Datatilsynets årsberetning 2008 og 2009

Udgiver: Datatilsynet
Tryk og layout: Rosendahls-Schultz Grafisk
Beretningen er sat med Meta
Oplag: 300
Marts 2010
ISSN nr: 1601-5657
ISBN nr: 978-87-992871-1-6

Indhold

Til Folketinget

Datatilsynet afgiver hermed sin årsberetning for 2008 og 2009. Beretningen afgives i henhold til persondatalovens § 65, hvorefter Datatilsynet afgiver en årlig beretning om sin virksomhed til Folketinget.

Årsberetningen omfatter både 2008 og 2009, da det på grund af travlhed i Datatilsynet ikke har været muligt at færdiggøre en årsberetning for 2008 inden udgangen af 2009.

Beretningen indeholder en omtale af væsentlige aktiviteter for Datatilsynet i 2008 og 2009, herunder nogle af Datatilsynets udtalelser til de lovforslag mv., som tilsynet har haft i høring i 2008 og 2009. Endvidere indeholder beretningen et afsnit om det internationale arbejde, som Datatilsynet har deltaget i samt et afsnit om sikkerhedsspørgsmål.

I afsnittet om tilsynsvirksomhed omtales de inspektioner (kontrolbesøg), som Datatilsynet har gennemført i 2008 og 2009.

På Datatilsynets hjemmeside www.datatilsynet.dk har tilsynet siden 2004 løbende offentliggjort udtalelser og afgørelser i sager, som vurderes at være af generel interesse. Årsberetningen indeholder derfor ikke referater af konkrete sager om behandling af personoplysninger. For yderligere oplysninger om Datatilsynets virksomhed henvises således til tilsynets hjemmeside.

København, marts 2010.

Henrik Waaben
Formand for Datarådet

Janni Christoffersen
Direktør

Datatilsynets virksomhed i 2008 og 2009

Datatilsynet administrerer lov om behandling af personoplysninger (persondataloven). Datatilsynet fører tilsyn med enhver behandling, der er omfattet af loven, bortset fra domstolenes behandling.

Af Datatilsynets aktiviteter i 2008 og 2009 kan blandt andet nævnes:

- Vejledning og rådgivning over for offentlige myndigheder, personer og virksomheder, herunder gå-hjem-møder
- Behandling af klager fra personer over registrering, videregivelse af oplysninger, manglende indsigt mv.
- Udtalelser om lovforslag og bekendtgørelser mv.
- Udtalelser om anmeldelser fra offentlige myndigheder
- Tilladelser til offentlige myndigheder og virksomheder mv.
- Tilladelser i forbindelse med anmeldelser fra forskere
- Bidrag til besvarelse af spørgsmål fra Folketinget
- Sager på Datatilsynets eget initiativ, herunder inspektioner hos offentlige myndigheder og private virksomheder mv. samt hos forskere
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsynsmyndigheder
- Deltagelse i arbejdsgrupper, udvalg mv. og oplæg på konferencer mv.

Datatilsynet har i 2008 registreret 5.042 nye sager, hvilket er et fald på 8 % i forhold til 2007, hvor der blev registreret 5.492 nye sager. Faldet i antallet af nyoprettede sager i 2008 set i forhold til 2007 skyldes især et stort fald i antallet af offentlige anmeldelser, efter at Datatilsynet har effektiviseret ordningerne vedrørende både kommuner og regioner. I 2009 registrerede Datatilsynet 4.859 nye sager, hvilket er et fald på 4 % i forhold til 2008. Faldet i 2009 skyldes også et

fald i antallet af offentlige anmeldelser. I begge år er til gengæld noteret en stor stigning i antallet af sager vedrørende lovforslag, bekendtgørelser mv., antallet af forespørgsler og klager samt antallet af sager på Datatilsynets eget initiativ. Der henvises til afsnittet om statistiske oplysninger.

Datatilsynets opgaver

Rådgivning og vejledning

En af Datatilsynets hovedopgaver er at yde en serviceorienteret rådgivning og vejledning om persondataloven over for myndigheder, virksomheder og enkeltpersoner. 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.

Dette sikres bl.a. via tilsynets hjemmeside, hvor principielle afgørelser mv. offentliggøres. Endvidere har tilsynet udarbejdet en generel informationspjece samt vejledninger mv. om persondataloven, som ligeledes kan ses på tilsynets hjemmeside. Det er muligt at tegne et elektronisk abonnement på tilsynets hjemmeside, således at abonnenterne automatisk modtager en e-post, når hjemmesiden opdateres. Tilsynet deltager ligeledes løbende i konferencer, møder og undervisningsforløb.

I de senere år har Datatilsynet deltaget i mange udvalg, møder og konferencer. Således har tilsynet både i 2008 og 2009 deltaget som paneldeltagere eller oplægsholdere på flere konferencer samt haft et stigende antal møder både med parter fra den offentlige og den private sektor.

Det kan bl.a. nævnes, at Datatilsynet inden for sundhedsområdet deltager som observatør i Informationssikkerhedsrådet under Sammenhængende Digital Sundhed i Danmark, og at tilsynet deltager i Den tværoffentlige arbejdsgruppe vedrørende privacy.

Datatilsynet har også deltaget i Udvalget om udveksling af oplysninger inden for den offentlige forvaltning, hvis arbejde førte til den nedenfor nævnte ændring af forvaltningsloven og persondataloven, Justitsministeriets Udvalg om offentlige myndigheders offentliggørelse af kontrolresultater mv. samt Udvalget vedrørende PET og FE.

Datatilsynet yder også rådgivning og vejledning på bilaterale møder med både offentlige myndigheder og private virksomheder. Det kan f.eks. være i forbindelse med digital forvaltning, som ofte også involverer private virksomheder, leverandører mv.

Datatilsynet modtager fortsat et meget stort antal telefoniske henvendelser. Det er tilsynets opfattelse, at telefonrådgivningen er en vigtig del af tilsynets arbejde, som især kan hjælpe dataansvarlige til at løse eventuelle problemer i opstarten.

På baggrund af tilsynets kvartalsvise stikprøvetællinger anslås antallet af telefoniske henvendelser til tilsynet i 2008 og 2009 at ligge over niveauet for 2007, det vil sige ca. 18.000 pr. år.

Datatilsynet afholdt i 2009 to gå-hjem-møder vedrørende tv-overvågning.

Klagesagsbehandling

I klagesagerne træffer Datatilsynet egentlige afgørelser om, hvorvidt en behandling er i overensstemmelse med loven. Det er af afgørende betydning, at borgere, der f.eks. mener sig udsat for behandling af oplysninger i strid med loven eller ikke får de oplysninger, de mener at have krav på efter reglerne om de registreredes rettigheder, kan få tilsynets vurdering af forholdet.

I 2008 har tilsynet registreret en stigning på 30 % i antallet af nye sager (forespørgsler og klager) vedrørende private virksomheder mv. (fra 662 i 2007 til 861 i 2008). I forhold til offentlige myndigheder er der i 2008 registreret en stigning på 27 % i antallet af tilsvarende nye sager (fra 360 i 2007 til 458 i 2008). I 2009 har tilsynet registreret en stigning på 11 % i antallet af sager (forespørgsler og klager) vedrørende private virksomheder mv. (fra 861 i 2008 til 960 i 2009). I forhold til offentlige myndigheder er der også i 2009 sket en stigning i antallet af tilsvarende nye sager. Stigningen er på 11 % (fra 458 i 2008 til 508 i 2009).

