsproces. Efter Datatilsynets opfattelse er denne opgave vigtig, dels fordi tilsynet er i besiddelse af ekspertviden om databeskyttelse, dels fordi tilsynet efter persondatalovens § 56 udøver sine funktioner i fuld uafhængighed.

Datatilsynet har igennem de senere år oplevet et stadigt stigende antal sager i denne kategori. I 2005 faldt antallet af disse sager dog noget i forhold til 2004 (fra 226 i 2004 til 195 i 2005), men der er stadig tale om en betydelig stigning fra 2003, hvor der blev registreret 109 sager.

En del af de lovforslag, som Datatilsynet modtog i høring i 2005, indeholdt forslag til regler, hvorefter der skal ske en offentliggørelse – typisk på internettet – af personoplysninger. Datatilsynets udtalelser til nogle af disse lovforslag er gengivet i afsnittet om udtalelser om lovforslag mv. Generelt kan det endvidere konstateres, at der er en tendens til, at lovforslagene lægger op til offentliggørelse af personhenførbare oplysninger i videre omfang, end det umiddelbart er muligt inden for rammerne af persondataloven. En anden tendens synes at være, at der i stigende omfang lægges op til, at offentlige myndigheder skal kunne foretage sammenstilling og samkøring af personoplysninger i kontroløjemed.

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

I en del tilfælde foreslås som nævnt regler, som indebærer en behandling af personoplysninger, der ikke umiddelbart kan ske inden for rammerne af persondataloven. Gennemførelsen kræver således, at der i særlovgivningen sker en fravigelse af persondataloven. I sådanne tilfælde gør tilsynet i sine høringssvar opmærksom på problemerne i forhold til persondataloven og anbefaler, at det tydeliggøres i lovforslaget, hvorvidt der er tale om en fravigelse af persondataloven, herunder om en sådan fravigelse kan ske inden for rammerne af databeskyttelsesdirektivet. Datatilsynet giver i den forbindelse normalt udtryk for, at en særskilt hjemmel til behandling af personoplysninger i videre omfang, end hvad der følger af persondataloven, kun bør tilvejebringes, hvis vægtige samfundsmæssige hensyn taler derfor. Om der konkret er så vægtige offentlige hensyn, der gør det nødvendigt at fravige det generelle beskyttelsesniveau, som lovgivningsmagten har fastlagt med persondataloven, beror i sidste instans på en politisk vurdering, som må udøves af Folketinget selv. På den baggrund undlader tilsynet i sådanne tilfælde ofte at udtale sig om, en sådan fravigelse bør gennemføres.

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

### *Strukturreformen*

Datatilsynet har igen i 2005 beskæftiget sig en del med strukturreformen.

Tilsynet har haft en række love og bekendtgørelser vedrørende strukturreformen i høring og har bl.a. udtalt sig om brugerstyring i borgerservicecentre på skatteområdet<sup>1</sup> og om den nye restanceinddrivelsesmyndigheds adgang til kommunernes systemer. Tilsynet har endvidere udtalt sig om ændringer af færdselsloven og pasloven.<sup>2</sup>

Ud over afgivelse af høringssvar har Datatilsynet i forbindelse med udarbejdelsen og udmøntningen af lovforslagene og en række andre projekter, der direkte eller indirekte har haft tilknytning til strukturreformen, ydet rådgivning og vejledning til de involverede myndigheder. Datatilsynet har bl.a. bidraget til

---

<sup>1</sup> Udtalelsen kan ses på Datatilsynets hjemmeside.

<sup>2</sup> I tilknytning hertil har Datatilsynet i 2006 udtalt sig om udkast til ny kørekortbekendtgørelse og pasbekendtgørelse, der medfører, at en række opgaver på pas- og kørekortområdet fremover skal varetages af kommunerne.

Videnskabsministeriets vejledning om overdragelse af IT-systemer i forbindelse med kommunalreformen.<sup>3</sup>

Datatilsynet og Kommunernes Landsforening har endvidere drøftet spørgsmålet om dataansvar i forbindelse med sammenlægningen af kommunerne. Når to eller flere kommuner skal lægges sammen, er der således ofte behov for – forud for 1. januar 2007 – at forberede en teknisk sikker overgang fra to eller flere adskilte porteføljer af systemløsninger til en fælles portefølje.

Kommunernes Landsforening har på baggrund af bl.a. drøftelserne med Datatilsynet udarbejdet et ”standardbrev”, som kommunerne kan anvende for at meddele Datatilsynet, at de har fælles dataansvar i en overgangsperiode. Ved udgangen af 2005 havde foreløbigt 11 kommuner benyttet denne fremgangsmåde. Datatilsynet har endvidere besvaret en del telefoniske henvendelser om håndteringen af sammenlægningssituationen.

Datatilsynet har herudover taget stilling til spørgsmålet om overdragelse af personalesager i forbindelse med strukturreformen.<sup>4</sup>

### *Sager på eget initiativ*

Datatilsynet har i 2005 registreret 112 sager rejst på tilsynets eget initiativ. Dette svarer til niveauet i både 2003 og 2004. Sagerne omfatter såvel inspektioner som andre ”egen drift-sager”.

I 2005 har Datatilsynet gennemført 61 inspektioner, heraf 23 hos offentlige myndigheder og 38 hos forskellige private virksomheder. I 2002 blev der gennemført i alt 116 inspektioner, mens antallet af inspektioner i perioden 2003 til 2005 har ligget noget lavere (71 i 2003 og 68 i 2004). Nedgangen i antallet af inspektioner er en følge af dels de pålagte besparelser, dels en meget væsentlig forøgelse af sagsantallet på tilsynets andre arbejdsområder. I øvrigt har antallet af inspektioner hos offentlige myndigheder været forholdsmæssigt lavere i 2005 end i de forudgående år, hvilket bl.a. skyldes, at Datatilsynet på grund af den forestående strukturreform i et vist omfang har prioriteret at bruge ressourcerne på inspektioner hos private dataansvarlige. Tilsvarende forventes at gøre sig gældende for inspektionerne i 2006.

Det er ofte på baggrund af henvendelser fra pressen, at Datatilsynet tager sager op til nærmere undersøgelse. Fra 2005 kan nævnes, at Datatilsynet på baggrund af presseomtale af, at nogle virksomheder overvåger deres kunders eventuelle navne- og adresseændringer ved hjælp af CPR-oplysninger, indledte en sag

---

<sup>3</sup> Datatilsynets bidrag kan ses på tilsynets hjemmeside, hvor der også er et link til Videnskabsministeriets vejledning.

<sup>4</sup> Udtalelsen kan ses på Datatilsynets hjemmeside.

vedrørende Indenrigs- og Sundhedsministeriets CPR-kontors videregivelse af oplysninger fra Det Centrale Personregister (CPR) til private virksomheder.

Datatilsynets sagsbehandling angik primært den situation, hvor CPR-kontoret videregiver oplysninger til en privat virksomheds databehandler, og hvor det er databehandleren, der af CPR-kontoret er registreret som abonnent på oplysningerne. Denne fremgangsmåde medførte bl.a., at den person, der videregives oplysninger om, ikke havde mulighed for at se, hvilken virksomhed der var den reelle modtager af oplysningerne. At en registreret ikke ved, hvem der er dataansvarlig, betyder bl.a., at den registrerede ikke umiddelbart kan gøre sine rettigheder efter persondataloven gældende.

Sagen blev behandlet i Datarådet, og Datatilsynet fandt bl.a., at det vil være bedst stemmende med persondatalovens princip om god databehandlingsskik, at de registrerede fremover sikres mulighed for at få kendskab til, hvilke dataansvarlige virksomheder mv. der abonnerer på CPR-oplysninger om dem. Datatilsynet henstillede, at Indenrigs- og Sundhedsministeriet, CPR-kontoret, tog initiativ til at sikre de registrerede denne mulighed.

Datatilsynet behandlede ved samme lejlighed en klage over en række private virksomheders behandling af tidligere kunders CPR-oplysninger i relation til bl.a. markedsføringsreglerne.<sup>5</sup>

Efterfølgende modtog Datatilsynet en række henvendelser fra registrerede personer, der ønskede at få at vide, hvilke dataansvarlige virksomheder der modtager CPR-oplysninger om dem via databehandlere. Datatilsynet hjalp de pågældende med at få de ønskede oplysninger, hvorefter de kan tage kontakt til den dataansvarlige modtager, hvis der skulle være behov herfor. Pr. 1. juli 2005 ændrede CPR-kontoret sine "Standardvilkår for dataleverancer fra CPR til private", således at det fremgår heraf, at registrerede har krav på af databehandleren at få oplyst, hvilke virksomheder mv. der via databehandleren abonnerer på oplysninger fra CPR om dem.

I forbindelse med behandlingen af sagerne om videregivelse af oplysninger til private fra CPR blev Datatilsynet i øvrigt opmærksom på kreditoplysningsbureauet Experian A/S' produkter "Aktiv Kreditsikring" og "Kreditvagten". Datatilsynet valgte på den baggrund og i forlængelse af tilsynets tidligere undersøgelser af produkterne i henholdsvis 1996 og 1999 at indlede en nærmere undersøgelse af disse produkters forenelighed med persondataloven.

Aktiv Kreditsikring fungerer på den måde, at Experian A/S driver et edb-servicebureau, hvor Experian A/S' abonnenters kunderegistre bliver lagt ind, således at

---

<sup>5</sup> Begge udtalelser kan ses på Datatilsynets hjemmeside.

abonnenten automatisk løbende modtager besked, hvis deres kunde bliver registreret hos Experian A/S med en betalingsanmærkning som ”dårlig betaler”.

Efter behandling i Datarådet fandt Datatilsynet, at det ikke kunne anses som stridende mod persondataloven, at den enkelte abonnent på Kreditvagten og Aktiv Kreditsikring undersøger, om deres kunder er blevet registreret hos Experian A/S, forudsat at der er tale om egentlige kunder hos abonnenten, dvs. hvor der er etableret et kreditforhold mellem den enkelte kunde og abonnenten. Indsamlingen må endvidere ske, når der er udstedt et betalingskort til kunden.

Datatilsynet forudsatte ved vurderingen, at abonnenternes kunder forinden modtager klar og udtrykkelig information herom.<sup>6</sup>

### ***Bibliotekssagen***

Datatilsynet modtog i 2005 en henvendelse fra Biblioteksstyrelsen vedrørende bibliotekers fremsendelse af ikke-krypterede kvitteringsmails til borgere, der har foretaget elektronisk bestilling af bøger på bibliotek.dk. Kvitteringsmails indeholder bl.a. titel og forfatter på det reserverede materiale.

Datatilsynet tilkendegav i den forbindelse, at oplysninger om, hvilke bøger en borger ønsker at låne, må betragtes som fortrolige oplysninger, og at det følger af sikkerhedsbekendtgørelsen, at transmission af fortrolige oplysninger over det åbne internet forudsætter kryptering.

Biblioteksstyrelsens offentliggørelse af Datatilsynets svar sammen med en nyhedstekst om, at efter krav fra Datatilsynet ville kvitteringsmails blive fjernet i bibliotek.dk., medførte en del reaktioner fra bl.a. brugere af systemet og pressen, og sagen blev efterfølgende drøftet på et møde i Datarådet. Herefter fandt Datatilsynet undtagelsesvist at kunne acceptere, at Biblioteksstyrelsen og bibliotekerne foreløbig i en periode på 5 år fortsætter med at sende elektroniske reserverings- og kvitteringsmeddelelser, der indeholder titel og forfatter på det reserverede materiale, i ikke-krypteret form til de brugere, der ønsker at benytte elektronisk kommunikation med biblioteksvæsenet. Sagen er omtalt nærmere under afsnittet ”Sikkerhedsspørgsmål”.

### ***Offentlige myndigheders offentliggørelse af personoplysninger***

Det er Datatilsynets opfattelse, at der er en stigende tendens til, at offentlige myndigheder offentliggør personhenførbare oplysninger på internettet. Datatilsynet modtager også en del henvendelser om, hvilke oplysninger der kan offentliggøres.

---

<sup>6</sup> Udtalelsen kan ses på Datatilsynets hjemmeside.

Ringkøbing Amt og Århus Amt rettede henvendelse til Datatilsynet, idet amterne ønskede at give fri adgang via internettet til sagsakter, der behandles i visse dele af de to amters journalsystemer. Herudover sker der offentliggørelse af postlister, dvs. oversigter over den ind- og eventuelt udgående post.

Efter at sagen havde været behandlet i Datarådet, udtalte Datatilsynet, at det er tilsynets opfattelse, at der ikke kan offentliggøres *følsomme* oplysninger på internettet, idet ingen af betingelserne for behandling i de relevante bestemmelser i persondataloven kan anses for opfyldt.

Datatilsynet fandt, at almindelige, *ikke-fortrolige* oplysninger kan offentliggøres på internettet inden for rammerne af persondataloven, og at der kan videregives *fortrolige* oplysninger, hvis oplysningerne er ”anonymiserede”, således at det ikke er muligt for udenforstående (dvs. for andre end amtet og den registrerede selv) at identificere den person, som oplysningerne vedrører.<sup>7</sup>

Datatilsynet tilkendegav samtidig, at det er tilsynets opfattelse, at de dataansvarlige amter, før en så vidtgående offentliggørelse sættes i værk, må foretage en nøje afvejning af på den ene side hensynet til de interesser, der forfølges med offentliggørelsen, og på den anden side hensynet til de personer, der – hvis offentliggørelsen gennemføres – ikke vil kunne skrive til amterne, uden at dette bliver gjort tilgængeligt for – i princippet – hele verden via internettet.

I forlængelse heraf fandt tilsynet, at det må anses for hensigtsmæssigt, at beslutningen om, hvorvidt der skal ske offentliggørelse i et omfang som beskrevet, træffes af den politiske ledelse. Hvis resultatet af afvejningen af disse modsatrettede hensyn bliver, at der skal ske offentliggørelse, fandt Datatilsynet ikke med henvisning til persondataloven at kunne udtale sig imod noget sådant.

Datatilsynet understregede endvidere i sin udtalelse vigtigheden af, at amterne inden offentliggørelsen nøje gennemgår det enkelte brev med henblik på at sikre, at brevet ikke indeholder fortrolige og/eller følsomme oplysninger, og vigtigheden af, at medarbejderne modtager grundig instruktion i, hvorledes offentliggørelsen af akter og postlister skal håndteres. Ubertigtet offentliggørelse af personoplysninger kan have betydelige negative konsekvenser for de personer, der berøres heraf. Det vil endvidere ofte være forbundet med store vanskeligheder at få oplysningerne fjernet fra eksempelvis søgemaskiner.<sup>8</sup>

Vigtigheden af, at en offentlig myndighed, der ønsker at offentliggøre personoplysninger på internettet, sørger for grundig instruktion af de relevante medarbejdere, understreges af, at Datatilsynet med jævne mellemrum modtager henvendelser om sager, hvor kommuner som følge af menneskelige fejl har offentliggjort

---

<sup>7</sup> Udtalelsen kan ses på Datatilsynets hjemmeside.

<sup>8</sup> Datatilsynet tog også stilling til spørgsmålet om oplysningspligt ved den påtænkte offentliggørelse af oplysninger.

fortrolige og/eller følsomme oplysninger om borgere på internettet. Et eksempel på en sådan sag er omtalt nærmere i afsnittet om "Sikkerhedsspørgsmål".

### *Opfølgning på forskningsprojekter*

Et videnskabeligt forsknings- eller statistikprojekt, der indebærer behandling af følsomme personoplysninger, kræver en forudgående tilladelse fra Datatilsynet. Antallet af ansøgninger er steget betydeligt gennem de seneste år,<sup>9</sup> og tilsynet bruger generelt mange ressourcer på at behandle disse sager.

En tilladelse fra Datatilsynet til at gennemføre et videnskabeligt projekt med følsomme personoplysninger er tidsbegrænset. Af tilladelsen fremgår, at forskeren skal underrette Datatilsynet, når projektet er afsluttet, og oplysningerne er slettet eller anonymiseret.

Datatilsynet blev imidlertid opmærksom på, at forskere muligvis havde glemt at give tilsynet besked, når projektet er afsluttet. Ligeledes syntes mange at glemme at søge om forlængelse, hvis projektet ikke kunne afsluttes inden tilladelsens udløb.

Datatilsynet så sig derfor nødsaget til at gøre en særlig indsats for at erindre forskerne om persondatalovens regler og vilkårene for Datatilsynets tilladelse. Et andet vigtigt formål med projektet er at sikre, at fortegnelsen på tilsynets hjemmeside giver et retvisende billede af projekter med gyldige tilladelser. I 2005 udsendte tilsynet ca. 1.700 rykkerbreve, og i alt vil der blive udsendt rykkere til ca. 2.300 forskere.

Arbejdet med at sende de mange rykkerbreve og den tilknyttede sagsbehandling er en stor og særdeles tidskrævende opgave, som Datatilsynet ikke i fremtiden vil kunne afsætte ressourcer til. Tilsynet besluttede derfor samtidig at ændre proceduren for tilladelser, der er givet efter 1. januar 2005. Fra denne dato fremgår det af tilladelsen, at Datatilsynet betragter projektet som afsluttet og personoplysningerne som slettet, anonymiseret, tilintetgjort eller overført til arkiv ved tilladelsens udløb, medmindre forskeren har anmodet om en forlængelse. Når tilladelsen er udløbet, fjerner Datatilsynet ligeledes anmeldelsen fra fortegnelsen på tilsynets hjemmeside.

Datatilsynet arbejder med planer om etablering af en elektronisk servicemeddelelse, hvorefter der automatisk udsendes en erindring til en forsker, når tiden for en tilladelsens udløb nærmer sig. Etableringen af et sådant system afhænger dog af, om opgaven kan løses teknisk – og ressourcemæssigt – tilfredsstillende.

---

<sup>9</sup> Udvikling i antallet af ansøgninger: 2002 = 694, 2003 = 943, 2004 = 1103, 2005 = 1260.

### ***Konference om persondataloven i relation til personaleadministration***

Datatilsynet deltog i oktober 2005 i planlægningen og gennemførelsen af Personalestyrelsens konference om persondata, hvis formål var at sætte persondatalovens rammer for behandling af personoplysninger i relation til den daglige personaleadministration, der finder sted hos offentlige myndigheder.

I tilknytning til konferencen har Personalestyrelsen med bistand fra Datatilsynet udarbejdet en vejledning om persondatalovens vigtigste regler af betydning for en offentlig personaleadministration.<sup>10</sup>

### ***Internationalt samarbejde***

Datatilsynets deltagelse i internationalt samarbejde er fortsat et område, der vokser i omfang. Datatilsynet deltager bl.a. i samarbejdet i de fælles tilsynsmyndigheder nedsat i henhold til Schengen- og Europol-konventionerne, i Europarådets arbejde og i andre internationale arbejdsgrupper både på EU-niveau og verdensplan. Aktiviteterne i de fælles tilsynsmyndigheder omtales nærmere i afsnittet om internationale sager.

Datatilsynet deltager endvidere i det nordiske samarbejde vedrørende databeskyttelse, og Danmark var i 2005 vært for det Nordiske Sagsbehandlermøde. Hovedformålet med mødet er at udveksle erfaringer og synspunkter i forhold til de nordiske tilsyns indsats og praksis på databeskyttelsesområdet og at styrke samarbejdet mellem myndighederne. Drøftelserne på det Nordiske Sagsbehandlermøde tjener endvidere til at identificere, hvilke aktuelle emner der er af sådan fællesnordisk interesse, at de bør drøftes nærmere på det Nordiske Datachefmøde.