Datatilsynet har ingen entydig forklaring på den store stigning i antallet af klager og forespørgsler over de seneste år. Der er formentlig flere årsager hertil, men en af disse kan være udbygningen af den borgerrettede information på tilsynets nye hjemmeside, som blev lanceret i begyndelsen af 2008.

Nedenfor i afsnittet om statistiske oplysninger er der uddybende informationer om klagesager. På tilsynets hjemmeside er bl.a. offentliggjort målsætninger for sagsbehandlingstider.

Høring over lovforslag mv.

Datatilsynet skal efter persondataloven afgive udtalelse ved udarbejdelse af generelle retsforskrifter, f.eks. lovforslag, direktivforslag, bekendtgørelser, mv., der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger. Datatilsynet belyser i sine udtalelser, hvilke konsekvenser for databeskyttelsen et lovforslag eventuelt har, og tilsynets udtalelser udgør således et bidrag til grundlaget for den politiske beslutningsproces. Tilsynet finder denne opgave vigtig, dels fordi tilsynet besidder en ekspertviden om databeskyttelse, dels fordi tilsynet efter persondataloven udøver sine funktioner i fuld uafhængighed.

I 2008 registrerede tilsynet 238 udtalelser til lovforslag mv., hvilket er omtrent samme niveau som i 2007, hvor antallet var 247. I 2009 er der sket en stigning i antallet af sager vedrørende til lovforslag mv. på 38 % i forhold til 2008 (fra 238 i 2008 til 329 i 2009). I perioden fra 2001 til 2006 har der været en stigning på 270 %.

En del af de lovforslag, som Datatilsynet har modtaget i høring i 2008 og 2009, rejser fortsat vanskelige spørgsmål om forholdet mellem de påtænkte regler, reglerne i persondataloven og databeskyttelsesdirektivet. I en del tilfælde foreslås regler, som indebærer en behandling af personoplysninger, der ikke umiddelbart kan ske inden for rammerne af persondataloven. Gennemførelsen kræver, at der i særlovgivningen sker en fravigelse af persondataloven. I sådanne tilfælde anbefaler tilsynet i sine høringssvar, at det tydeliggøres i lovforslaget, om der er tale om en fravigelse af persondataloven og i givet fald, om en sådan fravigelse kan ske inden for rammerne af databeskyttelsesdirektivet. I disse situationer er det som udgangspunkt tilsynets holdning, at der kun bør tilvejebringes en særskilt hjemmel til behandling af personoplysninger i videre omfang end, hvad der følger af persondataloven, hvis der er tale om vægtige samfundsmæssige hensyn. Om der konkret er tale om sådanne vægtige samfundsmæssige hensyn, der taler for at fravige det generelle beskyttelsesniveau, beror i sidste ende på en politisk vurdering, som må foretages af Folketinget. Datatilsynet har imidlertid i en del tilfælde udtrykt betænkeligheder i forhold til den påtænkte lovgivning.

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

Sager på eget initiativ

Datatilsynet har i 2008 registreret 160 sager, rejst på tilsynets eget initiativ. I 2007 var tallet 113 sager. I 2009 registrerede Datatilsynet 170 sager rejst på tilsynets eget initiativ. Sagerne omfatter såvel inspektioner som andre "egen drift sager".

I 2008 har Datatilsynet gennemført 94 inspektioner, 32 hos offentlige myndigheder og 62 hos forskellige private virksomheder. Dette er en mindre stigning i forhold til niveauet i 2007 (66 inspektioner), og antallet lever op til det fastsatte mål på mindst 85 inspektioner for 2008.

I 2009 gennemførte Datatilsynet 83 inspektioner, 34 hos offentlige myndigheder og 49 hos forskellige private virksomheder. Antallet af inspektioner i 2009 er mindre end i 2008 og også en smule mindre end det fastsatte mål på 85 inspektioner. Det mindre antal inspektioner må ses i lyset af, at der i 2008-09 har været en ganske voldsom stigning i sager om sikkerhedsbrister, som Datatilsynet har behandlet, jf. nedenfor i afsnittet om sikkerhed.

Datatilsynet tager løbende initiativer rettet mod afgrænsede områder, f.eks. en bestemt branche eller en bestemt type behandling af personoplysninger. I 2008 og 2009 har Datatilsynet bl.a. haft fokus på tv-overvågning.

Strafniveau for overtrædelse af persondataloven

Datatilsynet har i perioden 2000-2008 indgivet politianmeldelse i 26 sager. Datatilsynet har bl.a. indgivet politianmeldelse i 9 sager vedrørende tv-overvågning og i 7 sager vedrørende manglende anmeldelse til Datatilsynet. I nogle af sagerne har Datatilsynet indgivet politianmeldelse umiddelbart efter, at der er konstateret en overtrædelse af persondataloven og i andre sager, er der først sket anmeldelse til politiet efter et længere sagsforløb i Datatilsynet.

I 2008 foretog Datatilsynet en gennemgang af sager, hvor der var enten var sket bødevedtagelse eller afsagt dom vedrørende overtrædelse af persondataloven. Pådømmelse af overtrædelserne er sket både på baggrund af politianmeldelser fra Datatilsynet og i sager, hvor Datatilsynet ikke har været involveret. I alt drejer det sig om 26 sager, herunder 3 ankedomme, vedrørende persondataloven i perioden 2000-2008.

5 af afgørelserne (dom og bødevedtagelser) vedrører behandling af kreditoplysninger. 4 afgørelser vedrører uberettiget søgning i RKI's registre. 1 afgørelse vedrører videregivelse til RKI af et bestridt skyldforhold. Fælles for afgørelserne er, at de alle ses at være afsluttet med en bøde på 5.000 kr.

Vedrørende uberettiget offentliggørelse på internettet har der været 3 strafferetlige afgørelser, herunder 1 med ankedom, og 1 afgørelse i en civilsag. De 3 straffesager er afgjort med bøder på mellem 2.000-7.000 kr.

Offentliggørelse af billeder (almindelige oplysninger) har således udløst en bøde på 2.000 kr., offentliggørelse af personnumre (fortrolige oplysninger) har udløst en bøde på 3.000 kr., og offentliggørelse af helbredsoplysninger (følsomme oplysninger) har udløst en bøde på 7.000 kr. De 3 afgørelser viser, at bødeniveauet har afspejlet karakteren af de offentliggjorte oplysninger.

Vedrørende tv-overvågning var der 2 afgørelser. Den ene er i en civil sag og vedrører overvågning, der fandtes i strid med persondatalovens § 5, stk. 1 og 2. Dommen resulterede i erstatning for tort på 25.000 kr., jf. erstatningsansvarsloven, og illustrer således ikke sanktionsniveauet for overtrædelser af persondataloven.

Den anden afgørelse vedrører uberettiget videregivelse efter den nye bestemmelse i persondatalovens § 26 a vedrørende tv-overvågning. Sagen resulterede i en bødevedtagelse på 5.000 kr.

Der er siden 2008 sket frifindelse ved domstolene i enkelte sager vedrørende reglerne i persondataloven om tv-overvågning på grundlag af en konkret vurdering af de fremlagte beviser. Herudover har en række virksomheder vedtaget bødeforelæg i sager, hvor Datatilsynet har foretaget politianmeldelse.