### ***Schengen-evaluering af de nordiske lande***

For at sikre, at de nordiske lande lever op til de krav, der stilles til Schengen-medlemsstaterne, samt at kontrollen ved de ydre grænser er effektiv, gennemførte Schengen-landene i 2005 en evaluering af de nordiske lande. Evalueringen blev indledt i begyndelsen af 2005, ved at de nordiske lande besvarede et omfattende spørgeskema angående implementering af Schengen-konventionen.

På databeskyttelsesområdet blev det undtagelsesvist besluttet, at evalueringen af de nordiske lande skulle samles i henholdsvis Reykjavik og København, således at Norge og Island blev evalueret i Reykjavik, og Sverige, Finland og Danmark blev evalueret i København.

---

<sup>10</sup> Vejledningen kan ses på Personalestyrelsens hjemmeside.

Ved evalueringen den 22. september 2005 i København var det Datatilsynet, der efter aftale med Justitsministeriet tog sig af den praktiske tilrettelæggelse af ekspertkomiteens besøg i København samt stod for Danmarks evaluering inden for databeskyttelsesområdet.

Det fremgår bl.a. af Rådets konklusioner på evalueringen, at Danmark alt i alt anvender Schengen-reglerne på en meget tilfredsstillende måde.

### ***Schengen-undersøgelse af nationale indberetninger i Schengen-informationssystemet***

Den Fælles Tilsynsmyndighed Schengen har i samarbejde med databeskyttelsesmyndighederne i de EU-lande, som deltager i Schengen-informationssystemet (SIS), samt Norge og Island, foretaget en fælles undersøgelse af landenes brug af SIS-systemet vedrørende indberetning af uønskede udlændinge, jf. Schengenkonventionens artikel 96.

Undersøgelsens resultat blev præsenteret i en samlet rapport af 20. juni 2005, som kan findes på Datatilsynets hjemmeside eller Den Fælles Tilsynsmyndighed Schengens hjemmeside [www.schengen-isa.dataprotection.org/](http://www.schengen-isa.dataprotection.org/).

Resultatet af undersøgelsen af de danske indberetninger gav anledning til kritik fra Datatilsynet. Der var sket fejlagtig indberetning i 25 tilfælde ud af 443. Herudover var der sket forskellige fejl i yderligere et antal tilfælde.

Indberetningerne til SIS kan få alvorlige konsekvenser for en registreret person, idet han eller hun efter konventionens artikel 5 som hovedregel ikke vil kunne få tilladelse til at indrejse i og opholde sig i Schengen-området.

Det var på den baggrund Datatilsynets opfattelse, at der var tale om et uacceptabelt højt antal fejl, og tilsynet fandt dette kritisabelt. Datatilsynet noterede sig, at Rigspolitiet havde taget skridt til at rette de konstaterede fejl, og at Rigspolitiet endvidere havde taget initiativer med henblik på at sikre, at de oplysninger, der optages i SIS, er korrekte og aktuelle. Datatilsynet orienterede Justitsministeriet om resultatet af undersøgelsen.

Datatilsynet udtalelse til Rigspolitiet kan ses på tilsynets hjemmeside.

### ***Rigsrevisionens gennemgang af tilsynets årsrapport for 2004***

Datatilsynet afgav i april 2005 sin årsrapport for 2004 indeholdende beretning om tilsynets resultater, målrapportering over tilsynets indsatspunkter for 2004 (sagsbehandlingstid, visioner og målsætninger for Datatilsynet, eDag2, stillings-

besættende virksomheder og Datatilsynets informationsindsats) og regnskab. Rapporten er offentliggjort på tilsynets hjemmeside.

Rigsrevisionen meddelte i april 2005, at Datatilsynet var blevet udvalgt til et besøg med henblik på en udvidet gennemgang af årsrapporten for 2004. Formålet med besøget og gennemgangen var at vurdere kvaliteten af årsrapportens indhold og at påse, om oplysningerne i rapporten er pålidelige og dokumenterede. Ved Rigsrevisionens gennemgang af årsrapporten er de opstillede mål og rapporteringen om mål og resultater blevet vurderet, og ved besøget er sammenhængen mellem rapporten og mål- og resultatstyringen samt tilrettelæggelsen af registreringer blevet vurderet, ligesom dokumentationen for udvalgte oplysninger (udviklingen i sagsantallet, antallet af inspektioner, sagsbehandlingstider for kreditoplysningsklager og personaletil- og afgang i 2004) i årsrapporten er blevet gennemgået.

Rigsrevisionen konkluderede som sin samlede vurdering, at Datatilsynets årsrapport for 2004 er tilfredsstillende.

Rigsrevisionen fandt rapporteringen om mål og resultater ikke helt tilfredsstillende, idet der efter Rigsrevisionens opfattelse er givet en tilfredsstillende redegørelse for status af de enkelte mål, ligesom Datatilsynets analyser er fundet realistiske og vurderende, mens Rigsrevisionen savnede en redegørelse for sammenhængen mellem de faglige og økonomiske resultater. En sådan redegørelse forudsætter, at der til angivelsen af målopfyldelsen kobles oplysninger om økonomi og ressourceforbrug, ligesom Rigsrevisionen lagde vægt på, om målopfyldelsen og ressourceforbruget kan sammenholdes for de enkelte mål eller grupper af mål.

Herudover fandt Rigsrevisionen, at samtlige andre forhold, der er blevet vurderet i forbindelse med den udvidede gennemgang af årsrapporten, var tilfredsstillende. Dette gælder Datatilsynets målopstilling, styringen af udarbejdelsen af årsrapporten, tilrettelæggelsen af målinger og registreringer, den anvendte regnskabspraksis samt dokumentationen vedrørende de udvalgte oplysninger i årsrapporten.

### ***Andre opgaver***

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

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

## **Datatilsynets organisation**

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

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

### ***Datarådet***

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

#### ***Datarådets medlemmer***

Pr. 31. december 2005

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

Medlemmerne beskikkes for 4 år ad gangen, og de er personligt udpeget i kraft af deres sagkundskab inden for bestemte sagsområder og er ikke repræsentan-ter 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.

### ***Ansatte i sekretariatet***

Pr. 31. december 2005

Direktør, cand.jur. Janni Christoffersen  
Kontorchef, cand.jur. Lena Andersen  
IT-chef, civilingeniør Ib Alfred Larsen  
Chefkonsulent, cand.jur. Tine Asmussen  
IT-sikkerhedskonsulent Nils Rasmussen  
IT-sikkerhedskonsulent Peter Smidt  
Specialkonsulent, mag.art. Camilla Daasnes  
Fuldmægtig, cand.jur. Anders Ankerstjerne  
Fuldmægtig, cand.jur. Christine Jensen Boeskov  
Fuldmægtig, cand.jur. Stine Dyhr  
Fuldmægtig, cand.jur. Emil Paldam Folker  
Fuldmægtig, cand.jur. Tina Fugl  
Fuldmægtig, cand.jur. Thomas Gønge  
Fuldmægtig, cand.jur. Maria Joost  
Fuldmægtig, cand.jur. Mia Staal Klintrup  
Fuldmægtig, cand.jur. Camilla Sonne Kristensen  
Fuldmægtig, cand.jur. Inge Birgitte Møberg  
Fuldmægtig, cand.jur. Henriette Vincens Nielsen  
Fuldmægtig, cand.jur. Jakob Gøtze Pedersen  
Fuldmægtig, cand.jur. Anne Broberg Rasmussen  
Fuldmægtig, cand.jur. Frederik Siegumfeldt  
Kontorfuldmægtig Kirsten Markussen  
Kontorfuldmægtig Anne-Marie Müller  
Kontorfuldmægtig Suzanne Stenkvist  
Overassistent Pernille Jensen  
Overassistent Mette Maj Leilund  
Overassistent Berit Pedersen  
Stud.jur. Ane Kallmayer Bach  
Stud.jur. Tina Wesselhoff Davidsen  
Stud.jur. Marie Gjesing Fynsk (orlov)  
Stud.jur. Maiken Toftgaard Knudsen

### *Datatilsynets ressourcer*

Antallet og omfanget af Datatilsynets opgaver er stigende, og tilsynet blev – i forbindelse med en Folketingsdebat om Datatilsynets ressourcer i november 2004 – på tillægsbevillingsloven for 2004 tilført en ekstra bevilling på 1,5 mio. kr. Det skete med henblik på, at tilsynet kan løfte den merbelastning, der bl.a. er en følge af strukturreformen og indførelsen af nye it-systemer.

Da de yderligere lønmidler først var til rådighed for Datatilsynet i slutningen af 2004, blev de videreført til 2005 til brug for en tiltrængt opnormering af tilsynets personale (tilsynets nettoudgiftsbevilling for 2005 var på 14,0 mio. kr.). Tilsynet har i 2005 opnormeret med to sagsbehandlere.

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

I tilknytning til persondataloven har Justitsministeriet udstedt en række bekendtgørelser.

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

**Datatilsynets hjemmeside** Loven, bekendtgørelserne og vejledningerne kan læses på Datatilsynets hjemmeside [www.datatilsynet.dk](http://www.datatilsynet.dk).

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

Datatilsynet har også i 2005 løbende udarbejdet nye tekster og informationsmateriale, som er offentliggjort på hjemmesiden, og fortsat arbejdet med i videre omfang end tidligere at offentliggøre tilsynets udtalelser og afgørelser i sager, der vurderes at være af generel interesse.

Enhver kan – gratis – tegne elektronisk abonnement på Datatilsynets hjemmeside. Abonnenterne modtager automatisk en e-post, når hjemmesiden opdateres. Ved udgangen af december 2005 var der i alt 3.767 abonnenter på Datatilsynets hjemmeside mod ca. 3.620 abonnenter i 2004, 3.170 i 2003 og 2.700 i 2002.

## Statistiske oplysninger

Oplysningerne i dette afsnit er baseret på registreringerne af nye sager i Datatilsynets journalsystem i 2005 og vedrører sager, som er oprettet i løbet af 2005. En del af Datatilsynets sagsbehandling er imidlertid fortsættelse af eksisterende sager. Dette er for eksempel tilfældet, når en anmeldelse ændres, eller en tilladelse forlænges. Disse sager er af praktiske årsager ikke omfattet af statistikken. Dog kan det konstateres, at Datatilsynet i 2005 har modtaget ca. 800 ændringer til eksisterende anmeldelser af private forsknings- og statistikprojekter.

Datatilsynet registrerede 4.585 nye sager i perioden fra den 1. januar 2005 til den 31. december 2005. Disse sager fordeler sig således:

Datatilsynets egen administration mv.	236
Lovforberedende arbejde	195
Forespørgsler og klager vedrørende private	692
Forespørgsler og klager vedrørende offentlige myndigheder	408
Anmeldelse for den private sektor	1.583
Anmeldelser for den offentlige sektor	1.157
Sager på Datatilsynets eget initiativ (egen drift-sager)	112
Sikkerhedsspørgsmål	27
Internationale sager	154
Datatilsynets kompetence efter anden lovgivning	21

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

### ***Forespørgsler og klager vedrørende private***

Datatilsynet registrerede i alt 692 nye sager om forespørgsler og klager vedrørende private dataansvarlige.

Sagerne havde følgende fordeling over forskellige virksomhedstyper:

Almindelige virksomheder	91
Den finansielle sektor	55
Fagforeninger, a-kasser, pensionskasser mv.	22
Telesektoren	78
Foreninger og organisationer	96
Sundhedssektoren (medicinalfirmaer, klinikker, læger mv.)	22
Kreditoplysningsbureauer	163
Advarselsregistre	9
Stillingsbesættende virksomheder	3
Ansøgninger om tilladelser	44
Diverse	103
Sager af generel karakter	2
Edb-servicebureauer	4

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2005,<sup>11</sup> var:

Klager	ca. 21%
Forespørgsler	ca. 79%

Af klagerne var ca. 45% berettigede, mens ca. 55% var uberettigede.

### ***Forespørgsler og klager vedrørende offentlige myndigheder***

Datatilsynet registrerede i alt 408 nye sager med klager og forespørgsler vedrørende offentlige myndigheder.

Sagerne var fordelt således:

Statslige myndigheder	157
Amtskommuner	25
Primærkommuner	114
Ansøgning om tilladelser	100
Diverse	12

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2005,<sup>12</sup> var:

Klager	ca. 11%
Forespørgsler	ca. 89%

Af klagerne var ca. 38% berettigede, mens ca. 62% var uberettigede.

### ***Anmeldelser for den private sektor***

Datatilsynet registrerede i alt 1.583 nye sager om anmeldelser for den private sektor. Fordelingen af sagerne var:

Forskning og statistik	1.289
Privates behandling af oplysninger om rent private forhold	181
Advarselsregistre	6
Spærrelister	4
Stillingsbesættende virksomheder	79
Edb-servicebureauer	23
Diverse sager af generel karakter	1

---

<sup>11</sup> Bemærk, at sagsgrundlaget for beregning af forholdet mellem klager og forespørgsler henholdsvis mellem berettigede og uberettigede klager er ændret siden Datatilsynets Årsberetning 2004. Tallene for 2005 er i modsætning til 2004 ikke opgjort på grundlag af sager, som er oprettet i 2005, men på grundlag af sager, som Datatilsynet har færdigbehandlet i 2005. Heriblandt er sager oprettet i 2005 og 2004 samt enkelte fra 2003. Denne metode er også benyttet, for så vidt angår tallene omkring klager og forespørgsler vedrørende offentlige myndigheder. Den ændrede opgørelsesmetode skyldes et ønske om at opgøre tallene på en måde, så de ikke ændrer sig afhængig af, hvornår man opgør dem.

<sup>12</sup> Se note 1.

### **Anmeldelser for den offentlige forvaltning**

Datatilsynet registrerede i alt 1.157 nye sager om anmeldelser for den offentlige sektor. Fordelingen af sagerne var:

Fællesanmeldelser	20
Kommuner	443
Amtskommuner	178
Statslige myndigheder	258
Tilslutninger, kommuner	78
Tilslutninger, amtskommuner	1
Tilslutninger, statslige myndigheder	178
Diverse/sager af generel karakter	1

### **Sager på Datatilsynets eget initiativ**

Datatilsynet registrerede i alt 112 nye sager oprettet på tilsynets eget initiativ. Fordelingen af sagerne var:

Inspektion og kontrol vedrørende private	49
Inspektion og kontrol vedrørende offentlige myndigheder	27
Sager rejst på grundlag af presseomtale og lign.	35
Diverse/sager af generel karakter	1

### **Sikkerhedsspørgsmål**

Datatilsynet registrerede i alt 27 nye sager under kategorien sikkerhedsspørgsmål. Fordelingen af sagerne var:

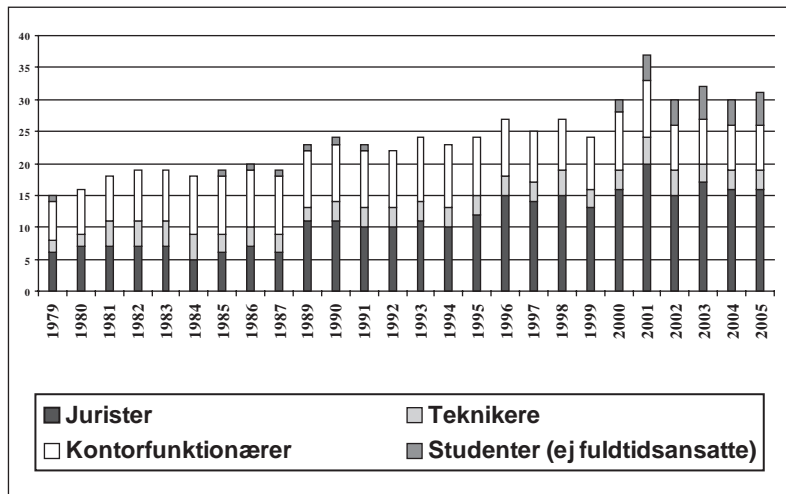
Private	14
Offentlige	12
Diverse	1

### **Internationale sager**

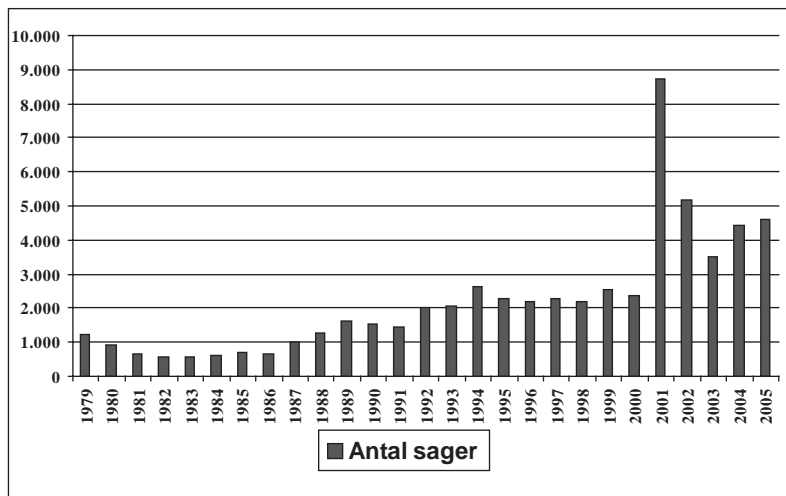
Datatilsynet registrerede i alt 154 nye internationale sager. Fordelingen af sagerne var:

Forespørgsler fra udlandet	50
Nordisk tilsynssamarbejde	1
Europarådet	4
EU	50
Konventioner	27
Datakommissærsamarbejdet	16
OECD	2
Diverse/sager af generel karakter	4

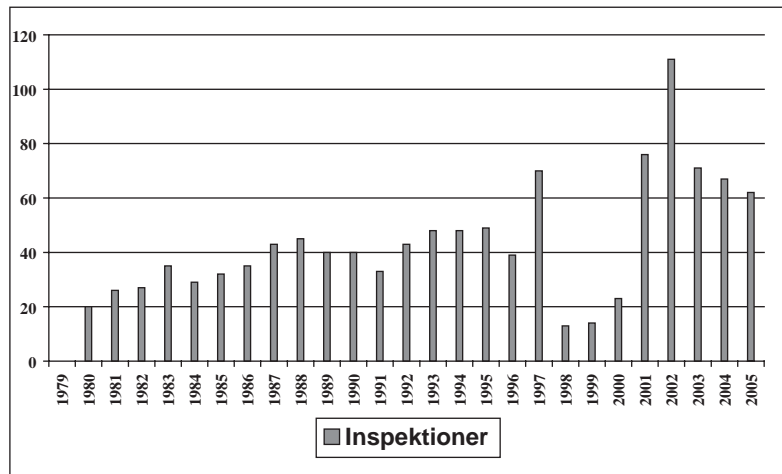
## Fordelingen af de forskellige personalegrupper hen over årene



## Antal sager



## Antal inspektioner



# Udtalelser over lovforslag mv.

## **Lov om registrering af køretøjer (Digital motorregistrering mv.)**

Skatteministeriet anmodede om Datatilsynets bemærkninger til udkast til forslag til lov om registrering af køretøjer (Digital motorregistrering mv.).

Lovforslaget lagde op til en digitalisering og delvis privatisering af registreringen af køretøjer. Endvidere vil private kunne omregistrere køretøjer over internettet. Centralregistret for Motorkøretøjer, som politiet driver, bliver erstattet af Køretøjsregistret, som skal drives af SKAT.

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

1. Der vil i Køretøjsregistret blive behandlet personoplysninger ved hjælp af elektronisk databehandling, og persondataloven finder derfor anvendelse.

Det fremgik bl.a. af bemærkningerne, at forhandlere af køretøjer og virksomheder, der er godkendt af Færdselsstyrelsen til at syne eller omsyne køretøjer, skal kunne autoriseres til at varetage opgaver vedrørende registrering af køretøjer. Videre fremgik det, at opgavefordelingen mellem skatteforvaltningen og autoriserede virksomheder vil blive baseret på, at autoriserede virksomheder ikke skal kunne udøve forvaltningsmyndighed.