På markedsføringsområdet har der været 3 afgørelser. 1 sag vedrører videregivelse i strid med persondatalovens § 36, og 2 af sagerne vedrører overtrædelse af persondatalovens § 6 og tillige overtrædelse af markedsføringsloven. Der blev henholdsvis givet bøder på 7.000 kr., på 7.500 kr. og på 25.000 kr. I sagen med bøden på 25.000 var der tale om salg af en hel kundedatabase. 2 ud af 3 sager omfattede også markedsføringsloven, hvorfor der næppe er grundlag for at konkludere, at overtrædelse af persondatalovens markedsføringsregler almindeligvis fører til højere bøder end overtrædelse af andre af lovens regler.

Der har i perioden været 2 afgørelser vedrørende private virksomheders ulovlige behandling af følsomme oplysninger. Sagerne er afgjort med bødeforelæg på henholdsvis 10.000 kr. og 5.000 kr.

Anmeldelser

Datatilsynet har også i 2008 behandlet en hel del anmeldelser og ansøgninger om tilladelser. Der er således blevet registreret 2.930 nye anmeldelser i 2008, mod 3.668 nye anmeldelser i 2007. Med hensyn til nye offentlige anmeldelser er der tale om et fald på 63 % i forhold til 2007. Det markante fald skyldes, at

kommuner og regioner i 2007 har tilsluttet sig nye fællesanmeldelser, der er blevet udarbejdet som følge af strukturreformen.

I 2009 blev der registreret 2.452 nye anmeldelser. Der er i forhold til 2008 sket et yderligere fald i offentlige anmeldelser på 42 %, hvilket bl.a. må tilskrives den nye ordning på regionernes område især med hensyn til forskningsanmeldelser.

Whistleblower

Datatilsynet har modtaget flere anmeldelser fra private virksomheder og koncerner, der ønsker at indføre en såkaldt whistleblower ordning, hvor det er muligt at rapportere uregelmæssigheder til virksomhedens ledelse.

Datatilsynet har – efter at sagen har været behandlet i Datarådet – udarbejdet en vejledning til anmeldelse af whistleblower ordninger. Vejledningen findes på Datatilsynets hjemmeside under blanketter. I vejledningen behandles bl.a., hvem der er dataansvarlig, hvilke oplysninger der kan behandles, hvem der kan rapportere i whistleblower ordningen, hvem der kan rapporteres om, og hvornår oplysningerne skal slettes.

Datatilsynet har endvidere offentliggjort et svar på en anmeldelse på en whistleblower ordning på følgende adresse: http://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/svar-paa-anmeldelse-af-whistleblower-system/.

Projekt i Grønland

Datatilsynet gennemførte i 2008 et projekt med henblik på ajourføring af registerforskrifter for offentlige myndigheder i Grønland. Datatilsynet afholdt orienterende møder med Hjemmestyret, departementerne, Grønlands Statistik og KANOKUKA (Kommunernes Landsforening). Datatilsynet fik ved møderne bl.a. lejlighed til at drøfte den forestående og omfattende strukturreform i Grønland og herunder udbygningen af det kommunale selvstyre. Tilsynet havde i den anledning udarbejdet en række forslag til opdaterede forskrifter for departementernes og kommunernes registre samt for registrene i Grønlands Statistik. På møderne blev de forskellige forslag gennemgået med henblik på kommende forskriftsrevisioner. For Datatilsynet var det også en anledning til at udbygge kontakten til de grønlandske myndigheder omkring registerspørgsmål og i øvrigt gøre sig nærmere bekendt med de grønlandske forhold.

Tv-overvågning

Generelt om tv-overvågning

Med lov nr. 519 af 6. juni 2007 ændredes lov om forbud mod tv-overvågning mv. og lov om behandling af personoplysninger (udvidelse af adgangen til tv-overvågning og styrkelse af retsbeskyttelsen ved behandling af personoplysninger i forbindelse med tv-overvågning). Ændringsloven trådte i kraft den 1. juli 2007.

Ændringerne i persondataloven indebærer, at al behandling af personoplysninger i forbindelse med tv-overvågning nu omfattes af loven, uanset om behandlingen er elektronisk eller analog. Der er endvidere indsat et nyt kapitel 6a i persondataloven, som særligt vedrører behandling af optagelser fra tv-overvågning, der foretages i kriminalitetsforebyggende øjemed.

Kapitlet indeholder regler for videregivelse af sådanne optagelser, for opbevaring og sletning af optagelser samt en henvisning til persondatalovens generelle regler om oplysningspligt, som gælder ved siden af reglerne om skiltning i lov om tv-overvågning. Lovændringen medfører også, at offentlige myndigheder ikke længere skal anmelde deres behandling af personoplysninger ved hjælp af tv-overvågning til Datatilsynet. Der er heller ikke anmeldelsespligt for private virksomheder, som benytter sig af tv-overvågning, men Datatilsynet har inspektionsadgang på området.

I forbindelse med ændringslovens ikrafttrædelse har Datatilsynet orienteret om lovændringerne, dels ved et brev til alle offentlige myndigheder, dels ved tekster på Datatilsynets hjemmeside. Endelig har Datatilsynet i samarbejde med Justitsministeriet udarbejdet en pjece om de regler i persondataloven og tv-overvågningsloven, som gælder for tv-overvågning. Pjecen er tilgængelig på Datatilsynets og Justitsministeriets hjemmesider.

Datatilsynet har i 2008 og 2009 behandlet en række sager om tv-overvågning, herunder klagesager. Flere af sagerne omhandlede klager over uberettiget videregivelse af tv-overvågningsoptagelser.

Siden lovændringen har Datatilsynet endvidere taget en række sager på tv-overvågningsområdet op af egen drift, bl.a. på baggrund af omtale i pressen. Sagerne har i langt de fleste tilfælde omhandlet ulovlig videregivelse af tv-overvågningsoptagelser via internettet eller til pressen.

Datatilsynet har i 2009 og navnlig i 2008 foretaget politianmeldelse i en række sager vedrørende overtrædelse af persondatalovens kapitel 6 a om tv-overvågning. I enkelte sager behandlet ved domstolene er der sket frifindelse på grundlag af en konkret vurdering af de fremlagte beviser. Herudover har en række

virksomheder vedtaget bødeforelæg i sager, hvor Datatilsynet har foretaget politianmeldelse.

I 2009 har Datatilsynet ikke haft anledning til at rejse så mange sager om uberettiget videregivelse af tv-overvågningsoptagelser. Dette må efter tilsynets vurdering bl.a. tilskrives massiv omtale i medierne af enkelte af sagerne fra 2007 og 2008.

Med de nye regler om tv-overvågning har Datatilsynet fra den 1. juli 2007 fået mulighed for at foretage inspektioner (kontrolbesøg) hos alle offentlige myndigheder og private dataansvarlige, der behandler personoplysninger i forbindelse med tv-overvågning. Inspektionerne beskrives nærmere i afsnittet om Datatilsynets tilsynsvirksomhed

Forslag om tv-overvågning i taxier
I begyndelsen af 2009 anmodede Færdselsstyrelsen Datatilsynet om en udtalelse i forbindelse med forslag til folketingsbeslutning om videoovervågning i taxier (B 79). Datatilsynet fremkom – efter at sagen havde været behandlet i Datarådet – med en udtalelse, hvor Datatilsynet på en række punktet forholdt sig kritisk til forslaget.

Senere i 2009 afgav Datatilsynet høringssvar vedrørende forslag til lov om ændring af lov om taxikørsel mv. (krav om obligatorisk tv-overvågning i taxier), som er en udmøntning af folketingsbeslutningen.

Med forslaget indføres der pligt for taxivognmænd til at installere videoovervågning i taxier med henblik på at forebygge og opklare røverier og overfald på taxichauffører.