På baggrund af bemærkningerne lagde Datatilsynet til grund, at skatteforvaltningen er dataansvarlig for administrationen af Køretøjsregistret, og at de autoriserede virksomheder er databehandlere i forbindelse med varetagelsen af opgaverne med registreringen af køretøjer. I andre henseender må virksomhederne imidlertid anses for selvstændigt dataansvarlige, jf. hertil pkt. 3.

Datatilsynet henlede i den forbindelse opmærksomheden på persondatalovens §§ 41 og 42.

Endvidere vil det være over for den dataansvarlige, at de registrerede skal gøre deres rettigheder efter loven gældende.

2. Det fremgik af lovudkastets § 17, at skatteministeren kan fastsætte regler om adgang til oplysninger, der er registreret i Køretøjsregistret.

Det var i bemærkningerne til lovudkastet anført, at:

”[a]lmindelige regler for behandling af personoplysninger er fastsat i persondataloven, offentlighedsloven og forvaltningsloven.

Efter lovforslaget bemyndiges skatteministeren til at fastsætte regler om yderligere adgang til oplysninger, der er registreret i Køretøjsregistret.”

Det fremgik, at forslaget bl.a. skal ses i sammenhæng med et principielt ønske om at give offentligheden adgang til oplysninger i det offentlige, hvor der ikke er væsentlige modstridende interesser som f.eks. ved personfølsomme eller erhvervsfortrolige oplysninger.

Det fremgik videre, at der ikke er planer om at fastsætte særlige regler om offentlige myndigheders adgang til oplysninger i Køretøjsregistret. Her vil de almindelige regler i persondataloven og eventuelle regler i særlovgivningen gælde.

Det var Datatilsynets opfattelse, at det fremstod uklart, om der med lovudkastets § 17 og bemærkningen om yderligere adgang var tilsigtet en fravigelse af persondataloven for så vidt angår private adgang til oplysninger i registret, og hvad der i givet fald tænktes på.

Datatilsynet gik imidlertid ud fra, at hensigten var, at det i de regler, der skal fastsættes af skatteministeren, med respekt af persondatalovens rammer præciseres, hvornår og i hvilket omfang private kan få adgang til registret.

Tilsynet anbefalede derfor, at det blev tydeliggjort, at de regler, der skal fastsættes, inden for persondatalovens rammer vil præcisere, hvornår og i hvilket omfang private kan få adgang til Køretøjsregistret.

Hvis det var hensigten at skabe adgang til Køretøjsregistret i videre omfang, end hvad der følger af persondataloven, var det Datatilsynets opfattelse, at en sådan fravigelse af persondataloven skal ske i selve loven om digital motorregistrering frem for i administrativt fastsatte regler.

En særskilt hjemmel til videregivelse af oplysninger i videre omfang, end hvad der følger af persondataloven, burde således underkastes en politisk beslutningsproces, og noget sådant burde efter tilsynets opfattelse kun gennemføres, hvis vægtige samfundsmæssige hensyn taler herfor.

Datatilsynet gjorde samtidig opmærksom på, at mulighederne for at fravige persondataloven er begrænsede af de rammer, som er fastsat i databeskyttelsesdirektivet.

3. Det fremgik af bemærkningerne, at forsikringselskaber og syns- og omsynsvirksomheder skal kunne indberette til og trække på oplysninger i Køretøjsregistret.

Det var tanken, at de nævnte virksomheder i et vist omfang skal have en adgang til registrerede oplysninger alene ved brug af køretøjets registrerings- eller stelnummer.

Det fremgik ikke af bemærkningerne, om der var tale om at etablere terminaladgang til Køretøjsregistret for de nævnte virksomheder. Det var imidlertid blevet oplyst telefonisk, at dette var tilfældet.

Datatilsynet anbefalede, at forholdet blev tydeliggjort i bemærkningerne til lovforslaget, herunder at det blev præciseret, til hvilke formål denne adgang etableres.

Tilsynet gik herved ud fra, at forsikringssekskabernes adgang alene knytter sig til sager om motorkøretøjsforsikring, og at syns- og omsynsvirksomheders adgang alene er til brug for opgaver med syn og omsyn af motorkøretøjer.

Datatilsynet gik ud fra, at de nævnte virksomheder ikke optræder som databehandlere, men derimod er selvstændigt dataansvarlige, i det omfang indhentelse af oplysninger i registret sker med henblik på varetagelse af virksomhedens egne formål i forbindelse med løsning af syns- eller forsikringsmæssige opgaver. Tilsynet gik derfor ud fra, at terminaladgangen og anden videregivelse skal ske under iagttagelse af persondataloven.

Terminaladgangen blev således forudsat tilrettelagt i overensstemmelse med persondataloven. Dette medfører navnlig, at de enkelte brugeres adgang skal begrænses til de oplysninger, som det er nødvendigt for dem at få adgang til, og som de lovligt må behandle.

Datatilsynet pegede i den forbindelse særligt på, at reglerne om behandling af personnumre i private virksomheder er restriktive, og at der således kan være behov for bl.a. at indrette terminaladgangen således, at der ikke er adgang til personnumre.

4. Efter udkastets § 8, stk. 2, nr. 2, fritoges personer med handicap under visse betingelser for at betale for nummerplader. Det samme gjaldt efter § 11, stk. 2, nr. 2, for så vidt angår betaling for registrering, hvis en ægtefælle i tilfælde af separation eller skilsmisse overtager et køretøj, der er registreret i den anden ægtefælles navn.

Det var oplyst telefonisk, at der skal opbevares dokumentation for disse forhold. Det var endvidere oplyst, at oplysningerne vil blive registreret på en sådan måde, at der ikke ved privates terminaladgang til Køretøjsregistret vil blive adgang til sådanne oplysninger.

Datatilsynet lagde på denne baggrund til grund, at der hverken indgår fortrolige eller følsomme oplysninger i den del af Køretøjsregistret, der kan blive tale om at give private adgang til, jf. dog pkt. 6 om ejerens/brugerens egen adgang til oplysninger.

Tilsynet henledte opmærksomheden på, at behandling af følsomme oplysninger, jf. persondatalovens §§ 7 og 8, medfører anmeldelsespligt til og krav om forudgående udtalelse fra Datatilsynet efter reglerne om anmeldelse af behandlinger, der foretages for den offentlige forvaltning, jf. persondatalovens kapitel 12.

5. Det fremgik af lovudkastets § 1, stk. 3, at skatteministeren fastsætter regler om registrering i Køretøjsregistret. Det fremgik af bemærkningerne, at skatteministeren efter bestemmelsen kan give borgere ret til selv at omregistrere køretøjer over internettet.

Af bemærkningerne fremgik bl.a., at skatteministeren fastsætter regler, hvorefter private kan få oplysninger om et bestemt køretøj ved brug af køretøjets registrerings- eller stelnummer og en særlig kontrolkode, der kan fremgå af registreringsattesten eller på anden særlig måde. Herved muliggøres, at ejeren eller brugeren af et køretøj løbende kan se alt, hvad der er registreret om køretøjet, og den, der skal registrere eller omregistrere køretøjet, vil kunne se disse oplysninger.

Endvidere var det tanken, at forsikringsselskaber og syns- og omsynsvirksomheder i et vist omfang skal have en adgang til registrerede oplysninger alene ved brug af køretøjets registrerings- eller stelnummer.

I sammenfatningen af rapporten om Digital Motorregistrering, som lovforslaget byggede på, var det vedrørende borgerbetjeningen foreslået, at den nye ejer i forbindelse med den digitale indregistrering skal godtgøre at være i besiddelse af den seneste registreringsattest ved at oplyse en kontrolkode, der skal fremgå af registreringsattesten. For at opnå størst mulig sikkerhed for, at køretøjet er registreret til den rette ejer, skal den nye ejer identificere sig selv med en digital signatur.

Datatilsynet henledte i den forbindelse opmærksomheden på persondatalovens sikkerhedsregler som uddybet i sikkerhedsbekendtgørelsen og vejledningen hertil, og tilsynet gik ud fra, at ordningen med borgeres registrering af køretøjer over internettet vil blive tilrettelagt under iagttagelse heraf.

6. Ifølge bemærkningerne vil der i forbindelse med selvbetjeningsløsningen for ejeren eller brugeren af et køretøj være løbende adgang til at se alt, hvad der er registreret om køretøjet.

Datatilsynet gik ud fra, at der alene sigtes til oplysninger om køretøjet, og at der således ikke vil være adgang for f.eks. brugeren til at se oplysninger om ejerens dokumentation for fritagelse for betaling, personnummer, betalingsrestancer og lignende, og at der heller ikke vil være adgang for ejeren/brugeren til at se personlige oplysninger om tidligere ejere/brugere.

Datatilsynet henlede desuden opmærksomheden på, at de registrerede personer herudover vil have ret til indsigt efter persondatalovens § 31.

## **Lov om et indkomstregister (eIndkomst)**

Skatteministeriet anmodede om Datatilsynets bemærkninger til udkast til forslag til lov om et indkomstregister (eIndkomst) samt til udkast til forslag til lov om ændring af forskellige love (konsekvensændringer som følge af lov om et indkomstregister (eIndkomst)).

Lovforslaget lagde op til, at der oprettes et såkaldt eIndkomstregister, hvortil oplysninger om den enkelte borgers månedlige indkomst samt arbejdsomfang skal indberettes.

Hovedformålet med indkomstregistret er at forenkle kommunikationen mellem virksomheder og borgere ved at sikre, at ingen skal indberette de samme indkomstoplysninger flere gange til offentlige myndigheder. Endvidere vil indkomstregistret kunne effektivisere den offentlige sagsbehandling, forbedre offentlige myndigheders kontrolmuligheder, muliggøre dannelsen af mere pålidelige og aktuelle statistikker samt danne grundlag for væsentlige regelforenklinger.

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

1. Datatilsynet så som udgangspunkt positivt på, at man anvender de teknologiske muligheder for effektivisering af det administrative arbejde. Datatilsynet kunne således generelt tilslutte sig, at det er hensigtsmæssigt at søge at undgå, at de samme oplysninger skal indberettes flere gange til forskellige myndigheder.

Datatilsynet anså det ligeledes for positivt, at man forbedrer datakvaliteten. Når indberetningerne sker på månedsbasis i stedet for årligt, vil de data, som myndighederne kan få adgang til, i langt højere grad være ajourførte, end hvis der indhentes oplysninger fra de årlige indberetninger til ToldSkat. Dette er i overensstemmelse med kravet i persondatalovens § 5, stk. 4, om datakvalitet og ajourføring.

Etablering af indkomstregistret medfører ikke alene muligheder for administrative lettelser af mere serviceorienteret art (f.eks. i selvbetjeningsløsninger for borgerne), men også muligheder for effektiv kontrol.

Det måtte efter Datatilsynets opfattelse bero på en politisk vurdering, i hvilket omfang der skal ske kontrol af borgerne. Datatilsynet måtte imidlertid forudsætte, at det i lovforslaget – og eventuel følgelovgivning – klart omtales, hvilken kontrol myndighederne kan udøve på grundlag af indkomstregistret. Endvidere må den regulering, der etableres, sætte de fornødne rammer om de databehandlinger, der vil kunne foretages.

2. Det fremgik af de almindelige bemærkninger til udkastet, at det i forbindelse med fastsættelse af nærmere regler for indkomstregisteret, aftaler om adgang til oplysninger i registeret og driften af registeret vil blive sikret, at persondatalovens regler overholdes. Lovforslaget gav således ikke mulighed for fravigelse af reglerne i persondataloven.

3. Datatilsynet forudsatte, at told- og skatteforvaltningen er den dataansvarlige for elndkomstregistret, jf. definitionen i persondatalovens § 3, nr. 4.

4. Som anført var der flere formål med oprettelsen af indkomstregisteret. Registeret sikrer, at de samme oplysninger ikke skal afgives til flere forskellige offentlige myndigheder, men kun til et register. Det fremgik således af bemærkningerne, at det administrative besvær hos myndighederne blandt andet består i, at der i dag er for lidt genbrug af data og funktioner hos de offentlige myndigheder.

Det fremgik endvidere, at de offentlige myndigheders kontrolmuligheder vil blive forbedret som følge af adgangen til opdaterede indkomstoplysninger. Indkomstregistret vil således ifølge det anførte give en hidtil uset mulighed for at opdage snyd og socialt bedrageri. Det vil fremover være muligt at udføre totalkontrol af dagpengeudbetalingerne.

Indkomstregistret vil herudover betyde en bedre statistikindsamling og som følge heraf gøre det muligt at danne en mere opdateret og præcis beskæftigelses- og ligelønsstatistik.

Danmarks Statistik vil kunne trække en række oplysninger direkte i indkomstregistret, og en indberetning til indkomstregistret vil således samtidig være en indberetning til Danmarks Statistik.

Datatilsynet henledte i den forbindelse opmærksomheden på persondatalovens § 5, stk. 2.

Finalité-princippet i persondatalovens § 5, stk. 2, er direktivbestemt,<sup>13</sup> og såvel persondataloven som direktivet sætter således en grænse for myndighedernes genbrug af data.

---

<sup>13</sup> 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.

Datatilsynet gik ud fra, at Skatteministeriet havde overvejet formålene med det foreliggende forslag i forhold til dette princip og fundet dem forenelige hermed. Tilsynet havde ikke grundlag for at anfægte, at de nævnte formål var saglige. Datatilsynet påpegede imidlertid, at efterfølgende etablering af adgang til oplysningerne i indkomstregistret må forudsætte, at en sådan adgang ikke er uforenelig med de angivne formål, jf. i øvrigt det nedenfor under pkt. 5 anførte.

Med hensyn til anvendelsen af registret til brug for udarbejdelse af statistik gjorde Datatilsynet opmærksom på, at persondataloven på en række punkter indeholder særregler for statistikoplysninger. Dette gælder bl.a. de materielle behandlingsregler, se særligt § 10, samt reglerne om oplysningspligt og indsigtret.

Oplysninger, som er indsamlet til statistikformål, skal imidlertid holdes adskilt fra andre oplysninger og må ikke anvendes til andre formål, herunder administrative formål.

Hvis oplysninger alene indberettes med henblik på statistik, må de således ikke senere videregives til brug for f.eks. kontrolformål. Datatilsynet anbefalede, at det uddybes i bemærkningerne, hvordan dette sikres.

Datatilsynet henledte endvidere opmærksomheden på persondatalovens § 5, stk. 3.

Tilsynet noterede sig, at det i lovforslagets bemærkninger var anført, at konsekvensen af forslaget bliver, at myndighederne får en mere samlet indsigt i borgernes indkomstforhold gennem registrering i et fælles offentligt register.

Henset til formålene med registret havde Datatilsynet ikke grundlag for at antage, at registret er i strid med proportionalitetsprincippet i persondatalovens § 5, stk. 3. Datatilsynet påpegede imidlertid, at efterfølgende etablering af adgang til oplysningerne i registret må forudsætte en selvstændig vurdering i forhold til § 5, stk. 3.

Datatilsynet gjorde endelig opmærksom på, at behandling af oplysninger skal ske i overensstemmelse med princippet om god databehandlingsskik, jf. persondatalovens § 5, stk. 1.

5. Efter lovudkastets § 7, stk. 1, kan oplysninger, som er registreret i indkomstregistret, stilles til rådighed for kommunale og statslige myndigheder, anerkendte arbejdsløsheds-kasser og andre, i det omfang de pågældende i henhold til anden lovgivning kan få stillet de pågældende oplysninger til rådighed.

Ligeledes fremgik det af de almindelige bemærkninger til lovudkastet, at adgang til oplysninger i registret kræver lovhjemmel og forudsætter, at der indgås en aftale med den dataansvarlige om adgangen til registret.

Udkastets § 7 giver således ikke selvstændig hjemmel til adgang til oplysninger, og hjemlen skulle ifølge bemærkningerne findes i lovgivningen på de enkelte myndigheders områder. Det samtidigt fremsendte udkast til lov om konsekvensændringer som følge af indkomstregisterloven (følgelovudkastet) skaber sådanne hjemler i en række love inden for Beskæftigelsesministeriets, Fødevareministeriets, Indenrigs- og Sundhedsministeriets, Integrationsministeriets, Skatteministeriets, Socialministeriets og Undervisningsministeriets sagsområder.

Datatilsynet noterede sig, at det vil være en betingelse for adgangen til registret, at ikke alene persondatalovens regler er opfyldt, men at der tillige i anden lovgivning skal være særskilt hjemmel hertil. Datatilsynet forudsatte, at de hjemler i særlovgivningen, der vil blive etableret, skal respektere persondatalovens rammer.<sup>14</sup>

Tilsynet understregede navnlig vigtigheden af, at det konkret overvejes, hvorvidt det er sagligt og nødvendigt at give adgang til indkomstregistret, og om der inden for det enkelte område kan gives alene en begrænset adgang til registrets oplysninger. Det er således et grundlæggende krav, at offentlige myndigheder mv. ikke må behandle eller have adgang til oplysninger, som de ikke har behov for i forbindelse med deres konkrete myndighedsudøvelse. Der henvises tillige til det anførte nedenfor under pkt. 7.

6. Det fremgik af udkastet til indkomstregisterloven, at lovforslaget ikke giver selvstændig hjemmel til samkøring af registre i kontroløjemed. I det omfang, der på det enkelte lovområde er særskilt hjemmel til samkøring i kontroløjemed, vil sådanne bestemmelser i kombination med bestemmelserne om adgang til indkomstregistret kunne indebære, at registrets oplysninger kan anvendes ved sådan kontrolsamkøring over for borgere og virksomheder.

Det fremgik af en række af bestemmelserne i følgelovudkastet og bemærkningerne hertil, at adgangen til indkomstregistret bl.a. gives med henblik på myndighedernes kontrol af f.eks. udbetalingsgrundlag. Det var dog ikke angivet udtrykkeligt, at der hermed skabes hjemmel til samkøring i kontroløjemed.

---

<sup>14</sup> Det fremgår af bemærkningerne til det fremsatte lovforslag (L 119 som fremsat af skatteministeren den 11. januar 2006), at terminaladgang til registret reguleres gennem udtrykkelige bestemmelser herom i den relevante særlovgivning.

Datatilsynet gengav betingelserne for myndigheders sammenstilling og samkøring i kontroløjemed, jf. tilsynets praksis.

Hvis det med følgelovudkastet var hensigten at skabe en række hjemler til samkøring i kontroløjemed, anbefalede Datatilsynet, at dette udtrykkeligt fremgik af bemærkningerne til de enkelte bestemmelser.

7. Ifølge bemærkningerne til udkastet til lov om et indkomstregister var det målet, at data oprettes og administreres på en kosteffektiv måde og stilles til rådighed via åbne, kontrollerede grænseflader, hvor andre it-systemer med legal autorisation får adgang til de data og funktioner, de har brug for.

I forlængelse heraf henledte Datatilsynet opmærksomheden på sikkerhedsbekendtgørelsens regler om autorisation og adgangskontrol.

8. Efter lovudkastets § 6 har den, de indberettede oplysninger vedrører, adgang til oplysninger, der er indberettet vedrørende den pågældende.

Det fremgik af bemærkningerne til bestemmelsen, at der etableres elektronisk adgang til egne indberettede oplysninger.

Datatilsynet bemærkede, at der herudover vil være ret til indsigt efter persondatalovens regler herom.

9. Efter lovudkastets § 7, stk. 2, stilles oplysningerne i indkomstregistret til rådighed i elektronisk form. Det fremgik af bemærkningerne, at myndighederne kan få adgang til oplysningerne via batchkørsel, webservice og online opslag.

Ved følgelovudkastets § 13, nr. 2 (kildeskattelovens § 48, stk. 1), var det foreslået, at den indeholdelsespligtige, som udbetaler A-indkomst til den skattepligtige, elektronisk skal indhente skattekort, bikort eller frikort (eSkattekort) fra told- og skatteforvaltningen.