Forslaget om tv-overvågning i taxier forventes behandlet i Folketinget i foråret 2010, og loven forventes at træde i kraft den 1. juli 2010.

Kreditoplysning

Datatilsynet modtager mange klager over registrering i et kreditoplysningsbureau. De fleste sager vedrører indberetning fra private til et kreditoplysningsbureau, og enkelte sager vedrører indberetning til et kreditoplysningsbureau fra offentlige myndigheder.

Reglerne for kreditoplysning er stort set en videreførelse af de regler, der var gældende også før persondatalovens ikrafttræden. Datatilsynet har på denne baggrund en omfattende praksis, men der opstår hele tiden nye problemstillinger, på baggrund af ændret lovgivning, udviklingen i samfundet og den teknologiske udvikling.

Der er sket en stigning på 17 % i antallet af sager på kreditoplysningsområdet fra 105 i 2008 til 123 i 2009. Stigningen kan skyldes, at der på grund af den økonomiske krise er sket et større antal indberetninger til kreditoplysningsbureauerne.

Et spørgsmål af mere generel karakter har været en anmodning om, at Datatilsynet tog stilling til, om det kunne tillades visse inkassobureauer at indestå for opfyldelse af betingelserne i persondatalovens § 23, stk. 3. Advokater kan allerede indestå for dette.

Under henvisning til bl.a. advokaters uddannelse og til, at advokater er underlagt tilsyn fra Advokatsamfundet og kan indklages for Advokatnævnet, fandt Datatilsynet, at der ikke er tilstrækkeligt grundlag for at give inkassovirksomheder adgang til at indestå for opfyldelse af betingelserne i persondatalovens § 23, stk. 3, ved indberetning til et kreditoplysningsbureau.

Sociale netværk

Datatilsynet har behandlet flere sager om sociale netværk på internettet og har i regi af Artikel 29-gruppen været med til at vedtage en udtalelse om sociale netværk på internettet.

De sociale netværk på internettet indsamler en række personoplysninger om brugerne og kommer i besiddelse af meget store informationsmængder.

Der er tale om et område i udvikling, og der opstår fortsat nye udfordringer i forhold til beskyttelse af privatlivets fred i forlængelse af den tekniske udvikling og udbydernes opsætning af privatlivspolitikker.

I Danmark er der mere end to millioner brugere af Facebook, og Facebook har givet anledning til stor opmærksomhed i medierne, ligesom en del borgere har rettet henvendelse til Datatilsynet vedrørende Facebook.

Datatilsynet har i starten af april måned 2009 indledt en dialog med Facebook og har i den forbindelse stillet en række spørgsmål – bl.a. baseret på de henvendelser, der er kommet fra danske brugere.

Datatilsynet har endvidere generelt bedt om at få mere at vide om, hvilke personoplysninger Facebook deler med tredjeparter, herunder også hvilke oplysninger der videregives til tredjeparter, når man bruger applikationer på Facebook.

Datatilsynet er fortsat i dialog med Facebook. Datatilsynet udbygger løbende informationen om sociale netværk på sin hjemmeside. Der findes bl.a. anbefalinger til beskyttelse af privatlivets fred i sociale netværk og konkrete afgørelser vedrørende sociale netværk.

Sikkerhedskrav i privat sektor

Datatilsynet besluttede i 2007 at overveje persondatalovens sikkerhedskrav i relation til private virksomheders overførsel af personoplysninger via internettet. Efter høring af brancheorganisationer og andre interessenter mv. og efter, at sagen havde været behandlet i Datarådet, fastsatte Datatilsynet nye krav og anbefalinger. Ved fastsættelsen af kravene og anbefalingerne skelnes der mellem kommunikation via hjemmesider og kommunikation via e-mail.

Datatilsynet stiller herefter udtrykkeligt krav om kryptering ved overførsel af følsomme oplysninger og oplysning om personnummer via hjemmesider samt i tilfælde, hvor behandlingen af personoplysninger i den private sektor sker efter tilladelse med vilkår om konkrete sikkerhedsforanstaltninger ved transmission over internet.

I en række andre situationer anbefaler Datatilsynet, at personoplysninger beskyttes, når de overføres via internet.

Datatilsynet opfordrer samtidig alle interessenter til at lade hensyn til beskyttelse af personoplysninger indgå ved udformning og valg af nye tekniske løsninger til overførsel af persondata.

Biometri

Biometri er den samlede betegnelse for en række teknologiske metoder til identifikation og genkendelse af personer ved hjælp af unikke biologiske kendetegn hos personerne.

De biometriske teknikker bygger for eksempel på elektronisk genkendelse af ansigt, øjne (iris), fingre (fingeraftryk), stemme, hænder, vener og gangart. Biometrisk teknologi anvendes i stigende omfang til personidentifikation i forbindelse med adgangs- og sikringssystemer. Biometri er f.eks. et billede eller et fingeraftryk

Datatilsynet har gennem de senere år modtaget flere henvendelser både fra private virksomheder og offentlige myndigheder, der ønsker at anvende biometri f.eks. i forbindelse med adgangskontrol.

I 2008 behandlede Datatilsynet en sag om adgangskontrol på diskoteker, hvor tilsynet undersøgte et konkret diskoteks – Crazy Daisy – behandling af personoplysninger. Diskoteket anmeldte i den forbindelse behandlingen "Adgangskontrol på diskotek – førelse af intern karantæneliste". Hovedformålet med behandlingen er at sikre et trygt og sikkert natteliv. Der vil ske behandling af oplysninger om

gæsterne i et elektronisk adgangssystem. Alle gæster skal registreres, og det vil ikke være muligt at være gæst på diskoteket, hvis man ikke lader sig registrere.

I det elektroniske adgangssystem sker der indsamling, registrering, brug, opbevaring og sletning af generelle kundeoplysninger, herunder oplysninger om navn, adresse, telefonnummer, e-mail-adresse, fødselsdato, køn og ankomsttidspunkt. Der sker desuden behandling af oplysninger i form af billede og fingeraftryk.

Oplysningerne vil blive behandlet med gæstens frivillige og udtrykkelige samtykke, der indhentes i forbindelse med oprettelsen af gæsten i systemet, og den registrerede vil forud for registreringen i systemet generelt blive oplyst om systemets funktion og indretning samt de nærmere omstændigheder ved indsamlingen af oplysninger.

Diskoteket gemmer ikke gæstens fingeraftryk, men en matematisk beregnet værdi af fingeraftrykket – en såkaldt template, som benyttes til at lave en positiv identifikation. Det er ikke muligt at gendanne et fingeraftryk på baggrund af templaten.

Sammenfattende konkluderede Datatilsynet, at diskoteket med gæstens udtrykkelige samtykke kan behandle oplysninger i form af fingeraftryk (template) og billede. Hvis gæsten tilbagekalder sit samtykke, skal diskoteket slette fingeraftrykket (templaten) og billedet.

Datatilsynet gav endvidere diskoteket tilladelse til behandling af følsomme personoplysninger i forbindelse med adgangskontrol på diskoteket og førelse af en intern karantæneliste under forudsætning af, at persondatalovens regler blev iagttaget.

Tilladelsen blev givet på følgende vilkår:

1. Behandling af følsomme personoplysninger i forbindelse med tildeling og administration af en karantæne må alene ske med den registreredes skriftlige samtykke. Samtykket skal være udtrykkeligt og skal opfylde persondatalovens krav. Dvs. det skal være en frivillig, specifik og informeret viljestilkendegivelse.

2. Tilbagekaldes samtykket, skal oplysninger om årsagen til karantæne slettes.

3. Behandlingen af følsomme personoplysninger skal ske under iagttagelse af beskrevne sikkerhedsregler.

4. Medarbejderne skal informeres om, at deres opslag logges, og at loggen kan bruges til at kontrollere uberettigede opslag samt til stikprøvekontrol.

Hele Datatilsynets afgørelse kan findes på Datatilsynets hjemmeside.

Internationalt samarbejde

Datatilsynet deltager i samarbejdet bl.a. i de fælles tilsynsmyndigheder, nedsat i henhold til Schengen- og Europol-konventionerne, i Europarådets arbejde og i andre internationale arbejdsgrupper, både i og uden for EU's regi. Datatilsynet deltager endvidere i det nordiske samarbejde om persondatabeskyttelse. Aktiviteterne omtales nærmere i afsnittet om internationalt samarbejde. På Datatilsynets hjemmeside er tilsynets internationale samarbejde ligeledes beskrevet under emnet Internationalt.

Datatilsynets organisation

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

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

Datarådet

Datarådet består af en formand og af 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. Forretningsordenen fremgår af bekendtgørelse nr. 1178 af 15. december 2000 om forretningsorden for Datarådet og kan findes på Datatilsynets hjemmeside.

Datarådets medlemmer
Pr. 31. december 2009
Formand, højesteretsdommer Henrik Waaben
Næstformand, advokat Janne Glæsel
Professor, dr. jur. Peter Blume
Overlæge Hans Henrik Storm
Direktør Rasmus Kjeldahl
Kommunaldirektør Niels Johannesen
Koncern IT-Sikkerhedschef Kim Aarenstrup

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

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

Sekretariatet

Sekretariatet varetager Datatilsynets daglige forretninger. Sekretariatet beskæftiger omkring 35 medarbejdere (jurister, it-sikkerhedskonsulenter, kontorpersonale og studenter), der varetager Datatilsynets daglige drift under ledelse af en direktør.

Datatilsynets ledelse
Direktør Janni Christoffersen
Kontorchef Lena Andersen
It-chef Sten Hansen

En oversigt over Datatilsynets medarbejdere findes på tilsynets hjemmeside under punktet "Om Datatilsynet".

Datatilsynets ressourcer

Tilsynets bevillingsmæssige forhold mv. fremgår af Datatilsynets årsrapport 2008 og 2009. Årsrapporten for 2008 er offentliggjort på tilsynets hjemmeside. Årsrapporten for 2009 vil blive offentliggjort på hjemmesiden medio april 2010.

Persondataloven

Persondataloven, jf. lov nr. 429 af 31. maj 2000 med senere ændringer, trådte i kraft den 1. juli 2000. Datatilsynets årsberetning 2000 indeholder baggrunden for og forarbejderne til loven. I tilknytning til persondataloven har Justitsministeriet udsendt en række bekendtgørelser. Endvidere har Datatilsynet udsendt en række vejledninger vedrørende loven.

Ændring af persondataloven og forvaltningsloven

Med lov nr. 503 af 12. juni 2009 blev forvaltningsloven og persondataloven ændret. Fra 1. juli 2009 regulerer persondataloven således også manuel videregivelse af personoplysninger mellem forvaltningsmyndigheder. Dette fremgår af persondatalovens § 1, stk. 3. Hidtil har ren manuel videregivelse af personoplysninger været reguleret i forvaltningslovens § 28, stk. 1-3. F.eks. når oplysninger fra en manuel sag er blevet kopieret og sendt med almindelige brevpost til en anden myndighed.

Videregivelse af personoplysninger fra en myndigheds it-system har hele tiden været omfattet af persondataloven, uanset om oplysningerne sendes manuelt

eller elektronisk. Det gælder f.eks., når oplysningerne indgår i et brev, som skrives i tekstbehandling og så udskrives og sendes med brevpost med det samme. Herudover er videregivelse af personoplysninger, der foretages elektronisk, omfattet af persondataloven.

Efter lovændringen gælder der samme adgang til at udveksle personoplysninger med en anden forvaltningsmyndighed, uafhængigt af, om der er tale om oplysninger fra myndighedernes it-systemer eller fra en manuel sag, og uanset på hvilken måde udvekslingen sker.

Både fortrolige og ikke-fortrolige personoplysninger omfattes af persondataloven

I modsætning til den hidtidige regulering i forvaltningsloven omfatter persondataloven adgangen til at videregive både fortrolige og ikke-fortrolige personoplysninger til andre forvaltningsmyndigheder.

Lovændringen betyder også en vis udvidelse af adgangen til at videregive personoplysninger mellem forvaltningsmyndigheder. Dette skyldes, at der er efter persondataloven er en øget mulighed for at videregive følsomme oplysninger, hvis det er nødvendigt af hensyn til den modtagende myndigheds sagsbehandling. Det fremgår af persondatalovens § 8, stk. 2, nr. 3.

Kun videregivelse mellem danske forvaltningsmyndigheder

Ændringen af persondataloven vedrører kun videregivelse af personoplysninger mellem forvaltningsmyndigheder.

De tilfælde af ren manuel videregivelse af personoplysninger, som hidtil ikke har været omfattet af forvaltningslovens § 28, omfattes heller ikke nu af persondataloven. Det gælder f.eks. en eventuel ren manuel videregivelse af personoplysninger til ikke-danske myndigheder og til domstolene.

Hvilke regler gælder for manuel videregivelse?

Persondatalovens § 1, stk. 3, indeholder en udtømmende opregning af de regler i persondataloven, som gælder for manuel videregivelse mellem forvaltningsmyndigheder:

- de grundlæggende principper i § 5, stk. 1-3,
- behandlingsreglerne i §§ 6-8,
- § 10 om forskning og statistik
- § 11, stk. 1, om personnummer
- § 38 om tilbagekaldelse af samtykke
- § 40 om klage til tilsynsmyndigheden
- kapitel 16 om tilsyn

Det er endvidere forudsat, at de begreber, som persondataloven bygger på, jf. § 3, også gælder for manuel videregivelse af personoplysninger mellem forvaltningsmyndigheder. Det gælder eksempelvis kravene til samtykke. jf. persondatalovens § 3, nr. 8.

Datatilsynet som tilsynsmyndighed
Datatilsynet er efter lovændringen tilsynsmyndighed også i forhold til ren manuel videregivelse af personoplysninger mellem forvaltningsmyndigheder. Datatilsynet er ikke tilsynsmyndighed i forhold til ren manuel videregivelse af personoplysninger mellem forvaltningsmyndigheder i de tilfælde, hvor reglerne for videregivelse findes i anden lovgivning, f.eks. den sociale retssikkerhedslov og sundhedsloven.

Ændringsloven bygger på betænkning nr. 1500/2008 om udveksling af oplysninger inden for den offentlige forvaltning. Ændringerne trådte i kraft den 1. juli 2009.

Datatilsynets hjemmeside

Persondataloven, bekendtgørelserne og vejledningerne kan læses på Datatilsynets hjemmeside: www.datatilsynet.dk under afsnittet om lovgivning. På hjemmesiden under afsnittet om publikationer er det muligt at læse Datatilsynets informationspjece "Persondataloven", som tilsynet udsendte i forbindelse med lovens ikrafttrædelse, ligesom tilsynets årsberetninger og Registertilsynets årsberetninger fra 1997 til 1999 er tilgængelige på hjemmesiden under samme afsnit.