I relation til elektronisk opslag i indkomstregistret og indhentelse/fremsendelse af eSkattekort bemærkede Datatilsynet, at persondatalovens sikkerhedskrav efter tilsynets opfattelse medfører, at der ved transmission af oplysninger, som må betragtes som fortrolige (f.eks. oplysninger om personnumre eller om økonomiske forhold o.l.), over det åbne internet som minimum skal foretages kryptering.

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

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

Datatilsynet noterede sig, at lovforslaget ikke gav mulighed for fravigelse af persondataloven og gik derfor ud fra, at såvel elektronisk indberetning til registret og videregivelse herfra som indhentelse/fremsendelse af eSkattekort vil ske under iagttagelse af de fornødne sikkerhedsforanstaltninger.

Datatilsynet henlede desuden opmærksomheden på den dataansvarliges forpligtelse til at fastsætte uddybende sikkerhedsregler, jf. § 5 i sikkerhedsbekendtgørelsen. Datatilsynet gik i øvrigt ud fra, at såvel told- og skatteforvaltningen samt de myndigheder mv., der får adgang til oplysningerne i registret, udarbejder en sikkerhedspolitik.

Efter lovudkastets § 6, stk. 2, fastsætter skatteministeren efter nærmere aftale med justitsministeren de nærmere regler for behandling af oplysninger i indkomstregistret.

Det fremgik af bemærkningerne til bestemmelsen, at der bl.a. kan fastsættes regler om sikkerhed ved modtagelse og videregivelse, opbevaring og sletning af oplysninger.

Datatilsynet gik ud fra, at der vil blive taget højde for ovenstående ved fastsættelse af sådanne regler.

10. Af lovudkastets § 7, stk. 1, fremgik det som anført, at oplysninger, som er registreret i indkomstregistret, kan stilles til rådighed for kommunale og statslige myndigheder, anerkendte arbejdsløsheds-kasser og andre, i det omfang de pågældende i henhold til anden lovgivning kan få stillet de pågældende oplysninger til rådighed.

Efter udkastets § 7, stk. 4, fastsætter skatteministeren efter aftale med justitsministeren og videnskabsministeren de nærmere regler for bl.a. adgang til at få stillet oplysninger fra indkomstregisteret til rådighed.

Af bemærkningerne til § 7, stk. 4, fremgik det, at det skal aftales, hvilke oplysninger de enkelte myndigheder må modtage. Indgåelsen af aftalerne vil ske under iagttagelse af reglerne i persondataloven. Det betød ifølge bemærkningerne, at told- og skatteforvaltningen skulle verificere myndighedernes aftaler hos Datatilsynet.

Det var oplyst, at der med ovenstående mentes, at told- og skatteforvaltningen i forbindelse med hver enkelt aftale skulle have verificeret hos Datatilsynet, at den pågældende myndighed har hjemmel til at modtage oplysninger fra indkomstregistret.

Datatilsynet fandt det uklart, hvad hensigten med § 7, stk. 4, var, herunder forholdet mellem § 7, stk. 1, og § 7, stk. 4, sammenholdt med bemærkningerne om aftaler, som skal verificeres af Datatilsynet.

Konkret med hensyn til aftalerne noterede Datatilsynet sig, at indgåelsen af aftalerne vil ske under iagttagelse af reglerne i persondataloven.

Tilsynet fandt derfor, at det i overensstemmelse med persondatalovens almindelige ordning må være den dataansvarlige, der i første omgang må vurdere, om betingelserne for videregivelse er opfyldt, dvs. om myndigheden mv. har den efter § 7, stk. 1, fornødne hjemmel.

I tvivlstilfælde vil Datatilsynet selvsagt stå til rådighed med rådgivning og vejledning.

Der vil endvidere kunne blive behov for, at de myndigheder, der skal indberette oplysninger til eller indhente oplysninger fra indkomstregistret, gennemgår deres eksisterende anmeldelser med henblik på at vurdere, om der skal foretages ændringer heri. Datatilsynet vil i forbindelse hermed være i dialog med de pågældende.

## **Lov om ændring af lov om dagpenge ved sygdom eller fødsel**

Arbejdsdirektoratet anmodede om Datatilsynets bemærkninger til udkast til forslag til lov om ændring af lov om dagpenge ved sygdom eller fødsel (Digital kommunikation, registersamkøring i kontroløjemed).

Tilsynets udtalelse gengives i alt væsentligt nedenfor.

1. Det fremgik af lovforslaget, at der som led i regeringsgrundlagets målsætning om at forenkle virksomhedernes administrative byrder samt øge brug af digitalisering ønskes etableret en landsdækkende digital løsning for anmeldelse af fravær og anmodning om refusion af syge- og barseldagpenge

2. Ved lovforslaget blev § 37 a, stk. 1, indsat, hvorefter beskæftigelsesministeren efter forhandling med ministeren for familie- og forbrugeranliggender kan fastsætte regler om muligheden for anvendelse af digital kommunikation i forbindelse med administration af sager om dagpenge.

Det fremgik af bemærkningerne, at bestemmelsen indsættes i loven, for at der kan fastsættes de tekniske krav til den landsdækkende digitale løsning samt fastlægges krav i forbindelse med anvendelse af den digitale mulighed for indberetning.

Datatilsynet forudsatte, at den digitale kommunikation og anden databehandling i forbindelse med den landsdækkende løsning skal foregå under iagttagelse af

persondataloven. Det vil bl.a. sige, at lovens betingelser for behandling af personoplysninger skal være opfyldt, at oplysningerne skal beskyttes med de fornødne sikkerhedsforanstaltninger, og at reglerne om de registreredes rettigheder skal iagttages.

Datatilsynet kunne i tilknytning hertil oplyse, at tilsynet i forbindelse med en række initiativer til fremme af elektronisk borgerservice i det offentlige har påtaget sig opgaven som central godkendelsesinstans. Datatilsynet henviste i øvrigt til persondatalovens § 57.

Datatilsynet forventede herefter at blive hørt inden fastsættelse af reglerne om digital kommunikation.

3. Ved lovforslaget blev endvidere indsat § 37 a, stk. 2, hvorefter direktøren for Arbejdsdirektoratet, til brug for kommunernes administration af loven, kan indhente oplysninger fra andre offentlige myndigheder, private firmaer og arbejdsløsheds-kasser, herunder oplysninger om enkeltpersoners indkomstforhold i elektronisk form, med henblik på registersamkøring i kontroløjemed. Resultatet af sammenkøringen kan videregives til den kommune, der behandler sagen om retten til dagpenge.

Det fremgik af bemærkningerne til lovforslaget, at der i forbindelse med den digitale landsdækkende indberetningsløsning vil blive mulighed for at lave elektronisk kontrol ved hjælp af digital "validering fra atypisk sygefravær" (VAS). VAS er et system, hvor alle anmeldelser og refusionsanmodninger i den digitale landsdækkende løsning skal beriges med data, der kan tilkendegive, om sagen afviger fra normaladfærden på en måde, der indikerer et misbrug eller fejl. Resultatet af VAS videresendes til sagsbehandlerne i kommunerne. Til at afgøre, om der er tale om atypisk sygefravær, genbruges registerdata, herunder oplysninger om eventuelle tidligere sygedagpengerefusioner, CVR-oplysninger og sammenligninger med andre virksomheder, CPR-data mv. Resultatet af samkøringen af data kan alene sendes videre til den kommune, der behandler sagen om dagpenge.

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

Datatilsynet gjorde i den forbindelse opmærksom på, at persondataloven omfatter fysiske personer. Oplysninger om juridiske personer, såsom aktieselskaber, anpartsselskaber m.v., falder uden for lovens almindelige regulering. Derimod er oplysninger om enkeltmandsejede virksomheder omfattet af loven.

Det samme gælder interessentskaber i det omfang, interessenterne er fysiske personer.

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

4. Datatilsynet noterede sig, at det fremgik af bemærkningerne, at VAS i udviklingsfasen har været anmeldt til Datatilsynet, og at anmeldelsen vil blive ændret i overensstemmelse med ønsket om registersamkøring i kontroløjemed.

Datatilsynet oplyste endvidere, at det fremgår af den eksisterende anmeldelse til Datatilsynet, at behandlingen udelukkende skal finde sted i videnskabeligt og statistisk øjemed.

Datatilsynet havde tidligere afgivet udtalelse til Arbejdsdirektoratet i anledning af anmeldelsen af VAS. I udtalelsen havde Datatilsynet bl.a. anført, at det følger af persondataloven § 10, stk. 1, at der kan behandles oplysninger som nævnt i lovens § 7, stk. 1, eller § 8, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for udførelsen af undersøgelsen. Af § 10, stk. 2, fremgår endvidere, at oplysninger omfattet af § 10, stk. 1, ikke senere må behandles i andet end statistisk eller videnskabeligt øjemed. Det samme gælder de ikke-følsomme oplysninger, som indgår i behandlingen, jf. § 10, stk. 2, 2. pkt. Oplysningerne må således ikke efterfølgende anvendes til at træffe foranstaltninger eller afgørelser vedrørende de registrerede personer. Oplysningerne må endvidere kun videregives til tredjemand efter forudgående tilladelse fra Datatilsynet, og i givet fald kun med henblik på udførelse af undersøgelser i statistisk eller videnskabeligt øjemed, jf. lovens § 10, stk. 3.

VAS er således anmeldt til Datatilsynet som et statistisk system, og oplysningerne i VAS må ikke i personhenførbart form anvendes til administrative formål eller til samkøring i kontroløjemed. Der kan således alene anvendes statistiske oplysninger fra VAS i ikke-personhenførbart form. Endvidere kan der ikke i den eksisterende anmeldelse af VAS foretages ændring i overensstemmelse med ønsket om registersamkøring i kontroløjemed.

Den nye kontrolsamkøring vil derimod kunne anmeldes til Datatilsynet som en ny behandling, men dette medfører dog ikke, at personoplysninger, der behandles i VAS, kan indgå i det nye system, bortset fra i fuldstændig anonym form.

5. Det ønskede system, hvor der skal ske kontrolsamkøring, vil efter det oplyste have til formål at understøtte kommunernes opgaver og ikke Arbejdsdirektoratets egne opgaver. En ordning, hvor Arbejdsdirektoratet skal være dataansvarlig for

dette system, synes ikke umiddelbart at være i tråd med persondatalovens krav om, at en myndighed kun må behandle de oplysninger, der er nødvendige for, at den kan varetage sine opgaver. Datatilsynet ville imidlertid ikke udelukke, at Arbejdsdirektoratet i loven kan tillægges en opgave som ansvarlig for systemet/registeret. Datatilsynet anbefalede, at dette i givet fald fastlægges i selve lovteksten, hvori det tillige bør anføres, hvad formålet med systemet/registeret er.

6. Herudover forudsatte Datatilsynet, at systemet vil blive opbygget og anvendt under iagttagelse af persondataloven.

Datatilsynet fremhævede bl.a., at antallet af sagsbehandlere, som er beskæftiget med sammenstilling og samkøring i kontroløjemed, efter Datatilsynets opfattelse skal begrænses mest muligt.

Datatilsynet fremhævede desuden forpligtigelsen efter persondatalovens § 29 til at give information til den registrerede. Denne regel medfører efter Datatilsynets umiddelbare opfattelse, at Arbejdsdirektoratet har pligt til at give meddelelse til de personer, der behandles oplysninger om, i hvert fald senest når den i § 37 a, stk. 2, beskrevne videregivelse af resultatet af samkøringen til kommunerne finder sted.

## **Lov om ændring af patentloven**

Patent- og Varemærkestyrelsen anmodede om Datatilsynets bemærkninger til udkast til forslag til lov om ændring af patentloven mv.

Lovforslaget havde til formål at implementere EU-direktiv 2004/48/EF om håndhævelse af intellektuelle rettigheder (håndhævelsesdirektivet) og indebar ændringer af såvel patentloven som andre immaterialretlige love. Samtidig forberedte kulturministeren tilsvarende ændringer i ophavsretsloven.

Lovforslaget åbnede bl.a. mulighed for, at den, der dømmes for krænkelse af en patentrettighed el.lign., efter begæring fra den krænkede kan dømmes til at skulle offentliggøre dommen.

Tilsynets udtalelse til lovforslaget gengives i alt væsentligt nedenfor.

### **1. Dataansvar**

Ud fra lovforslaget var det Datatilsynets umiddelbare vurdering, at den ret, der bestemmer, at en dom skal offentliggøres, ligeledes må anses for at være dataansvarlig, når dommen herefter offentliggøres (i overensstemmelse med rettens bestemmelse), jf. definitionen i persondatalovens § 3, nr. 4.

Datatilsynet lagde herved vægt på, at den pågældende ret ifølge lovforslagets bemærkninger, ud over spørgsmålet om selve offentliggørelsen, også vil have

kompetence til at træffe afgørelse om offentliggørelsens omfang, form og placering etc. Tilsynet gik desuden ud fra, at det er den pågældende ret, der har formuleret dommen.<sup>15</sup>

## 2. Datatilsynets kompetence

Datatilsynet udtalte, at tilsynet med behandling af oplysninger, der foretages for domstolene, hører under Domstolsstyrelsen henholdsvis vedkommende ret, jf. reglerne i persondatalovens kapitel 17. Det ligger således uden for Datatilsynets kompetenceområde at tage stilling til spørgsmål vedrørende domstolenes behandlinger af personoplysninger.

Datatilsynet bemærkede desuden, at det fremgår af persondatalovens § 68, stk. 2, at ved udarbejdelse af bekendtgørelser eller lignende generelle forskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, der foretages for domstolene, skal der indhentes en udtalelse fra Domstolsstyrelsen. Det er endvidere forudsat i lovens forarbejder, at der indhentes en udtalelse fra Domstolsstyrelsen i forbindelse med regeringens udarbejdelse af lovforslag, der vedrører behandling af oplysninger, der foretages for domstolene. Høringspligten gælder både, for så vidt angår retternes administrative forhold, og med hensyn til de judicielle funktioner.

Datatilsynet begrænsede sig derfor til mere generelle databeskyttelsesretlige bemærkninger i det følgende.

## 3. Persondatalovens anvendelsesområde

Datatilsynet udtalte, at i de tilfælde, hvor der i forbindelse med offentliggørelse af domme vedrørende krænkelser af immaterielle rettigheder indgår personoplysninger, vil offentliggørelsen som udgangspunkt være omfattet af persondatalovens anvendelsesområde.

Datatilsynet noterede sig, at det følger af håndhævelsesdirektivets betragtning 15, at direktivet ikke bør berøre 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 (databeskyttelsesdirektivet).

Datatilsynet noterede sig endvidere, at det af bemærkningerne til lovforslaget fremgik, at offentliggørelse af dommene skal ske med respekt af de gældende regler i persondataloven.

---

<sup>15</sup> I det fremsatte lovforslag (L 48 som fremsat af økonomi- og erhvervsministeren den 9. november 2005) fremgår det af bemærkningerne, at det er krænkeren, der er at anse for dataansvarlig.

#### 4. Offentliggørelse af oplysninger

Det fremgik af den foreslåede § 60 a i patentloven, at retten på begæring kan bestemme, at dommen skal offentliggøres i sin helhed eller i uddrag.

Datatilsynet noterede sig, at det fremgik af bemærkningerne til bestemmelsen, at de pågældende oplysninger anonymiseres, hvis der efter en konkret vurdering ikke er hjemmel i persondataloven til offentliggørelse.

Datatilsynet forudsatte i den sammenhæng, at det er den pågældende ret, der som dataansvarlig foretager vurderingen af, hvorvidt oplysninger i en dom skal slettes/anonymiseres inden offentliggørelse. Datatilsynet gik ud fra, at denne vurdering må foretages under iagttagelse af persondataloven, således som loven gælder for domstolene. Datatilsynet henledte i den forbindelse opmærksomheden på, at eksempelvis persondatalovens § 8 kun vedrører den offentlige forvaltning, og at domstolenes behandling af de typer af oplysninger, der er omfattet af bestemmelsen, som konsekvens heraf skal følge reglerne i lovens § 6.

Uanset dette var det dog Datatilsynets opfattelse, at offentliggørelse af oplysninger om strafbare forhold (eksempelvis på internettet) er en meget indgribende form for behandling, og tilsynet foreslog, at det nøje overvejes i forhold til persondataloven og databeskyttelsesdirektivet, i hvilket omfang en sådan offentliggørelse skal kunne ske, og i hvilket omfang der skal ske sletning eller anonymisering inden offentliggørelse. Opmærksomheden henledtes særligt på databeskyttelsesdirektivets artikel 8, stk. 5 og 6.

Ligeledes for så vidt angik de kategorier af følsomme oplysninger, der er omfattet af persondatalovens § 7, samt oplysninger om personnumre, ville offentliggørelse efter Datatilsynets opfattelse være en meget indgribende behandling. Tilsynet anbefalede også på dette punkt, at det nøje overvejes, om og i givet fald i hvilken form og på hvilket grundlag sådanne oplysninger skal offentliggøres.

#### **Lov om ændring af lov om jordbrugets anvendelse af gødning og om plantedække**

Ministeriet for Fødevarer, Landbrug og Fiskeri anmodede Datatilsynet om en udtalelse over forslag til lov om ændring af lov om jordbrugets anvendelse af gødning og om plantedække.

Lovforslaget var et element i regeringens initiativer til fremme af den miljøteknologiske udvikling på landområdet. Med lovforslaget blev barriererne for udvikling af alternativ anvendelse af husdyrgødning fjernet. Som noget nyt blev det foreslået, at der blev indsat en hjemmel til offentliggørelse af bl.a. oplysninger, som jordbrugsvirksomheder indberetter i forbindelse med indsendelse af gødningsregnskaber.

Tilsynets udtalelse gengives i det væsentligste nedenfor.

1. Af lovforslaget fremgik, at ministeren for fødevarer, landbrug og fiskeri eller den, ministeren bemyndiger dertil, hos andre offentlige myndigheder kan indhente de oplysninger, der er nødvendige for at kontrollere overholdelsen af loven og regler udstedt i medfør heraf. Ministeren eller den, ministeren bemyndiger dertil, kunne i forbindelse hermed foretage *sammenstilling* og *samkøring* af oplysninger, herunder personoplysninger, i *kontroløjemed* samt videregive oplysninger, herunder sammenstillede og samkørte oplysninger.

Det fremgik endvidere af bemærkningerne, at hjemlen umiddelbart tænkes brugt i forbindelse med kontrol af, om mængden af kvælstofholdige gødninger, som jordbrugerne indfører direkte fra tredjelande eller samhandler direkte her i landet, også figurerer i vedkommende jordbrugs gødningsregnskab.

Endvidere fremgik det af bemærkningerne, at der vil kunne ske samkøring af oplysninger fra henholdsvis Direktoratet for FødevarerErhverv, støtteoplysninger, og Fødevarestyrelsen, CHR-registret, med Plantedirektoratets register for afgiftsfritagelse. Denne samkøring kan anvendes til at kontrollere, om en virksomhed med mere end 10 dyreenheder overholder pligten til at være tilmeldt registret for afgiftsfritagelse samt til at foretage en kvalitetskontrol af de oplysninger, der skal afgives i forbindelse med indberetning til den fælles husdyrindberetning og til den fælles indberetning.

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

Datatilsynet lagde i denne forbindelse vægt på, at det i øvrigt er Datatilsynets opfattelse, at antallet af sagsbehandlere, som er beskæftiget med sammenstilling og samkøring i kontroløjemed, skal begrænses mest muligt.

2. Af lovforslaget fulgte endvidere, at ministeren eller den, ministeren bemyndiger dertil, kan *videregive* oplysninger, herunder sammenstillede og samkørte oplysninger.