Datatilsynet udarbejder løbende nye tekster og informationsmateriale, der offentliggøres på hjemmesiden sammen med tilsynets afgørelser af mere generel interesse.

Enhver kan gratis tegne et elektronisk abonnement på Datatilsynets hjemmeside, således at abonnenterne automatisk modtager en e-post, når hjemmesiden opdateres. I december 2009 var der 4.193 abonnenter på Datatilsynets hjemmeside. Dette er en stigning siden udgangen af 2007, hvor der var 3.734.

Databeskyttelsesdag

Den 28. januar er fastsat til at være Den Europæiske Databeskyttelsesdag. Den Europæiske Databeskyttelsesdag er et initiativ fra Europarådet, som støttes af Europa Kommissionen og de europæiske datatilsyn.

Formålet med databeskyttelsesdagen er at forøge viden hos de europæiske borgere om, at deres personlige oplysninger bliver indsamlet og behandlet, hvorfor dette sker samt, hvilke rettigheder de har i den forbindelse.

Datatilsynet markerede dagen i 2008 ved at gå i luften med tilsynets nye hjemmeside. Hjemmesiden findes stadig på www.datatilsynet.dk, men indhold, design og navigation er ændret. Hjemmesiden er bl.a. blevet inddelt i sektioner, som er rettet specifikt henholdsvis til: Borgere, Erhverv og Offentlig. Her findes målrettet information om de områder, som er relevante for netop den målgruppe, sektionen henvender sig til.

I 2009 satte Datatilsynet fokus på en række aktiviteter, bl.a. blev informationsmøder om tv-overvågning annonceret. Endvidere var Datatilsynet gået sammen med Teknologirådet og andre om nyt undervisningsmateriale til elever i 7.-9. klasse. Der er tale om et online, interaktivt magasin, som er tilgængeligt på http://www.dubestemmerselv.dk. Projektet blev præsenteret i forbindelse med Sikker Internet Dag i regi af Medierådet for Børn og Unge, som sammen med Cyberhus også er med i projektet. Det er Datatilsynets håb, at magasinet vil være med til at åbne de unges øjne for beskyttelse af deres egne og andres personlige oplysninger.

Statistiske oplysninger

Oplysningerne i dette afsnit udgør registreringerne af nye sager i Datatilsynets journalsystem i 2008 og 2009 og vedrører sager, som er oprettet i løbet af 2008 og 2009. En del af Datatilsynets sagsbehandling er imidlertid en 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.

Statistik for 2008:

Datatilsynet registrerede 5.042 nye sager i perioden fra den 1. januar 2008 til den 31. december 2008. Disse sager fordeler sig således:

Datatilsynets egen administration mv.	209
Lovforberedende arbejde	238
Forespørgsler og klager vedrørende private	861
Forespørgsler og klager vedrørende offentlige myndigheder	458
Anmeldelse for den private sektor	2.287
Anmeldelser for den offentlige sektor	643
Sager på Datatilsynets eget initiativ (egen drift-sager)	160
Sikkerhedsspørgsmål	24
Internationale sager	148
Datatilsynets kompetence efter anden lovgivning	14

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

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 861 nye sager om forespørgsler og klager vedrørende private dataansvarlige.

Sagerne havde følgende fordeling over forskellige virksomhedstyper:

Almindelige virksomheder	121
Den finansielle sektor	74
Fagforeninger, a-kasser, pensionskasser mv.	28
Telesektoren	119
Foreninger og organisationer	85
Sundhedssektoren (medicinalfirmaer, klinikker, læger mv.)	30
Kreditoplysningsbureauer	105
Advarselsregistre	22
Stillingsbesættende virksomheder	8
Ansøgninger om tilladelser	75
Diverse	193
Sager af generel karakter	0
Edb-servicebureauer	1

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2008[1], var:

1 I lighed med Datatilsynets Årsberetning 2007 er tallene for 2008 ikke opgjort på grundlag af sager, som er oprettet i 2008, men på grundlag af sager, som Datatilsynet har færdigbehandlet i 2008. Heriblandt er sager oprettet i 2008 og 2007 samt enkelte fra 2006. Opgørelsesmetoden skyldes et ønske om at opgøre tallene på en måde, så de ikke ændrer sig afhængig af, hvornår man opgør dem.

Klager	17, 5 %
Forespørgsler	70,8 %
Ikke kategoriserede	11,7 %

Forespørgsler og klager vedrørende offentlige myndigheder
Datatilsynet registrerede i alt 458 nye sager med klager og forespørgsler vedrørende offentlige myndigheder.

Sagerne var fordelt således:

Statslige myndigheder	174
Regioner	23
Primærkommuner	129
Ansøgning om tilladelser	119
Diverse	13

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2008[2], var:

Klager	13,1 %
Forespørgsler	59,5 %
Ikke kategoriserede	27,4 %

Anmeldelser for den private sektor
Datatilsynet registrerede i alt 2.287 nye sager om anmeldelser for den private sektor. Fordelingen af sagerne var:

Forskning og statistik	1.316
Privates behandling af oplysninger om rent private forhold	711
Advarselsregistre	13
Spærrelister	4
Kreditoplysningsbureauer	4
Stillingsbesættende virksomheder	42
Edb-servicebureauer	18
Diverse sager af generel karakter	179

2 Se note 1.

Anmeldelser for den offentlige forvaltning
Datatilsynet registrerede i alt 643 nye sager om anmeldelser for den offentlige sektor. Fordelingen af sagerne var:

Fællesanmeldelser	2
Kommuner	32
Regioner	19
Statslige myndigheder	266
Tilslutninger, kommuner	330
Tilslutninger, regioner	0
Tilslutninger, statslige myndigheder	0
Diverse/sager af generel karakter	0

Sager på Datatilsynets eget initiativ
Datatilsynet registrerede i alt 160 nye sager oprettet på tilsynets eget initiativ. Fordelingen af sagerne var:

Inspektion og kontrol vedrørende private	64
Inspektion og kontrol vedrørende offentlige myndigheder	33
Sager rejst på grundlag af presseomtale og lign.	59
Diverse/sager af generel karakter	4

Sikkerhedsspørgsmål
Datatilsynet registrerede i alt 24 nye sager under kategorien sikkerhedsspørgsmål.
Fordelingen af sagerne var:

Private	16
Offentlige	8
Diverse	0

Internationale sager
Datatilsynet registrerede i alt 148 nye internationale sager. Fordelingen af sagerne var:

Forespørgsler fra udlandet	73
Nordisk tilsynssamarbejde	4
Europarådet	3
EU	48
Datakommissærsamarbejdet	13
OECD	2
Diverse/sager af generel karakter	5

Statistik for 2009:

Datatilsynet registrerede 4.859 nye sager i perioden fra den 1. januar 2009 til den 31. december 2009. Disse sager fordeler sig således:

Datatilsynets egen administration mv.	214
Lovforberedende arbejde	329
Forespørgsler og klager vedrørende private	960
Forespørgsler og klager vedrørende offentlige myndigheder	508
Anmeldelse for den private sektor	2.077
Anmeldelser for den offentlige sektor	375
Sager på Datatilsynets eget initiativ (egen drift-sager)	170
Sikkerhedsspørgsmål	30
Internationale sager	157
Datatilsynets kompetence efter anden lovgivning	39

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

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 960 nye sager om forespørgsler og klager vedrørende private dataansvarlige.