Datatilsynet redegjorde for persondatalovens § 5, stk. 1 og 2, § 6, stk. 1, nr. 7, og § 8, stk. 1.

Datatilsynet henledte i denne forbindelse ministeriets opmærksomhed på, at behandling, herunder videregivelse, af personoplysninger alene kan ske, såfremt de nævnte betingelser i persondataloven er opfyldt.

3. Det fulgte af lovforslaget, at ministeren for fødevarer, landbrug og fiskeri bemyndiges til at fastsætte regler om offentliggørelse med navns nævnelse af indberettede oplysninger, oplysninger om overtrædelser og andre resultater på grundlag af kontrol, som gennemføres i henhold til loven eller regler udstedt i medfør af loven. Ministeren for fødevarer, landbrug og fiskeri kan endvidere bestemme, at offentliggørelsen skal ske elektronisk på internettet.

Af de almindelige bemærkninger til lovforslaget fremgik, at eftersom gødningsregnskaberne kan indeholde oplysninger om strafbare forhold, der kan betegnes som fortrolige, og som dermed vil kunne undtages fra aktindsigt, er der behov for en udtrykkelig lovhjemmel til offentliggørelse af alle indberettede oplysninger.

Det stod ikke Datatilsynet klart, hvilke nærmere oplysninger om overtrædelser der ville blive offentliggjort, og tilsynet anbefalede, at det overvejedes tydeliggjort.

a) I det omfang, der indgår oplysninger om personers strafbare forhold, henledte Datatilsynet opmærksomheden på persondatalovens § 8, stk. 2, hvorefter oplysninger om strafbare forhold som udgangspunkt ikke må videregives. Videregivelse kan dog ske, såfremt en af betingelserne i § 8, stk. 2, nr. 1-4 er opfyldt. Herudover følger det af § 8, stk. 6, at videregivelse i øvrigt kan finde sted, hvis betingelserne i § 7 er opfyldt.

Det var Datatilsynets umiddelbare vurdering, at disse betingelser ikke er opfyldt i forbindelse med offentliggørelse af oplysninger om navngivne personer, som har overtrådt lovgivningen.

I den forbindelse henledte Datatilsynet opmærksomheden på persondatalovens § 2, stk. 1, og forarbejderne til denne bestemmelse om forholdet mellem persondataloven og anden lovgivning. Konsekvensen af reglen er, at persondataloven går forud for regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en dårligere retsstilling end persondataloven. Dette gælder dog ikke, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod databeskyttelsesdirektivet.

I forbindelse med Folketingets behandling af forslag til lov om behandling af personoplysninger (L147, 1999-2000) tilkendegav Justitsministeriet i et svar på et spørgsmål (nr. 3<sup>16</sup>) fra Folketingets retsudvalg, at for så vidt angår ”nye særlovsbestemmelser” – dvs. særlovsbestemmelser, der træder i kraft efter ikrafttrædelsen af loven om behandling af personoplysninger – bør der i forslaget til særloven eller i bemærkningerne hertil udtrykkeligt tages stilling til, om den

---

16 L 147 bilag 17. Justitsministeriets svar på spørgsmål om ministerens kommentar til notat fra Det Retsvidenskabelige Institut B.

registrerede skal have en dårligere retsstilling end den, der er fastsat i den generelle lov om behandling af personoplysninger.

Datatilsynet henstillede derfor, at det tydeliggjordes i lovforslagets bemærkninger, hvorvidt der tilsigtes en fravigelse af persondataloven. Såfremt dette var tilfældet, henstillede Datatilsynet desuden, at Ministeriet for Fødevarer, Landbrug og Fiskeri foretog en vurdering af, hvorvidt den ønskede lovregel om offentliggørelse af oplysninger var forenelig med databeskyttelsesdirektivet. Ministeriet skulle navnlig foretage en vurdering i forhold til direktivets artikel 8, stk. 4-6. Ud over at der i den nationale lovgivning skal gives tilstrækkelige, specifikke garantier som beskrevet i direktivets artikel 8, stk. 5, henlede Datatilsynet opmærksomheden på forpligtelsen til at underrette kommissionen i artikel 8, stk. 6.

I tilknytning hertil henlede Datatilsynet opmærksomheden på, at det i afsnit 10 om forholdet til EU-retten var anført, at lovforslaget ikke indeholdt EU-retlige aspekter. Datatilsynet foreslog, at databeskyttelsesdirektivet overvejedes anført.

b) Offentliggørelse af navnene på de personer, der overtræder loven, ville i medfør af loven kunne ske. Derimod var der ikke i forslaget fastsat regler for, hvilken hjemmel modtagerne af oplysninger har til at behandle oplysningerne.

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

.....

Efter afgivelse af høringssvaret blev der afholdt et møde mellem Ministeriet for Fødevarer, Landbrug og Fiskeri og Datatilsynet, og i forbindelse med udsendelse af et revideret forslag til lov om ændring af lov om jordbrugets anvendelse af gødning og om plantedække anmodede ministeriet på ny Datatilsynet om en udtalelse.

Tilsynets udtalelse gengives i alt væsentligt nedenfor.

1. Det reviderede lovforslag omfattede en hjemmel til offentliggørelse af gødningsregnskaber, kontrolresultater, herunder påtaler og vedtagne administrative bødeforelæg på internettet. I bemærkningerne var bl.a. anført, at hensigten hermed er at lade et kendskab til gødskning med husdyr- og handelsgødning af betydning for miljøet indgå i lokal debat og planlægning. En åbenhed omkring forhold af betydning for miljøet er netop en af de bærende tanker bag FN/ECE-

konventionen om adgang til oplysninger, offentlig deltagelse i beslutningsprocesser samt adgang til klage og domstolsprøvelse på miljøområdet ("Århuskonventionen"), der er ratificeret af såvel Danmark som EU.

En viden om gødskning med husdyr- og handelsgødning – f.eks. inden for en enkelt kommune eller i forhold til et bestemt naturområde – og her samtidig et kendskab til de jordbrugsvirksomheder, der har foretaget overgødsning – kan medvirke til at forbedre borgernes grundlag for at deltage i debatten om miljøforhold i det pågældende område.

Med lovforslaget var det hensigten, at Fødevarerministeriet skal kunne offentliggøre oplysningerne fra gødningsregnskaberne, kontrolresultater, herunder påbud, samt vedtagne administrative bødeforelæg. Der er behov for en udtrykkelig lovhjemmel til offentliggørelse, hvis offentliggørelsen skal omfatte som udgangspunkt fortrolige oplysninger efter de almindelige regler om tavshedspligt.

Med lovforslaget kan offentliggørelse af gødningsregnskaber, hvortil er knyttet en sanktion i form af administrative bøder, kun finde sted, såfremt jordbrugsvirksomheden tydeligt og skriftligt er blevet gjort opmærksom på, at vedtagelse af den administrative bøde vil have den konsekvens, at gødningsregnskab og sanktion vil blive offentliggjort på internettet.

Ved offentliggørelse af de rene gødningsregnskabsoplysninger vil en evt. overgødsning fremgå, når kvælstofforbruget holdes op mod arealet. Offentligheden kan alene med disse oplysninger og med ganske stor præcision kalkulere størrelsen på den bøde, som overgødsningen udløser. Dette skyldes det særlige forhold, at bødeniveauer direkte fremgår af bemærkningerne til forslag til lov om jordbrugets anvendelse af gødning og om plantedække (L 58, 1997-98, 2. samling).

I lovforslagets bemærkninger til § 1, nr. 5, om indsættelse af bestemmelsen i § 28 a var anført, at de virksomhedsoplysninger, som foreslås offentliggjort, vedrører jordbrugsvirksomheder, hvor en opdeling i en forretningsmæssig del og en privat del ikke er mulig, og hvor de oplysninger, der ønskes offentliggjort, omhandler jordbrugsvirksomhedens drift. Offentliggørelse tænkes i praksis gennemført efter følgende principper:

Offentliggørelsen sker første gang, når ændringer i oplysningerne som følge af Plantedirektoratets sagsbehandling og kontrol er afsluttet ca. 9 måneder efter deres indsendelse. For de sager, hvor sagsbehandlingen fortsat pågår, vil der løbende ske offentliggørelse, når sagsbehandling og kontrol er afsluttet. Offentliggørelsen vedrører oplysninger om aftaler med andre jordbrugsvirksomheder om overførsel af husdyrgødning. Typen af den enkelte aftale og hvem den er indgået med, vil ikke fremgå af offentliggørelsen.

For gødningsregnskaber, der har været udtrukket til kontrol, påføres i forbindelse med offentliggørelsen koder for henholdsvis ingen bemærkninger, påtale, eller vedtaget administrativt bødeforelæg.

Alle oplysninger, herunder gødningsregnskaber, vedrørende sager, der er videregivet til politiet med anmodning om tiltalerejsning, samt sager hvor der er faldet dom, vil ikke blive offentliggjort.

Jordbrugsvirksomhederne vil i forbindelse med et administrativt bødeforelæg tydeligt og skriftligt blive oplyst om, at oplysningerne vil blive offentliggjort på internettet ved vedtagelse af bøden.

Oplysningerne vil være tilgængelige på internettet i 5 år. Oplysninger, der inden for denne 5-års frist viser sig urigtige eller vildledende, vil i overensstemmelse med persondatalovens almindelige behandlingsregler blive slettet eller berigtiget.

Lovens indhold skal være kendt forud for indsendelse af det gødningsregnskab, som lægges til grund for den første offentliggørelse. Som følge heraf vil første offentliggørelse kunne ske for planperioden 2005/06. Gødningsregnskabet for denne planperiode indsendes 31. marts 2007 og vil således kunne offentliggøres ved udgangen af 2007.

2. Datatilsynet bemærkede, at oplysninger om påtaler efter tilsynets opfattelse kan være af fortrolig karakter. Sådanne oplysninger vil som udgangspunkt ikke umiddelbart kunne offentliggøres inden for persondatalovens rammer.

Med hensyn til offentliggørelse af oplysninger om strafbare forhold var der efter Datatilsynets opfattelse ligeledes tale om en fravigelse af persondataloven, der medfører en ringere retsstilling for de registrerede personer.

Som beskrevet i Datatilsynets første høringssvar kan persondataloven fraviges ved særlovgivning, hvis denne ikke strider mod databeskyttelsesdirektivet.

Datatilsynet anbefalede, at forholdet til persondataloven blev beskrevet i lovforslaget, herunder at der er tale om en fravigelse, der medfører en ringere retsstilling for de registrerede personer end persondataloven.

En særskilt hjemmel til registrering og videregivelse af oplysninger i videre omfang, end hvad der følger af persondataloven, forudsætter efter tilsynets opfattelse en selvstændig vurdering af, hvilke vægtige samfundsmæssige hensyn der taler for en sådan ordning.

Det må i sidste ende bero på en politisk vurdering, om der i det konkrete tilfælde foreligger sådanne vægtige samfundsmæssige interesser. Tilsynet pegede imidlertid på, at offentliggørelse af oplysninger om strafbare forhold på internettet er den mest vidtgående form for videregivelse af oplysninger. Erfaringsmæssigt er oplysninger på internettet meget vanskelige at berigtige eller slette effektivt på grund af søgemaskiner mv.

3. Herudover må forholdet til databeskyttelsesdirektivet indgå i vurderingen af, om persondataloven kan fraviges.

I lovforslagets afsnit 10 om forholdet til EU-retten var anført, at den foreslåede offentliggørelses hjemmel i § 28 a betegner en fravigelse af de processuelle bestemmelser i artikel 8, stk. 5, i Europa-Parlamentets 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 (databeskyttelsesdirektivet). Art. 8, stk. 5 fastsætter således, at behandling af oplysninger om lovovertrædelser, straffedomme og sikkerhedsforanstaltninger som udgangspunkt kun må foretages under kontrol af en offentlig myndighed, eller hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning. Ved en offentliggørelse af oplysninger om strafbare forhold på internettet, som tredjemand derefter vil kunne (videre)behandle, opstår spørgsmålet om, hvordan art. 8, stk. 5, da kan opfyldes.

At behandling af oplysninger om strafbare forhold efter omstændighederne kan finde sted, også uden at det sker under direkte kontrol af en offentlig myndighed, fremgår således implicit af direktivets art. 8, stk. 5, men forudsætter, at der i den nationale lovgivning i øvrigt gælder tilstrækkelige, specifikke garantier for behandlingen af oplysningerne. Persondataloven gælder for tredjemands behandling af enhver af de gødningsregnskabsoplysninger, som Fødevarerministeriet offentliggør. Journalistisk behandling af oplysningerne er underkastet særlige regelsæt, herunder medieansvarsloven og lov om massemediers informationsdatabaser. Endvidere indeholder retsplejeloven særlige regler for pressens adgang til oplysninger om verserende straffesager. Herudover var det anført, at det i lovforslaget som specifik national garanti for offentliggørelse af strafbare forhold sanktioneret ved vedtagne administrative bøder var foreslået, at jordbrugsvirksomheder i forbindelse med et administrativt bødeforelæg tydeligt og skriftligt oplyses om, at oplysningerne i gødningsregnskabet og oplysningerne om den administrative bøde, vil blive offentliggjort på internettet ved vedtagelse af bøden.

Datatilsynet bemærkede i den forbindelse, at en række modtagere af oplysningerne vil være undtaget fra persondatalovens regler. Konsekvensen heraf vil være, at behandlingen hos disse modtagere som udgangspunkt ikke vil være underlagt nogen form for tilsyn. Dette forhold kan næppe karakteriseres som en

garanti i forhold til databeskyttelsesdirektivet. Det bemærkes herved, at direktivets krav om tilstrækkelige, specifikke garantier må forudsættes opfyldt i forhold til offentliggørelsesordningen som helhed.

Herudover bemærkede Datatilsynet, at tilsynet fandt, at henvisningen til retsplejeloven er uhensigtsmæssig og bør udgå. Datatilsynet henviste herved til, at der efter retsplejeloven er tale om aktindsigt i modsætning til en offentliggørelsesordning som i det foreliggende lovforslag. Herudover gælder der efter retsplejeloven regler, der begrænser modtagerens anvendelse af oplysninger i domme og kendelser i straffesager.<sup>17</sup>

Datatilsynet havde i øvrigt noteret sig det af Ministeriet for Fødevarer, Landbrug og Fiskeri anførte, hvorefter jordbrugsvirksomhederne i forbindelse med et administrativt bødeforelæg tydeligt og skriftligt vil blive oplyst om, at oplysningerne i gødningsregnskabet og oplysningerne om den administrative bøde, vil blive offentliggjort på internettet ved vedtagelse af bøden.

Samlet set fandt Datatilsynet herefter ikke at have grundlag for antage, at den påtænkte ordning vil være i strid med databeskyttelsesdirektivet.

Datatilsynet foreslog imidlertid, at udtrykket ”processuel” udgik af beskrivelsen af bestemmelsen i direktivets artikel 8, stk. 5.

4. I sit første høringssvar havde Datatilsynet desuden rejst problemstillingen angående hjemlen til modtagernes behandling af de oplysninger, der offentliggøres.

Hvis der ikke i et eventuelt lovforslag fastsættes regler for, hvilken hjemmel modtagerne af oplysninger har til at behandle oplysningerne, vil persondatalovens regler finder anvendelse på modtagerens behandling af oplysninger.

Datatilsynet understregede, at dette spørgsmål selvsagt kun er aktuelt inden for persondatalovens anvendelsesområde.

Problemet består i, at enhver behandling hos modtagerne, dvs. også indsamling, lagring/opbevaring og anden behandling, kun lovligt kan ske, hvis persondatalovens regler er opfyldt.

For strafbare forhold er persondatalovens regler restriktive, og private vil som udgangspunkt kun kunne behandle oplysninger af denne karakter med samtykke, ligesom der gælder krav om tilladelse fra Datatilsynet.

---

<sup>17</sup> I henhold til retsplejelovens § 1017 d, stk. 1, må domme og kendelser i straffesager kun gengives offentligt, når de er anonymiseret, således at sigtedes, tiltaltes, forurettedes eller vidners identitet ikke fremgår. Overtrædelse straffes med bøde.

Datatilsynet bemærkede i den forbindelse, at det formentlig ikke vil forekomme modtagerne særligt indlysende, at oplysningerne videregives fra myndighederne, men ikke uden videre kan opbevares lovligt hos modtagerne.

Samtidig understregede Datatilsynet, at tilsynet ikke har ressourcer til at føre særskilt tilsyn med dette område.

## **Lov om ændring af lov om omsætning af fast ejendom m.fl.**

Erhvervs- og Selskabsstyrelsen anmodede om Datatilsynets bemærkninger til udkast til forslag til lov om ændring af lov om omsætning af fast ejendom, lov om leje af erhvervslokaler mv. og lov om leje.

Lovforslaget indebar bl.a. oprettelse af et disciplinærnævn for ejendomsmæglere, hvis afgørelser ifølge forslaget vil blive offentliggjort.

Tilsynets udtalelse gengives i alt væsentligt nedenfor.

### **1. Oplysninger om afgivne bud**

Det fulgte af lovforslagets § 1, nr. 2, at økonomi- og erhvervsministeren bemyndiges til at fastsætte nærmere regler for licitationssalg ved udbud af fast ejendom, herunder om ret til oplysning om afgivne bud.

Det var i de specielle bemærkninger til lovforslaget anført, at der ved fastlæggelsen af reglerne bl.a. skal tages højde for ”behovet for at beskytte budgivers identitet”.

Det stod ikke Datatilsynet klart, hvilke oplysninger der i givet fald vil blive videregivet om budgiver, men Datatilsynet gik ud fra, at i det omfang der er tale om videregivelse af oplysninger omfattet af persondataloven, vil videregivelsen skulle ske inden for rammerne af persondataloven, herunder behandlingsreglerne i kapitel 4.

### **2. Offentliggørelse af disciplinærnævnets afgørelser**

Med lovforslagets § 1, nr. 14, foresloges kapitel 4 a om ”Disciplinærnævn for ejendomsmæglere” indsat i lov om omsætning af fast ejendom. Nævnet oprettes af Erhvervs- og Selskabsstyrelsen som et uafhængigt organ, der er en del af den offentlige forvaltning, og skal behandle klager over, at en ejendomsmægler har tilsidesat de pligter, som følger af lov om omsætning af fast ejendom. Nævnet kan træffe afgørelser om at tildele advarsler eller pålægge bøder. Nævnet kan endvidere træffe afgørelse om at begrænse en ejendomsmæglers adgang til at udøve ejendomsformidling eller om at slette den pågældende fra registeret over ejendomsmæglere (rettighedsfrakendelse). Nævnet vil alene kunne pålægge disciplinært ansvar, mens strafferetligt ansvar og erstatningsansvar behandles

for domstolene. Forslaget om oprettelse af nævnet var ifølge de specielle bemærkninger inspireret af den tilsvarende disciplinærordning for revisorer.

Det fremgik af den foreslåede § 29 a, stk. 6, at disciplinærnævnet skal offentliggøre sine afgørelser.

I de specielle bemærkninger til 29 a, stk. 6, var det anført, at der i forbindelse med Erhvervs- og Selskabsstyrelsens udarbejdelse af forretningsorden for disciplinærnævnet vil blive fastsat nærmere regler om offentliggørelse af afgørelser, herunder oplysninger om mæglerens eller mæglervirksomhedens navn.

En sådan offentliggørelse kendes fra Disciplinærnævnet for Revisorer, som offentliggør sine afgørelser under angivelse af navnene på de revisorer eller revisionsvirksomheder, som sagerne omhandler, og fra Klagenævnet for Ejendomsformidling, som offentliggør sine afgørelser under angivelse af de omhandlede mægleres navne.