Sagerne havde følgende fordeling over forskellige virksomhedstyper:

Almindelige virksomheder	116
Den finansielle sektor	53
Fagforeninger, a-kasser, pensionskasser mv.	24
Telesektoren	165
Foreninger og organisationer	79
Sundhedssektoren (medicinalfirmaer, klinikker, læger mv.)	26
Kreditoplysningsbureauer	123
Advarselsregistre	17
Stillingsbesættende virksomheder	6
Ansøgninger om tilladelser	108
Diverse	236
Sager af generel karakter	2
Edb-servicebureauer	5

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2009[3], var:

Klager	13,6 %

3 I lighed med Datatilsynets Årsberetning 2007 er tallene for 2009 ikke opgjort på grundlag af sager, som er oprettet i 2009, men på grundlag af sager, som Datatilsynet har færdigbehandlet i 2009. Heriblandt er sager oprettet i 2009 og 2008 samt enkelte fra tidligere. Opgørelsesmetoden skyldes et ønske om at opgøre tallene på en måde, så de ikke ændrer sig afhængig af, hvornår man opgør dem.

Forespørgsler	65,7 %
Ikke kategoriserede	20,6 %

Forespørgsler og klager vedrørende offentlige myndigheder
Datatilsynet registrerede i alt 508 nye sager med klager og forespørgsler vedrørende offentlige myndigheder.

Sagerne var fordelt således:

Statslige myndigheder	212
Regioner	24
Primærkommuner	144
Ansøgning om tilladelser	117
Diverse	11

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2009[4], var:

Klager	8,3 %
Forespørgsler	53,5 %
Ikke kategoriserede	38,2 %

Anmeldelser for den private sektor
Datatilsynet registrerede i alt 2.077 nye sager om anmeldelser for den private sektor. Fordelingen af sagerne var:

Forskning og statistik	1.256
Privates behandling af oplysninger om rent private forhold	580
Advarselsregistre	2
Spærrelister	1
Kreditoplysningsbureauer	0
Stillingsbesættende virksomheder	40
Edb-servicebureauer	23
Diverse sager af generel karakter	175

Anmeldelser for den offentlige forvaltning
Datatilsynet registrerede i alt 375 nye sager om anmeldelser for den offentlige sektor. Fordelingen af sagerne var:

4 Se note 3.

Fællesanmeldelser	3
Kommuner	58
Regioner	6
Statslige myndigheder	229
Tilslutninger, kommuner	79
Tilslutninger, regioner	0
Tilslutninger, statslige myndigheder	0
Diverse/sager af generel karakter	0

Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 170 nye sager oprettet på tilsynets eget initiativ. Fordelingen af sagerne var:

Inspektion og kontrol vedrørende private	62
Inspektion og kontrol vedrørende offentlige myndigheder	39
Sager rejst på grundlag af presseomtale og lign.	68
Diverse/sager af generel karakter	1

Sikkerhedsspørgsmål

Datatilsynet registrerede i alt 30 nye sager under kategorien sikkerhedsspørgsmål. Fordelingen af sagerne var:

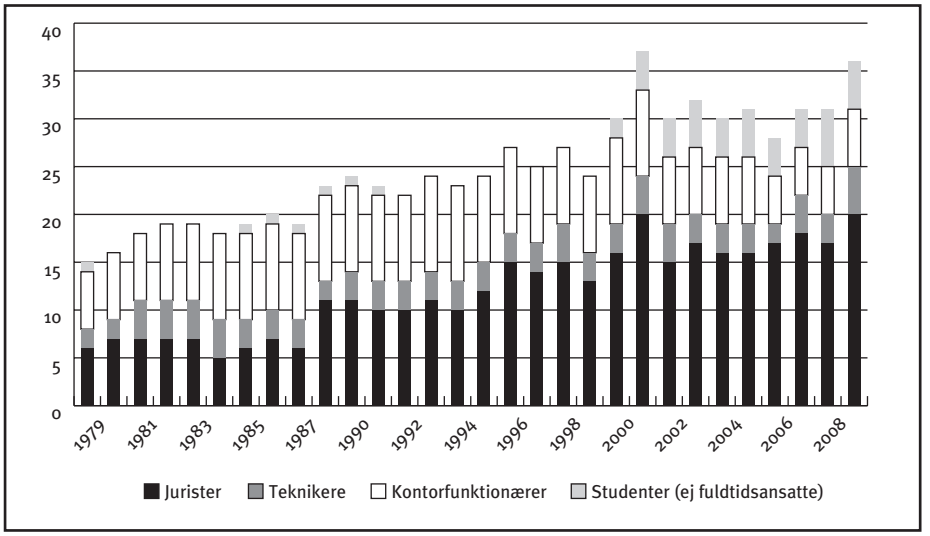
Private	15
Offentlige	13
Diverse	2

Internationale sager

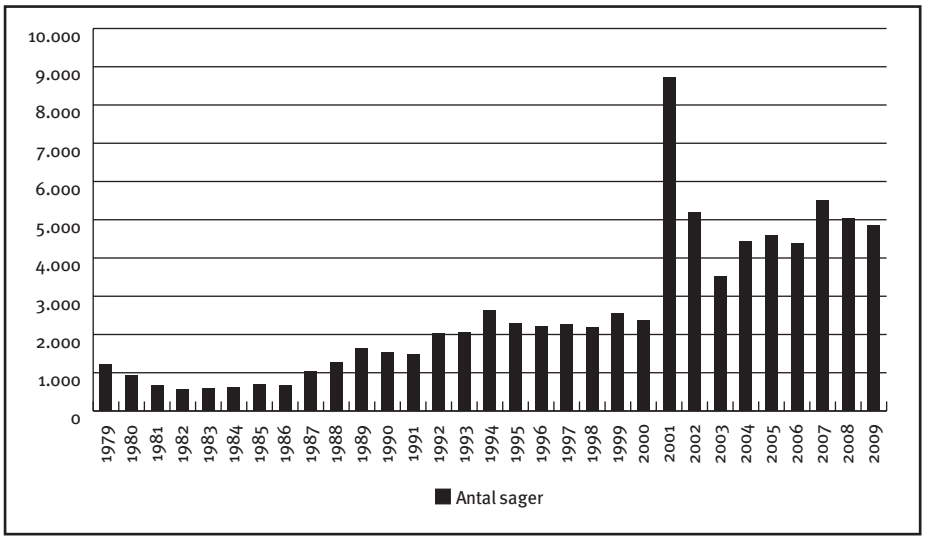
Datatilsynet registrerede i alt 157 nye internationale sager. Fordelingen af sagerne var:

Forespørgsler fra udlandet	74
Nordisk tilsynssamarbejde	5
Europarådet	9
EU	51
Datakommissærsamarbejdet	13
OECD	2
Diverse/sager af generel karakter	3

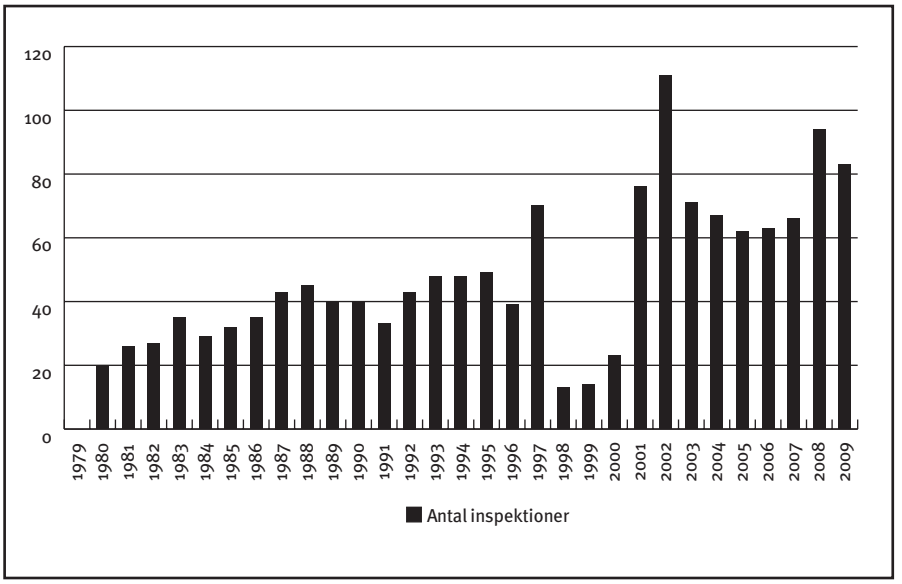
Personalesammensætning



Antal sager



Antal inspektioner



Udtalelser over lovforslag mv.