Erhvervs- og Selskabsstyrelsen havde vurderet, at de hensyn, der begrundet offentliggørelsesordningen, herunder hensynet til forbrugeroplysning samt sikring af lige konkurrencevilkår, er tilstrækkeligt vægtige til, at der på internettet bør være adgang til at offentliggøre navne på ejendomsmæglere, der har fået tildelt en advarsel eller bøde eller har fået begrænset eller frataget retten til at udøve ejendomsformidlingsvirksomhed.

Formålet med offentliggørelsen er bl.a. at sikre, at forbrugere og virksomheder får en reel mulighed for i forbindelse med valg af ejendomsmæglere at undlade at benytte mæglere, der har handlet i strid med reglerne i lov om omsætning af fast ejendom og/eller i strid med god ejendomsmægleretik. Denne mulighed afskæres, hvis det ikke er muligt ud fra offentliggørelsen at identificere den mægler eller mæglervirksomhed, der pålægges en sanktion af disciplinærnævnet, og en anonymisering inden offentliggørelse ville derfor være ensbetydende med, at selve formålet med offentliggørelsen forspildes.

2.1. Det var Datatilsynets opfattelse, at offentliggørelse via internettet af oplysninger om ejendomsmæglere vil være omfattet af persondatalovens anvendelsesområde. Endvidere vil offentliggørelse af oplysninger om ejendomsmæglervirksomheder være omfattet, i det omfang oplysningerne kan henføres til fysiske personer. Oplysninger om enkeltmandsejede virksomheder og visse interessentskaber er således omfattet af persondataloven.

Det var i den forbindelse Datatilsynets opfattelse, at disciplinærnævnet vil være dataansvarlig for behandlingen af oplysninger i forbindelse med nævnets offentliggørelse af sine afgørelser, jf. persondatalovens § 3, nr. 4, om, at den dataansvarlige er den fysiske eller juridiske person, offentlige myndighed,

institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.

2.2. Overtrædelse af en række bestemmelser i lov om omsætning af fast ejendom er strafsanktioneret, jf. lovforslagets § 1, nr. 15.

Behandlingen af personoplysninger i forbindelse med offentliggørelse af disciplinærnævnets afgørelser ville derfor efter Datatilsynets opfattelse i nogle tilfælde kunne være omfattet af persondatalovens § 8 om behandling af oplysninger om strafbare forhold.

Efter persondatalovens § 8, stk. 2, må oplysninger om strafbare forhold som udgangspunkt ikke videregives. Videregivelse kan dog ske, når visse nærmere opregnede betingelser er opfyldt. Det var Datatilsynets umiddelbare vurdering, at disse betingelser ikke i alle tilfælde kan antages at være opfyldt i forbindelse den foreslåede § 29 a, stk. 6, om offentliggørelse af oplysninger om navngivne personer, som har overtrådt lovgivningen.

2.3. Persondataloven indeholder i § 9 særregler for eksterne retsinformationssystemer. Det følger således af lovens § 9, stk. 1, at oplysninger som nævnt i lovens § 7, stk. 1, eller § 8 må behandles, hvis dette sker med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning. Bestemmelsen anvendes i praksis bl.a. i forhold til myndigheders offentliggørelse af afgørelser på deres hjemmesider.

Det følger af persondatalovens § 9, stk. 3, at tilsynsmyndigheden (Datatilsynet) kan meddele nærmere vilkår for de i bestemmelsens stk. 1 nævnte behandlinger af oplysninger. Tilsvarende gælder for de i lovens § 6 nævnte oplysninger, som alene behandles i forbindelse med førelsen af retsinformationssystemer.

På Datatilsynets hjemmeside findes tilsynets standardvilkår for offentliggørelse af afgørelser.

Af Datatilsynets standardvilkår 1 fremgår bl.a., at i afgørelser, som indeholder fortrolige oplysninger eller oplysninger om enkeltpersoners rent private forhold, skal de pågældende oplysninger anonymiseres i overensstemmelse med vilkår 2, jf. dog vilkår 3, før videregivelse må finde sted.

Det følger af vilkår 2, at en eventuel anonymisering består i udeladelse af personnavne, præcise adresseangivelser og eventuelle andre identifikationsoplysninger vedrørende personer. I stedet for de udeladte oplysninger kan indsættes neutrale betegnelser. Personnumres løbenumre udelades.

2.4. Forholdet til persondataloven sås ikke omtalt i bemærkningerne til den foreslåede § 29, stk. 6.

Datatilsynet anbefalede derfor, at Erhvervs- og Selskabsstyrelsen i lovbemærkningerne præciserede, hvorvidt det med bestemmelsen er tilsigtet, at offentliggørelse af disciplinærnævnets afgørelser kan ske, uanset at videregivelsen af de pågældende oplysninger ikke i alle omstændigheder kan ske inden for rammerne af persondatalovens §§ 8 og 9 samt de standardvilkår, som Datatilsynet har fastsat i medfør af lovens § 9, stk. 3.

I givet fald gik Datatilsynet ud fra, at der alene bliver tale om at fravige Datatilsynets vilkår om anonymisering i relation til de pågældende ejendomsmæglere, hvilket eventuelt kan præciseres i forslaget.

Datatilsynet gik endvidere ud fra, at forslaget vil kunne forenes med tilsynets standardvilkår om, at hvis en afgørelse har været behandlet af en højere instans, skal dette samt udfaldet heraf fremgå af gengivelsen af sagen. Ligeledes gik tilsynet ud fra, at tilsynets vilkår om, at det skal kontrolleres, at der ikke er fejl i gengivelse af afgørelserne, og at fejl og lignende skal rettes eller slettes, vil kunne fastsættes uanset det foreliggende lovforslag.

2.5. Persondataloven kan fraviges ved særlovgivning, hvis denne ikke strider mod databeskyttelsesdirektivet. Datatilsynet henlede i den forbindelse særligt opmærksomheden på databeskyttelsesdirektivets artikel 8, stk. 5-6.

Det er Datatilsynets opfattelse, at en særskilt hjemmel til registrering og videregivelse af oplysninger i videre omfang end det, der følger af persondataloven, kun bør tilvejebringes, hvis vægtige samfundsmæssige hensyn taler herfor. Hvorvidt dette var tilfældet, fandt Datatilsynet ikke at burde udtale sig om.

2.7. Offentliggørelse af navnene på de ejendomsmæglere og ejendomsmæglervirksomheder, der har overtrådt lovgivningen, vil kunne ske i medfør af lovforslagets § 1, nr. 14. Derimod var der ikke i forslaget fastsat regler for, hvilken hjemmel modtagerne har til at behandle oplysningerne.

I den forbindelse bemærkede Datatilsynet, at persondatalovens regler i nogle tilfælde vil finde anvendelse på modtagernes behandling af oplysninger, hvorefter modtagerne kan behandle oplysningerne, i det omfang det er i overensstemmelse med lovens regler. Hertil bemærkede Datatilsynet, at tilsynet ikke har ressourcer til at føre særskilt tilsyn med dette område.

2.8. Datatilsynet henlede i øvrigt Erhvervs- og Selskabsstyrelsens opmærksomhed på persondatalovens § 5, stk. 4, og § 37.

Datatilsynet forudsatte, at persondatalovens § 5, stk. 4, og § 37 vil blive efterlevet i forbindelse med de af lovforslaget omfattede behandlinger. Dette indebærer efter tilsynets opfattelse bl.a., at den dataansvarlige (disciplinærnævnet) bør være behjælpelig, hvis der skulle opstå en situation, hvor en ejendomsmægler eller en ejendomsmæglervirksomhed er registreret med ukorrekte eller vildledende oplysninger i en søgemaskine eller lignende.

2.9. Det fremgik ikke af lovforslaget, hvor længe disciplinærnævnets afgørelser skal være offentligtgjort.

Datatilsynet forudsatte, at den periode, hvor oplysningerne skal være offentliggjort, vil blive fastsat i overensstemmelse med persondatalovens § 5, stk. 5.

### 3. Offentliggørelse af navne mv. på bygningssagkyndige

Det foresloges med lovforslagets § 4 om ændring af lov om forbrugerbeskyttelse ved erhvervelse af fast ejendom, at økonomi- og erhvervsministeren bemyndiges til at fastsætte regler om tildeling af påtaler, advarsler eller inddragelse af godkendelsen som bygningssagkyndig, herunder om offentliggørelse af navne på og firmatilknytningsforhold for bygningssagkyndige, der har fået tildelt advarsler eller fået beskikkelsen inddraget. Det er en betingelse for tildeling af advarsel og inddragelse af beskikkelse, at der foreligger alvorlige eller gentagne fejl i den pågældendes tilstandsrapporter.

Formålet med bemyndigelsesbestemmelsen var, under hensyn til en hushandels store betydning for den enkelte, at styrke forbrugeroplysningen og at forbedre tilstandsrapporternes kvalitet og sikre lige konkurrencevilkår.

Offentliggørelse kan tidligst ske 4 uger efter tildelingen af advarslen/inddragelsen af beskikkelsen, medmindre afgørelsen indbringes for domstolene, hvor offentliggørelse først kan ske, når endelig dom foreligger. Sletning vil ske efter højst 3 år.

Det var Datatilsynets opfattelse, at en oplysning om, at en byggesagkyndig har fået tildelt en advarsel, en påtale eller har fået sin beskikkelse inddraget kan være af fortrolig karakter. Sådanne oplysninger vil som udgangspunkt ikke umiddelbart kunne offentliggøres inden for persondatalovens rammer.

Såfremt der er tale om offentliggørelse af oplysninger om overtrædelse af strafsanktioneret lovgivning, kan behandlingen af oplysningerne endvidere være omfattet af persondatalovens § 8.

Datatilsynet henviste i den forbindelse til det ovenfor under punkt 2. anførte.

# Internationalt arbejde

**Indledning** Som beskrevet i tidligere årsberetninger, senest i Datatilsynets Årsberetning for 2004, 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 OECD’s internationalt dækkende Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, som indeholder en række hovedprincipper for persondatabeskyttelse, og som har størst betydning for de lande, der ikke har ratificeret Europarådskonventionen.

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

Både FN’s Menneskerettighedskonvention og Den Europæiske Menneskerettighedskonvention indeholder bestemmelser, der omhandler respekten for privatlivets fred.

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

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

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende.
2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og

på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører ham/hende, og til berigtigelse heraf.

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

En engelsk oversættelse af lov om behandling af personoplysninger er tilgængelig på Datatilsynets hjemmeside [www.datatilsynet.dk](http://www.datatilsynet.dk).

Nedenfor gives en kort beskrivelse af det formelle grundlag for tilsynets aktiviteter på det internationale område suppleret med oplysninger om de væsentligste sager, som tilsynet har beskæftiget sig med i 2005. Desuden omtales også det mere uformelle, internationale samarbejde, som har udviklet sig gennem årene.

**Europarådet** Konventionens navn: Den europæiske konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (COE 180).

Ikrafttræden: Den 1. februar 1990 i Danmark.

Efter sammenlægningen i 2003 af Den Rådgivende Komité T-PD (Consultative Committee T-PD) og Databeskyttelsesekspertgruppen (CJ-PD) på grund af manglende økonomiske ressourcer har T-PD også i 2005 fortsat CJ-PD's arbejde med behandling af personoplysninger ved brug af biometriske data. T-PD's drøftelser er beskrevet i en statusrapport (progress report), som kan ses på Europarådets hjemmeside. T-PD fortsatte endvidere drøftelserne om "Application of Data Protection Principles to the Internet". Drøftelserne skal danne grundlag for T-PD's fremtidige arbejde i relation til behandling af personoplysninger på internet.

T-PD vedtog i 2000 et forslag til tillægsprotokoltekst til konventionen, som vedrører oprettelse af databeskyttelsesmyndigheder og forholdet til tredjelande. Tillægsprotokollen blev i 2001 vedtaget af Ministerkomitéen og efterfølgende fremlagt til underskrivelse. I slutningen af 2005 har 29 lande underskrevet tillægsprotokollen, heraf har 12 lande ratificeret protokollen.

Europarådets hjemmeside kan findes via et link fra Datatilsynets hjemmeside.

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

Ikrafttræden: I Danmark blev gennemførelsen af konventionen vedtaget ved lov nr. 415 af 10. juni 1997. Ifølge lovens § 6 fastsætter justitsministeren tidspunktet

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

**Formål:** Gennem oprettelse af en europæisk politienhed med en national enhed i hver EU-medlemsstat at forbedre effektiviteten hos medlemsstaternes kompetente myndigheder og disses samarbejde om forebyggelse og bekæmpelse af bl.a. terrorisme, ulovlig narkotikahandel og andre former for grov international kriminalitet.

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

Den Fælles Kontrolinstans har i 2005 afholdt 4 møder, hvor man bl.a. har behandlet spørgsmål, som vedrører Europol's adgang til Schengen-informationssystemet, indgåelse af aftaler om videregivelse af personoplysninger mellem Europol og Canada samt Australien og opbygning af et nyt Europol indekssystem. Den Fælles Kontrolinstans udtalelser kan findes på kontrolinstansens hjemmeside <http://europoljsb.ue.eu.int/>.

Det Fælles Klageudvalg har i 2005 afholdt 4 møder. Klageudvalget afgjorde bl.a. i december 2005 to klagesager vedrørende begæringer om indsigt hos Europol. Afgørelserne kan findes på Den Fælles Kontrolinstans' hjemmeside.

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 Rigspolitiets regi.

### ***Schengen-konventionen (Schengen-samarbejdet)***

Konventionens navn: Konvention om gennemførelse af Schengen-aftalen af 14. juni 1985 mellem regeringerne for staterne i Den Økonomiske Union Benelux, Forbundsrepublikken Tyskland og Den Franske Republik om gradvis ophævelse af kontrollen med de fælles grænser (Schengen-konventionen).

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

Ikrafttræden: Folketinget bemyndigede ved lov nr. 418 af 10. juni 1997 om Danmarks tiltrædelse af Schengen-konventionen regeringen til at ratificere tiltrædelsesaftalen på Danmarks vegne, og ratifikationen fandt sted den 23. september 1997. Loven blev delvis sat i kraft (§ 1, jf. § 4, stk. 1), men således at Justitsministeriet blev bemyndiget til at fastsætte ikrafttrædelsestidspunktet for lovens øvrige bestemmelser. I medfør af lovens § 4, stk. 2, traf justitsministeren ved bekendtgørelse nr. 1366 af 20. december 2000 bestemmelse om, at lovens regler om Schengen-informationssystemet trådte i kraft den 1. januar 2001, og at lovens øvrige bestemmelser trådte i kraft den 25. marts 2001. Loven er senere ændret ved lov nr. 227 af 2. april 2003 og lov nr. 448 af 9. juni 2004.

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

Den Fælles Tilsynsmyndighed har i 2005 afholdt 5 møder. Tilsynsmyndigheden har bl.a. i samarbejde med de databeskyttelsesmyndigheder i EU-landene, som deltager i Schengen-informations-systemet (SIS), herunder Norge og Island, foretaget en fælles undersøgelse af landenes brug af SIS-systemet vedrørende indberetning af uønskede udlændinge, jf. Schengen-konventionens artikel 96. Undersøgelsen er nærmere omtalt i afsnittet om væsentlige aktiviteter i 2005.

Tilsynsmyndigheden har endvidere fortsat drøftelserne af et kommende SIS II system, herunder myndighedens fremtidige arbejde set i lyset heraf. Den Fælles Tilsynsmyndigheds udtalelser kan findes på tilsynsmyndighedens hjemmeside, <http://www.schengen-ja.dataprotection.org>. Tilsynsmyndighedens hjemmeside er endnu ikke tilgængelig på dansk.

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

### ***Toldinformations-systemet***

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

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

Ikrafttræden: Konventionen blev undertegnet den 26. juli 1995, og Danmark ratificerede konventionen 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.

I henhold til konventionens artikel 18 er der nedsat en fælles tilsynsmyndighed bestående af 2 repræsentanter fra hver af medlemsstaterne, udpeget blandt medlemsstaternes uafhængige tilsynsmyndigheder. Denne myndighed fører tilsyn med en central database, som er oprettet i EU-regi i Bruxelles, med terminaladgang for samtlige medlemsstaters myndigheder.

I 2005 blev der afholdt 1 møde i Den Fælles Tilsynsmyndighed, hvor man bl.a. drøftede CIS-toldinformationssystemet og en fremtidig udvikling af dette.

CIS-toldinformationssystemet skal udgøre en del af en fælles edb-database, hvori der også indgår oplysninger, som er omfattet af Rådets Forordning (EF) nr. 515/97 af 13. marts 1997 om gensidig bistand mellem medlemsstaternes administrative myndigheder og om samarbejde mellem disse og Kommissionen med henblik på at sikre den rette anvendelse af told- og landbrugsbestemmelserne. Tilsynet med den forordningsregulerede del af systemet (søjle I) føres af den uafhængige kontrolinstans, der er omhandlet i EU-traktatens artikel 286.

### ***Sekretariatet for de fælles tilsynsmyndigheder***

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

grænser (Schengen-konventionen), se EF-Tidende 2000, nr. L 271 af 24. oktober 2000, s. 1-3.

Det er udtrykkeligt fastslået, at databeskyttelsessekretariatet skal være uafhængigt, idet det ved udførelsen af sine opgaver kun er bundet af instrukser fra de fælles tilsynsmyndigheder. Af praktiske grunde er databeskyttelsessekretariatets administration dog tæt knyttet til Generalsekretariatet for Rådet. I overensstemmelse med Rådets afgørelse begyndte sekretariatet sit virke i september 2001. Sekretariatet ledes af en jurist med stor erfaring inden for databeskyttelse.

### ***Napoli II-konventionen***

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

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

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

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

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

### ***Eurodac-systemet***

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

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

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

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

Det følger af Eurodac-forordningens artikel 19, stk. 1, at hver medlemsstat drager omsorg for, at den eller de nationale tilsynsmyndigheder, der udpeges i henhold til artikel 28, stk. 1, i direktiv 95/46/EF, i fuld uafhængighed og i overensstemmelse med den pågældende medlemsstats nationale ret overvåger, at den pågældende medlemsstats behandling af personoplysninger i overensstemmelse med Eurodac-forordningen, herunder videregivelsen af oplysninger til den centrale enhed, foregår på lovlig vis.

Folketinget har i 2005 vedtaget ændringer i udlændingeloven, så Danmark på mellemstatsligt grundlag kan tilknytte sig Eurodac-forordningen om oprettelse af et fælles europæisk fingeraftrykssystem og Dublin-forordningen om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en asylansøgning, der er indgivet i en medlemsstat.

Af lov om ændring af udlændingeloven (Tilknytning til Eurodac-forordningen og Dublin-forordningen på mellemstatsligt grundlag m.v.) § 58 i, stk. 6, fremgår, at Datatilsynet her i landet fører tilsyn med behandlingen og anvendelsen af de oplysninger, der er videregivet og modtaget efter reglerne i Eurodac-forordningen. Loven trådte i kraft den 1. april 2006, jf. bekendtgørelse nr. 235 af 17. marts 2006

Den 28. september 2005 deltog Datatilsynet som observatør i et møde om Eurodac-systemet i EDPS – European Data Protection Supervisor. Baggrunden for mødet var dels et ønske om at oplyse generelt om opbygningen af den centrale enhed af Eurodac og dels et ønske om koordinering af de nationale tilsynsmyndigheders håndtering af deres tilsynsforpligtelse i forhold til Eurodac.

### ***Det generelle databeskyttelsesdirektiv***

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

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

Artikel 29-gruppen har i 2005 afholdt 5 to dages-møder og 1 endagsmøde. Datatilsynet har endvidere deltaget i en underarbejdsgruppe ”Internet Task Force”, som særligt arbejder med beskyttelse af personoplysninger i forbindelse med anvendelse af internet og anden ny teknologi.

Artikel 29-gruppen har i 2005 vedtaget en række henstillinger, udtalelser mv.

Der er således vedtaget dokumenter om følgende:

- Udtalelse nr. 1/2005 om tilstrækkeligheden af beskyttelsesniveauet sikret i Canada for overførslen af Passenger Name Records (PNR) og Advance Passenger Information fra flyselskaber (WP 103)
- Arbejdsdokument vedrørende beskyttelse af personoplysninger i forbindelse med beskyttelsen af immaterielle rettigheder (WP 104)
- Arbejdsdokument vedrørende beskyttelse af personoplysninger i forbindelse med anvendelse af RFID teknologi (WP 105)
- Rapport om pligten til at foretage anmeldelse til de nationale tilsynsmyndigheder, den bedste anvendelse af undtagelserne og simplificering og databeskyttelsesofficerers rolle i EU (WP 106)

- Arbejdsdokument om etableringen af en samarbejdsprocedure for udtalelser om tilstrækkelige garantier som følge af ”Binding Corporate Rules” (BCR) (WP 107)
- Arbejdsdokument om etableringen af checkliste for godkendelsen af ”Binding Corporate Rules” (BCR) (WP 108)
- Artikel 29-gruppens arbejdsprogram for 2005 (WP 109)
- Udtalelse nr. 2/2005 om forslag til Europa Parlamentet og Rådets forordning vedrørende Visuminformationssystemet (VIS) og udvekslingen af oplysninger mellem medlemsstater om kortopholdsvisum (WP 110)
- Resultater af den offentlige høring af artikel 29-gruppens arbejdsdokument vedrørende beskyttelse af personoplysninger i forbindelse med anvendelse af RFID teknologi (WP 111)
- Udtalelse nr. 3/2005 om implementering af Rådets forordning nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedsforanstaltninger og biometri i pas og rejsedokumenter udstedt af medlemslande (WP 112)
- Udtalelse nr. 4/2005 om forslag til Europa Parlamentet og Rådets direktiv om logning af data behandlet i forbindelse med den elektroniske kommunikationssektor samt ændring af direktiv 2002/58/EC (WP 113)
- Arbejdsdokument om en fælles fortolkning af artikel 26, stk. 1, i direktiv 95/46/EC af 24. oktober 1995 (WP 114)
- Udtalelse nr. 5/2005 om brug af lokaliseringsdata med henblik på levering af ekstra-tjenester (WP 115)
- Udtalelse nr. 6/2005 om forslag til Europa Parlamentet og Rådets forordning (COM (2005) 236 final) og Rådets beslutning (COM (2005) 230 final) om etablering, drift og brug af 2. generation af Schengen Informationssystemet (SIS II) og et forslag til Europa Parlamentet og Rådets forordning vedrørende adgang til 2. generation af Schengen Informationssystemet (SIS II) for de nationale enheder ansvarlige for udstedelse af registreringsbeviser for motor-køretøjer (COM (2005) 237 final) (WP 116)

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

### ***Databeskyttelse internt i EU-/EF-institutionerne***

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

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

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

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

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

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

### ***Eurojust***

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

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

Formål: Eurojust har til opgave at lette den egentlige koordinering mellem medlemslandenes retsforfølgende myndigheder og støtte efterforskningen i kriminalsager vedrørende organiseret kriminalitet, især med udgangspunkt i Europols analyser. Eurojust skal endvidere arbejde tæt sammen med det Europæiske Retlige Netværk vedrørende forenkling og efterkommelse af retsanmodninger.

Arbejdsopgaver: I henhold til Eurojust-afgørelsens artikel 23 oprettes der en fælles kontrolinstans til overvågning af Eurojusts aktiviteter med henblik på at sikre, at disse aktiviteter finder sted i overensstemmelse med Eurojust-afgørelsens bestemmelser vedrørende datasikkerhed. Forretningsordenen for den fælles kontrol instans blev vedtaget i 2004, og instansen har efterfølgende løbende afholdt møder.

Datatilsynet er repræsenteret i den fælles kontrolinstans.

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

#### ***EU-datatilsynets arbejde***

Alle EU's medlemsstater har nu lovgivning om persondatabeskyttelse.

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

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

I 2005 blev den årlige EU-datatilsynskonference afholdt i Krakow af det polske datatilsyn (Generalny Inspektor Ochrony Danych Osobowych). På konferencen drøftedes en række spørgsmål af fælles interesse, bl.a. udveksling af oplysninger mellem retshåndhævelsesmyndighederne i medlemslandene og problemstillinger vedrørende databeskyttelse på tredje søjle.

### **International Konference for databeskyttelsesmyndigheder mv.**

Det 27. årlige internationale møde for datatilsynsmyndighederne blev i september 2005 afholdt i Montreux, Schweiz, arrangeret af det schweiziske datatilsyn. På konferencen blev der behandlet en række emner af fælles interesse, herunder bl.a. en harmonisering af databeskyttelsesprincipper og brug af biometri i pas, identitetskort og rejsedokumenter.

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

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

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

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

### **Nordisk Samarbejde**

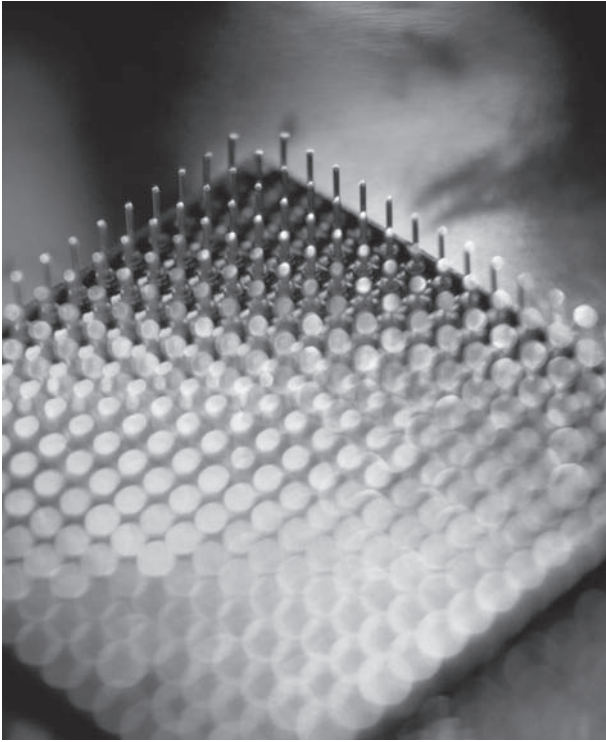
Det nordiske samarbejde mellem datatilsynsmyndighederne i Danmark, Finland, Island, Norge og Sverige er blevet fortsat. I 2005 stod det danske datatilsyn for afholdelse af det fællesnordiske sagsbehandlermøde, hvor også det færøske datatilsyn deltog.

På mødet udvekslede deltagerne oplysninger om såvel generelle som konkrete spørgsmål. Bl.a. diskuterede deltagerne spørgsmål i tilknytning til offentliggørelse af personoplysninger på internet, tilsynsmyndighedernes rolle i forhold til spam, udstrækningen af oplysningspligten, indsigt i logregistre og forskellige former for overvågning og kontrol.

I 2005 blev der afholdt Nordisk Teknikermøde i Stockholm og Nordisk Datachefmøde i Norge. I Stockholm blev bl.a. spørgsmålene om anvendelse af biometri i pas og ID-kort, digital forvaltning, fremgangsmåden ved inspektioner, anvendelse af cookies m.m. diskuteret, mens der på det Nordiske Datachefmøde bl.a.

blev drøftet tv-overvågning, anonym færdsel, anvendelse af biometri, behandling af oplysninger i sundhedssektoren, personoplysninger på internet og datasikkerhed.

Det er besluttet, at Nordisk Datachefmøde fremover afholdes hvert andet år.



# Sikkerhedsspørgsmål

## **Persondata- lovens krav om datasikkerhed**

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

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

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

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

## **Bibliotekssagen**

*Udtalt, at Datatilsynet undtagelsesvist kunne acceptere, at Biblioteksstyrelsen og bibliotekerne foreløbig i en periode på 5 år fortsætter med at sende elektroniske reserverings- og kvitteringsmeddelelser, der indeholder titel og forfatter på det reserverede materiale, i ikke-krypteret form til de brugere, der ønsker at benytte elektronisk kommunikation med biblioteksvæsenet (Datatilsynets j.nr. 2004-082-0188)*

Biblioteksstyrelsen anmodede Datatilsynet om en udtalelse angående fremsendelse af e-post-kvittering ved bestilling af materiale via [www.bibliotek.dk](http://www.bibliotek.dk).

Det fremgik af henvendelsen, at en bruger ved bestilling af materiale via [www.bibliotek.dk](http://www.bibliotek.dk) kan vælge at bestille en kvittering i form af en e-post-kvittering eller opsætte brugeropsætningen således, at brugeren altid får tilsendt en e-post-kvittering. E-post-kvitteringen indeholder den oplyste låneridentifikation i form af navn og e-postadresse. Derudover indeholder e-posten titlen på det bestilte materiale.

Datatilsynet udtalte bl.a., at en personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person. Et navn eller en postadresse er selvsagt personhenførbare oplysninger, men også en e-post-adresse eller en IP-adresse er personhenførbare oplysninger. En e-post-meddelelse behøver således ikke indeholde modtagerens navn eller postadresse for at være personhenførbare i persondatalovens forstand.

Persondataloven skelner mellem såkaldte almindelige ikke-følsomme oplysninger (§ 6), følsomme oplysninger (§ 7) og oplysninger om andre rent private forhold (§ 8). Denne opdeling har bl.a. betydning i forhold til, hvilke krav der stilles til en sikker behandling af oplysningerne.

Af persondatalovens § 41, stk. 3, fremgår, at der skal træffes 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. Denne pligt påhviler såvel den dataansvarlige som en eventuel databehandler.

For transmission af personoplysninger over internettet er der generelt en risiko for, at oplysningerne undervejs læses og endog ændres af uvedkommende. Disse risici må vurderes af den dataansvarlige i den konkrete situation, således at der kan træffes de fornødne sikkerhedsforanstaltninger, jf. § 41, stk. 3. Efter Datatilsynets opfattelse bør der ved transmission af fortrolige oplysninger, herunder personnummer, som minimum foretages kryptering. Hvis de transmitterede oplysninger er af følsom karakter (omfattet af persondatalovens § 7, stk. 1, og § 8, stk. 1) skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.

Pligten til at træffe sikkerhedsforanstaltninger efter persondataloven er ufravigelig og bortfalder således ikke, selv om den, som oplysningerne vedrører, giver sit samtykke til det.

Oplysning om, hvilke bøger en person låner på biblioteket, er en såkaldt almindelig, ikke-følsom oplysning. Det må dog lægges til grund, at der er tale om en fortrolig oplysning, jf. undtagelsesbekendtgørelsens<sup>18</sup> § 12, jf. persondatalovens § 44.

En e-post-kvitteringsmeddelelse er omfattet af persondatalovens anvendelsesområde. Fremsendelse af sådanne elektroniske reserveringsmeddelelser, der indeholder titel og forfatter på det reserverede materiale, kræver efter Datatilsynets opfattelse kryptering. Dette skyldes, at det er fortrolige oplysninger, som sendes over det åbne internet.

---

<sup>18</sup> Bekendtgørelse nr. 529 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning.

Hvis man i stedet fremsendte en reserveringsmeddelelse, der ikke indeholder oplysninger om, hvilket materiale der er reserveret, men alene indeholder oplysninger om, at det reservede materiale er klar til udlån, var det Datatilsynets umiddelbare opfattelse, at meddelelsen ikke ville indeholde fortrolige oplysninger og dermed ikke kræve kryptering.

Biblioteksstyrelsen offentliggjorde Datatilsynets svar med en nyhedstekst om, at kvitteringsmails fjernes i bibliotek.dk efter krav fra Datatilsynet, hvilket medførte en del reaktioner fra bl.a. brugere og pressen.

Biblioteksstyrelsen og Datatilsynet drøftede efterfølgende problemstillingen og mulige løsningsmodeller.

Sagen blev endvidere drøftet på et møde i Datarådet, hvorefter Datatilsynet i alt væsentligt udtalte følgende:

1. Det er Datatilsynets opfattelse, at oplysninger om, hvilke bøger en borger reserverer og låner på biblioteket, er af fortrolig karakter.

Det er endvidere Datatilsynets opfattelse, at der generelt er behov for at træffe sikkerhedsforanstaltninger, når offentlige myndigheder sender (transmitterer) oplysninger af fortrolig karakter over det åbne internet.

Tilsynet henviste herved til § 14 i Justitsministeriets bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, hvorefter der for den offentlige forvaltning kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger. De nærmere krav er omtalt i Datatilsynets sikkerhedsvejledning.

Datatilsynet henviste endvidere til foranstaltningerne i forbindelse med eDag2-projektet, hvorefter alle borgere og virksomheder skal have tilbud om at kommunikere digitalt og sikkert med offentlige myndigheder.

2. Elektronisk kvitteringsmeddelelse fra Biblioteksstyrelsens hjemmeside bibliotek.dk og elektronisk reserveringsmeddelelse fra bibliotekerne er en serviceydelse, som det er muligt at benytte sig af for brugere af biblioteker. Der er tale om en serviceydelse rettet mod en stor kreds af befolkningen, og det er indtrykket, at mange borgere i praksis benytter og sætter pris på denne service.

Det er i dag teknologisk muligt at sende og modtage krypterede e-post-meddelelser. Det må imidlertid erkendes, at afsendelse og modtagelse af krypterede e-post-meddelelser endnu ikke er særligt udbredt i befolkningen,

hvilket bl.a. kan skyldes, at de aktuelle muligheder for kryptering af mange opleves som mindre brugervenlige.

Datatilsynet fandt på den baggrund undtagelsesvist at kunne acceptere, at Biblioteksstyrelsen og bibliotekerne foreløbig i en periode på 5 år fortsætter med at sende elektroniske reserverings- og kvitteringsmeddelelser, der indeholder titel og forfatter på det reserverede materiale, i ikke-krypteret form til de brugere, der ønsker at benytte elektronisk kommunikation med biblioteksvæsenet.

Det var en forudsætning for Datatilsynets vurdering af sagen, at Biblioteksstyrelsen og bibliotekerne i denne periode arbejder på at indføre tekniske løsninger, der generelt højner sikkerhedsniveauet ved transmission af oplysningerne over internettet.

Datatilsynet oplyste, at tilsynet senere vil sætte sig i forbindelse med Biblioteksstyrelsen med henblik på at følge de foranstaltninger, der iværksættes for at højne sikkerhedsniveauet i denne sammenhæng. Tilsynet følger i øvrigt den generelle teknologiske udvikling med hensyn til sikkerhedsforanstaltninger ved transmission af personoplysninger over internettet.

Hvis der i praksis skulle vise sig konkrete uhensigtsmæssigheder ved den omhandlede løsning set i forhold til de beskyttelseshensyn persondataloven varetager, vil Datatilsynet tage sagen op til fornyet overvejelse.

### **Kommunes offentliggørelse af person- oplysninger**

*Udtalt, at en kommune, der ved en administrativ fejl havde offentliggjort fortrolige og følsomme personoplysninger på kommunens hjemmeside, ikke havde udvist den fornødne omhu, og at kommunen dermed ikke havde overholdt kravene i persondatalovens § 41, stk. 3 (Datatilsynets j.nr. 2005-632-0078)*

På baggrund af en henvendelse fra en journalist blev Datatilsynet opmærksom på, at Gladsaxe Kommune havde offentliggjort fortrolige og følsomme personoplysninger på kommunens hjemmeside.

Datatilsynet kontaktede samme dag telefonisk Gladsaxe Kommune og opfordrede til, at oplysningerne hurtigst muligt blev fjernet fra kommunens hjemmeside. Det blev aftalt, at Gladsaxe Kommune ville undersøge sagen nærmere og orientere Datatilsynet.

Gladsaxe Kommune oplyste efterfølgende bl.a., at kommunen som følge af en misforståelse ved en meget beklagelig administrativ fejl havde offentliggjort personoplysninger i strid med persondatalovens § 8. Fejlen var nu rettet, og de pågældende oplysninger var ikke længere offentligt tilgængelige. Kommunens tekniske medarbejdere ville sørge for, at oplysningerne også blev slettet fra

søgemaskiner på internettet. Gladsaxe Kommune beklagede meget det skete, og kommunen ville fremover arbejde for at undgå, at lignende fejl opstår.

Datatilsynet udtalte på den baggrund bl.a., at det følger af lovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

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

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

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

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

I det konkrete tilfælde, hvor fortrolige og følsomme personoplysninger var blevet offentliggjort, fandt Datatilsynet ikke, at Gladsaxe Kommune havde udvist den fornødne omhu, og kommunen havde dermed ikke overholdt kravene i persondatalovens § 41, stk. 3. Datatilsynet fandt det skete meget beklageligt.

Datatilsynet noterede sig, at der havde været tale om en administrativ fejl som følge af en misforståelse, og at Gladsaxe Kommune straks havde fjernet oplysningerne fra hjemmesiden og taget initiativ til at sikre, at oplysningerne blev slettet fra eventuelle søgemaskiner på internet. Kommunen havde endvidere beklaget det passerede.

Gladsaxe Kommune havde endelig oplyst, at kommunen fremover vil arbejde for at undgå lignende fejl, og Datatilsynet anmodede kommunen om at oplyse, hvilke forholdsregler kommunen ville tage for at sikre, at der ikke fremover sker uberettiget offentliggørelse af personoplysninger på kommunens hjemmeside.

Gladsaxe Kommune oplyste efterfølgende bl.a., at kommunens forvaltningschef-gruppe havde drøftet sagen, og at det var blevet understreget, at der ved den dagsordensgodkendelse, som forvaltningscheferne har ansvaret for, skal være fokus også på persondataloven, når det vurderes, om en sag og dens bilag opføres på den åbne del af dagsordenen. Forvaltningscheferne vil også sikre, at de medarbejdere, der arbejder med dagsordenstekster, bliver grundigt informeret om, hvorledes man behandler personoplysninger i relation til persondatalovens § 41, stk. 3.

Endvidere vil der ske en udbygning af kommunens udvalgssekretærvejledning, når det gælder håndtering af udvalgsdagsordenssager, som eventuelt indeholder følsomme og fortrolige personoplysninger.

Datatilsynet noterede sig, at det var kommunens vurdering, at der med disse tiltag var gjort tilstrækkeligt for at forebygge, at der sker tilsvarende fejl i fremtiden.

**Vilkår om  
sikkerhed  
ved privat  
anmeldelse**

*Under hensyn til registerets karakter og omfang fastsatte Datatilsynet vilkår om sikkerhed i forbindelse med tilladelse til Brancheorganisationen Danske Bedemænds behandling af oplysninger i "Centralregister for 'Min Sidste Vilje'" (Datatilsynets j.nr. 2005-42-0797)*

Brancheorganisationen Danske Bedemænd anmeldte behandlingen "Centralregister for 'Min Sidste Vilje'" til Datatilsynet og ansøgte om tilladelse i henhold til lovens § 50, stk. 1, nr. 1.

Det fremgik af bl.a. af anmeldelsen, at behandlingens formål er registrering af begravelsesønsker, og at de registrerede oplysninger vil kunne blive videregivet til bedemænd i Danmark.

Datatilsynets tilladelse blev givet på følgende vilkår:

1. Indsamling, registrering og anden behandling af følsomme oplysninger må alene ske med den registreredes udtrykkelige samtykke. Samtykket skal opfylde persondatalovens krav.
2. Behandlingen af personoplysninger skal ske under iagttagelse af de i bilag 1 beskrevne sikkerhedsregler.
3. De enkelte bedemænd skal informeres om, at deres opslag logges, og at loggen kan bruges til at kontrollere uberettigede opslag samt til stikprøvekontrol.

Af bilag 1 til tilladelsen fremgår:

Sikkerhedsregler for behandling af personoplysninger, der er anmeldt til Datatilsynet af en privat dataansvarlig:

I medfør af § 50, stk. 5, i lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven) fastsætter Datatilsynet i forbindelse med meddelelse af tilladelse til den anmeldte behandling nærmere vilkår for udførelsen af behandlingen til beskyttelse af de registreredes privatliv.

Den dataansvarliges behandlingssikkerhed skal leve op til kravene i persondatalovens kapitel 11. Til uddybning af disse krav har Datatilsynet stillet vilkår om, at behandlingen af personoplysninger skal ske under iagttagelse af de sikkerhedsregler, der er beskrevet i dette bilag.

Generelle sikkerhedsbestemmelser:

1. Den dataansvarlige skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i virksomheden til uddybning af de regler, der fremgår af dette bilag. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for virksomheden. De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i virksomheden.
2. Den dataansvarlige skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af punkt 1.
3. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.
4. Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.
5. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes

de fornødne foranstaltninger for at sikre, at persondatalovens § 41, stk. 3, overholdes.

Inddatamateriale som indeholder personoplysninger:

6. Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddatering. Materialet skal opbevares aflåst, når det ikke anvendes, og slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, hvortil det er indsamlet, dog senest efter en af den dataansvarlige fastsat frist. Ved tilintetgørelse skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

Uddatamateriale som indeholder personoplysninger:

7. Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages. Materialet skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt heri. Når materialet ikke længere skal anvendes til de formål, som behandlingen varetager, dog senest efter en af den dataansvarlige fastsat frist, skal det slettes eller tilintetgøres.

Autorisation og adgangskontrol:

8. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles ved hjælp af edb. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

9. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles, samt personer, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

10. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i punkt 8 og 9. Kontrol heraf skal foretages mindst en gang hvert halve år.

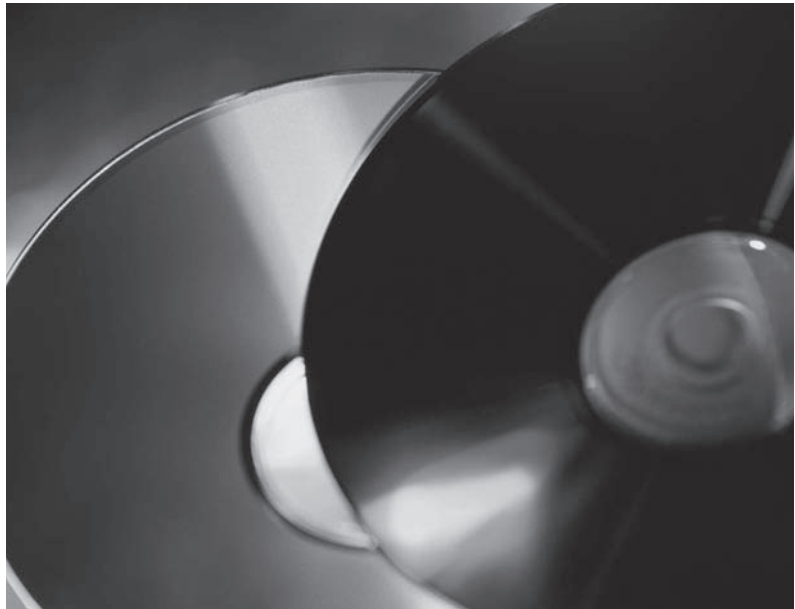
11. Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, som behandles ved hjælp af edb, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

12. Der skal foretages registrering af alle afviste forsøg på adgang til edb-systemet. Hvis der registreres et nærmere fastsat antal på hinanden følgende

afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg.

Logning:

13. I edb-registre skal der foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes.



# Tilsynsvirksomhed

## Generelt om Datatilsynets inspektioner

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

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

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

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

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

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

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

anmeldelsespligten i lovens § 53. Se eventuelt Datatilsynets årsberetning for 2001, side 78, i afsnittet ”Inspektioner hos private virksomheder”.

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

## **Gennemførelse af inspektioner**

Inspektioner tager oftest udgangspunkt i de behandlinger, den dataansvarlige har anmeldt til Datatilsynet. De anmeldte behandlinger gennemgås, og behandlinger, som den dataansvarlige har vurderet ikke-anmeldelsespligtige, drøftes. Datatilsynet anmoder således rutinemæssigt forud for en inspektion den dataansvarlige myndighed om at få tilsendt en oversigt over behandlinger af personoplysninger, som myndigheden har vurderet ikke at være anmeldelsespligtige. Formålet hermed er bl.a., at en sådan oversigt er velegnet som udgangspunkt for en drøftelse/vurdering af den dataansvarliges egen vurdering af de konkrete behandlinger. Oversigten kan endvidere være et nyttigt redskab for den dataansvarlige i tilfælde, hvor en registreret person anmoder om indsigt i de oplysninger, den dataansvarlige behandler om den pågældende.

Herefter gennemgås en række emner af generel karakter samt emner, som vurderes at være særligt relevante for den pågældende dataansvarlige. Eksempler på emner kan være:

- Logning og sletning
- Oplysningspligt, indsigtbegæringer og samkøring i kontroløjemed
- Billeder og andre informationer på internet
- Kontrol af medarbejderes brug af internet og e-mail
- Elektronisk borgerbetjening og transmission af oplysninger via hjemmeside
- Hjemmearbejdspladser og mobile arbejdspladser
- Trådløse netværk

I efteråret 2004 og igen i 2005 har Datatilsynet i forbindelse med inspektioner hos offentlige myndigheder valgt at lægge særlig vægt på et mere afgrænset antal af emner, idet der derved bliver tid til en mere grundig gennemgang og drøftelse af de enkelte emner. Følgende emner har været valgt:

- Den registreredes rettigheder

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

Efter gennemgang af relevante emner gennemgås ved de inspektioner hos offentlige myndigheder, hvor en af Datatilsynets IT-sikkerhedskonsulenter deltager, de uddybende sikkerhedsregler, som myndigheden har fastsat i henhold til sikkerhedsbekendtgørelsens § 5, og som myndigheden forud for inspektionen har indsendt til Datatilsynet. Tilsynet tilkendegiver sit overordnede indtryk og giver eventuelle specifikke kommentarer til de uddybende regler. Herefter kan man eventuelt gå i en dybere dialog om enkelte emner og undersøge særlige forhold vedrørende driftsprocedurer, anvendelse af sikkerhedsforanstaltninger mv. Ved inspektioner, hvor der ikke deltager en IT-sikkerhedskonsulent, giver tilsynet en mere summarisk feedback på de uddybende sikkerhedsregler, og der fokuseres i højere grad på andre emner end de rent teknisk-sikkerhedsmæssige.

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

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

Det har i forbindelse med inspektioner hos private dataansvarlige i flere år været praksis at afslutte inspektionssagen på stedet, når der under inspektionen ikke blev observeret forhold, der skulle undersøges nærmere eller bringes i orden, før sagen kunne afsluttes.

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

Efter denne procedure gennemgår Datatilsynet mere indgående end hidtil sine observationer med den dataansvarlige myndighed, inden tilsynets repræsentanter forlader stedet, og den dataansvarlige får udleveret en kopi af tilsynets noter. Selv om sagen ikke kan slutes på stedet, kan udlevering af noterne bidrage til, at myndigheden med det samme kan få et bedre overblik over tilsynets observationer, herunder hvilke forhold der skal undersøges nærmere eller bringes i orden.

Uanset at den nye procedure i 2004 kun i en enkelt kommune resulterede i, at inspektionen kunne afsluttes på stedet, var erfaringerne med den nye procedure efter Datatilsynets opfattelse lovende.

På denne baggrund besluttede Datatilsynet i 2005 indtil videre at benytte den nye procedure ved kommuneinspektioner. Datatilsynet overvejer endvidere, om samme praksis med fordel kan tages i brug over for andre offentlige myndigheder.

Ved kommuneinspektionerne i 2005 kunne flere sager afsluttes på stedet. Datatilsynet vurderer dette som positivt. Dels derved, at man ikke under disse inspektioner har konstateret forhold, der gav anledning til nærmere undersøgelser, eller som skulle bringes i orden, før inspektionen kunne afsluttes, og dels derved, at det bidrager til at reducere omfanget af – ikke kun Datatilsynets, men også den pågældende myndigheds – administration knyttet til en inspektion. Endvidere er det klart Datatilsynets indtryk, at effekten ved en inspektion forøges ved, at den inspicerede myndighed får tilsynets umiddelbare respons.

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

### **Udvælgelse af dataansvarlige til inspektion i 2005**

På grund af den forestående strukturreform, der bl.a. betyder, at kommuner og amter er i gang med omfattende organisationsomlægninger, herunder omlægning af procedurer og sagsgange, valgte Datatilsynet i 2005 i et vist omfang at prioritere sine ressourcer på inspektioner hos private dataansvarlige. Af samme grund blev der ikke i 2005 udvalgt et bestemt geografisk område som fokus for årets inspektioner på samme måde, som det er sket i årene 2002 til 2004. I stedet udvalgte et antal dataansvarlige efter et kriterium om, at Datatilsynet ønskede at se nærmere på dataansvarliges anvendelse af ny teknologi. Der har således ved Datatilsynets inspektioner i 2005 været fokus på områderne digital borgerbetjening og elektronisk patientjournal. Tilsynet ønskede endvidere at få et foreløbigt indtryk af udbredelsen af mobile systemer og eventuelle erfaringer hermed.

## **Datatilsynets observationer ved inspektioner i 2005**

Datatilsynets inspektioner har – uanset at tilsynet i et vist omfang har prioriteret at foretage inspektioner hos private dataansvarlige – igen i 2005 været bredt fordelt over forskellige typer af private og offentlige dataansvarlige: Kommuner og amter, offentlige sygehuse, politiet, staten i øvrigt, private forskere og øvrige private virksomheder – herunder private virksomheders personaleadministration – forsikringsselskaber, kreditoplysningsbureauer og stillingsbesættende virksomheder (headhuntere). Tilsynet har endvidere foretaget inspektion hos en biobank og hos en virksomhed, der har anmeldt et advarselsregister.

I det følgende beskrives i store træk de observationer, som Datatilsynet har gjort i forbindelse med inspektionerne i 2005. Der er ikke foretaget en egentlig statistisk bearbejdning af inspektionsresultaterne, men beskrivelsen er egnet til at illustrere de generelle tendenser, som tilsynet har oplevet på inspektionerne.

### ***Anmeldelser***

Det overordnede indtryk efter inspektionerne afholdt i 2005 er fortsat, at de dataansvarlige generelt er opmærksomme på pligten til at anmelde behandlinger af personoplysninger til Datatilsynet. Tilsynet konstaterede på det kommunale område enkelte manglende anmeldelser, men de dataansvarlige har i det store hele foretaget anmeldelse af de anmeldelsespligtige behandlinger, de foretager. Der synes i det hele taget at være god bevågenhed omkring persondatalovens regler.

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

Det er desværre fortsat Datatilsynets erfaring, at en del dataansvarlige har vanskeligt ved at udarbejde en sådan oversigt. Tilsynet finder dette beklageligt, idet det tyder på, at den dataansvarlige ikke har overblik over alle de behandlinger af personoplysninger, som den dataansvarlige foretager.

### ***Opfyldelse af logningskrav og sletning af data***

Inspektionerne gav i en del tilfælde Datatilsynet anledning til at fremhæve kravet om, at fortrolige og følsomme personoplysninger, der behandles i tekstbehandlingssystemer og lignende, hvor der ikke sker logning, skal slettes efter en vis kortere periode. Tilsynet stødte på enkelte eksempler på, at tekstbehandlings-

dokumenter o.l. ikke var slettet i overensstemmelse med reglerne i sikkerhedsbekendtgørelsen.

Det er endvidere Datatilsynets indtryk, at der især på sygehusområdet kan herske nogen usikkerhed i relation til at få slettet patientdata inden for slettefristerne. Inspektioner på sygehuse giver derfor nogle gange anledning til, at Datatilsynet anmoder om nærmere oplysninger om, hvorvidt sygehuset har etableret formaliserede procedurer for sletning af patientdata – og i givet fald hvilke.

### ***Elektronisk borgerbetjening mv.***

De dataansvarlige myndigheder er tilsyneladende generelt opmærksomme på reglerne for transmission af personoplysninger over internettet. Det er endvidere tilsynets indtryk, at de løsninger, der benyttes til elektronisk borgerbetjening, ofte er leveret af leverandører, som er godt bekendt med reglerne på området. I et enkelt tilfælde var det vanskeligt at få afdækket, om fortrolige personoplysninger, som blev indsamlet over internettet i forbindelse med rekruttering af medarbejdere, var tilstrækkeligt beskyttet mod at komme til uvedkommendes kendskab.

Det var Datatilsynets indtryk, at anvendelsen af mobile systemer ikke er særlig udbredt. Men der kan tydeligt spores en interesse. Tilsynet får således af og til spørgsmål om emnet fra kommuner og leverandører, og ved et par af de besøgte kommuner var der konkrete overvejelser om at tage mobile systemer i brug på omsorgsområdet inden for en nær fremtid.

### ***Uddybende sikkerhedsregler***

Ved tilsynets inspektioner er det typiske billede fortsat, at de dataansvarlige følger god praksis i forhold til it-sikkerhed. Der synes at kunne spores en øget opmærksomhed på sikkerhedsbekendtgørelsens krav om udarbejdelse af interne uddybende sikkerhedsregler, men tilsynet kunne dog igen i 2005 konstatere manglende, mangelfulde eller forældede uddybende sikkerhedsregler hos offentlige myndigheder.

Formålet med de uddybende sikkerhedsregler er at beskrive, hvordan myndigheden i praksis lever op til sikkerhedsbekendtgørelsens krav. De uddybende sikkerhedsregler skal således beskrive eller referere til beskrivelser af ansvarsforhold, etablerede sikkerhedsforanstaltninger, arbejdsgange osv.

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

### **Besigtigelse af fysisk sikkerhed**

I Datatilsynets inspektioner indgår som regel en besigtigelse af publikumsområder, serverrum og arkiver, hvor der behandles eller opbevares personoplysninger.

Ved besigtigelse af serverrum undersøger Datatilsynet forhold vedrørende fysisk adgang, sikring mod brand- og vandskader, forsyningssikkerhed mv.

På det private forskningsområde ses der i nogle tilfælde at være problemer omkring opbevaring af manuelt materiale i arkiver og lignende, hvor uvedkommende i forhold til projektet også har adgang. Uvedkommende i forhold til et projekt kan være øvrige ansatte på en sygehusafdeling, som huser et privat forskningsprojekt, der udføres af en ansat på afdelingen. I de vilkår, der er fastsat af Datatilsynet, er der typisk et krav om at opbevare personoplysninger under lås.

### **Oversigt over udførte inspektioner i 2005**

På nedenstående oversigt er der indsat markeringen ”” ved de inspektioner, som har givet Datatilsynet anledning til at underrette kommunalbestyrelsen/ amtsrådet eller en overordnet myndighed om resultatet af Datatilsynets inspektion. Enkelte inspektionssager er endnu ikke færdigbehandlet.

#### **Staten (7):**

Politimesteren i Grenå  
Politimesteren i Randers  
Politimesteren i Silkeborg  
Politimesteren i Århus  
Politimesteren på Bornholm  
Rigspolitichefen, afd. D  
Udlændingestyrelsen (US-SIS)

#### **Kommuner og amter (13):**

i Albertslund Kommune  
Bornholms Regionskommune  
Ebeltoft Kommune  
Frederiksværk Kommune  
Fyns Amt  
Gladsaxe Kommune  
Grenå Kommune  
Helsingør Kommune  
Helsingør Kommune  
Hillerød Kommune  
Kalundborg Kommune

Odense Kommune  
Vinderup Kommune

**Offentlige sygehuse (3):**

Bornholms Centralsygehus, administrative patientdata, sundhedsdatabanken  
Københavns Amt Gentofte, administrative patientdata  
Københavns Amt, Steno Diabetes Center, elektronisk patientjournal

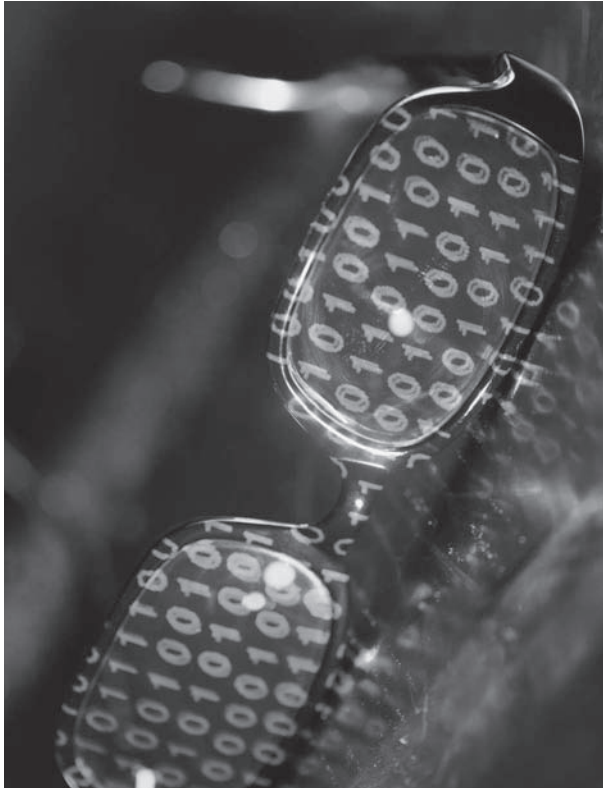
**Private forskere (26):**

Anders Krarup-Hansen  
Anna Thit Johnsen, Bispebjerg Hospital  
Bettina Bach, Danmarks Pædagogiske Universitet  
Birgitte Brandstrup, Bispebjerg Hospital  
Birgitte Uldum, Kbh. Kom. Børne- og Ungdomstandpleje  
Bo Abrahamsen, Odense Universitetshospital  
Børge G. Nordestgaard, KAS Herlev  
Erik Jakobsen, Odense Universitetshospital  
Esben Boeskov Øzhayat, Københavns Tandlægeskole  
Hannah Bro, Bispebjerg Hospital  
Henning Hansen, Casa  
Iben Bache, Panum Institutet  
Joachim Knop, H:S Institut for Sygdomsforebyggelse  
Lisbeth Tranebjærg, Bispebjerg Hospital  
Lone Klinge, Odense Universitetshospital  
Merete W. Nielsen, Danmarks Farmaceutiske Universitet  
Michael Norup, Afdeling for Videnskabsteori, Panum Institutet  
Mogens Grønvold, Bispebjerg Hospital  
Olfred Hansen, Odense Universitetshospital  
Poul Holm-Pedersen, Københavns Tandlægeskole  
Sigurd Benjaminsen, Odense Universitetshospital  
Steffen Loft, Panum Institutet, KU  
Torben Barington, Odense Universitetshospital  
Vibeke Backer, Bispebjerg Hospital  
Vibeke Lind Due, KAS Herlev  
Vibeke Rømming Sørensen, Rigshospitalet

**Øvrige private (12):**

Dansk Supermarked Administration A/S' bortvisningsregister  
De grafiske Fags Leverandørforening  
Debitorregisteret  
Etac A/S  
Financial Insurance Company Limited  
Jobcenter Østdanmark  
KOB

L'Oréal Danmark A/S  
NB TV Productions ApS  
Randstad A/S  
RKI  
SOS-International



Datatilsynet

Borgergade 28, 5.

1300 København K

Telefon: 3319 3200

Telefax: 3319 3218

Epost: [dt@datatilsynet.dk](mailto:dt@datatilsynet.dk)

Hjemmeside: [www.datatilsynet.dk](http://www.datatilsynet.dk)