Ændring af apotekerloven og sundhedsloven

Ministeriet for Sundhed og Forebyggelse anmodede om Datatilsynets eventuelle bemærkninger til forslag til lov om ændring af apotekerloven og sundhedsloven.

Apoteksoplysninger om ordination af antipsykotika – forslagets § 1, nr. 2

Med en foreslået ændring i apotekerlovens bestemmelse i § 11, stk. 4, skulle der – udover den gældende adgang til videregivelse til Sundhedsstyrelsen af oplysninger om ordinationer af afhængighedsskabende lægemidler – etableres en adgang til videregivelse af oplysninger om ordinationer af antipsykotika.

Det fremgik af de almindelige bemærkninger, at adgang til apoteksdata om ordination af antipsykotika vil give Sundhedsstyrelsen – i tilsynssammenhæng – mulighed for et bredere og mere målrettet tilsyn med lægerne, som i sidste ende vil gavne patientsikkerheden blandt andet ved at reducere antallet af fejlmedicineringer.

I de specielle bemærkninger var bl.a. anført, at "Det er nødvendigt for Sundhedsstyrelsen entydigt at kunne identificere patienten med henblik på eventuelt senere at vurdere hensigtsmæssigheden af ordinationen i lyset af patientens fulde ordinationsbillede i Medicinprofilen."

Det fremgik endvidere, at de omhandlede apoteksdata kun skulle opbevares på cpr-nummerniveau i 3 måneder i Lægemiddelstyrelsen.

Forslaget gav efter Datatilsynets opfattelse anledning til betænkeligheder og rejste væsentlige spørgsmål i forhold til grundlæggende principper om nødvendighed og proportionalitet, jf. persondatalovens[5] § 5, som bygger på artikel 6 i databeskyttelsesdirektivet[6]. Datatilsynet henviste til, at der med forslaget tilsigtes opbygget et fuldstændigt register i Sundhedsstyrelsen over patienter, der har fået ordineret antipsykotika, med henblik på – som tilsynet havde forstået det – at føre stikprøvekontrol på området. De registrerede oplysninger var ifølge det anførte endvidere ikke underlagt de begrænsninger, f.eks. med hensyn til sletning, som gælder for oplysninger i Medicinprofilen og apoteksdata i Lægemiddelstyrelsen.

5 Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
6 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 fandt, at det meget nøje måtte overvejes, om det af hensyn til tilsynet med lægerne er nødvendigt og proportionalt at registrere alle patientoplysninger i umiddelbar personhenførbar form, når det må formodes kun at være i mindre omfang, der vil opstå behov for at vurdere patientens fulde ordinationsbillede. I givet fald må oplysningerne om det fulde ordinationsbillede for de relevante patienter kunne indhentes fra den pågældende læge.

Under henvisning til det anførte og til, at der er tale om de mest følsomme oplysninger, gav forslaget som nævnt Datatilsynet anledning til betænkeligheder i forhold til beskyttelsen af de registreredes privatliv.

Datatilsynet gjorde opmærksom på, at det er oplysningspligten i persondatalovens § 29, som skal iagttages ved behandlingen af de omhandlede apoteksdata. Bestemmelsen omhandler oplysningspligt i situationer, hvor oplysninger ikke er indsamlet hos den registrerede.

Det anførte om oplysningspligten i lovforslagets specielle bemærkninger måtte derfor genovervejes, herunder at information i pjecer mv. som udgangspunkt ikke opfylder oplysningspligten.

Datatilsynet gjorde tillige opmærksom på en problemstilling vedrørende logning og indsigt.

Det fremgik af de specielle bemærkninger, at "Ved enhver søgning af de registrerede oplysninger vil der blive foretaget en automatisk registrering (logning) af, hvem der har haft adgang til oplysningerne. Disse oplysninger vil kunne indhentes af medicinbrugeren hos den dataansvarlige."

Ved elektronisk indsigt i Medicinprofilen har de registrerede adgang også til den maskinelle registrering (logning) af alle anvendelser af de registrerede oplysninger. I denne situation gik Datatilsynet imidlertid ud fra, at der er tale om registreringer, hvor Sundhedsstyrelsen er dataansvarlig, og de registrerede vil således efter Datatilsynets opfattelse ikke have mulighed for indsigt som beskrevet i forslaget – medmindre en sådan adgang etableres.

Overbliksbilleder i Medicinprofilen

Med en foreslået ændring i sundhedslovens § 157, stk. 2, ønskedes adgangen til dannelse af overbliksbilleder i Den Personlige Elektroniske Medicinprofil (Medicinprofilen) udvidet. Med ændringen ville overbliksbillederne ikke længere være afgrænset til at vise lægemiddelbehandlingen af praktiserende lægers egne, fast tilknyttede patienter, men ville omfatte alle lægers lægemiddelordinationer til alle patienter, som den pågældende læge har udskrevet lægemidler til.

Baggrunden for udvidelsen var ifølge det anførte, at overbliksbillederne dels vil skulle fungere som et kvalitetsværktøj for ordinerende læger og dels vil skulle anvendes af Sundhedsstyrelsen i tilsynsøjemed.

Det var anført i forslagets almindelige bemærkninger, at patientsikkerhedsmæssige hensyn tilsiger, at såvel lægernes som Sundhedsstyrelsens adgang til overbliksbilleder bør være så bred som mulig.

Datatilsynet fandt, at de anførte patientsikkerhedsmæssige hensyn nøje måtte afbalanceres over for de registreredes privatliv henset til den meget følsomme karakter af oplysninger i Medicinprofilen.

Det forekom efter tilsynets opfattelse vidtgående at udvide anvendelsen af overbliksbilleder som foreslået, og det rejste væsentlige spørgsmål i forhold til grundlæggende principper om saglighed, nødvendighed og proportionalitet, jf. persondatalovens § 5.

Datatilsynet henviste til, at eksempelvis i situationer, hvor der er tale om enkeltstående ordination fra en læge, f.eks. ved konsultation hos en vagtlæge eller en vikarierende læge, forekommer det hverken nødvendigt eller proportionalt, at umiddelbart personhenførbare oplysninger om den pågældende patient indgår i overbliksbilleder hos vagtlægen eller den vikarierende læge.

Datatilsynet lagde herved også til grund, at ansvaret for opfølgning mv. i forhold til den pågældende ikke påhviler vagtlægen eller den vikarierende læge. Det var derfor Datatilsynets opfattelse, at de hensyn, som ønskedes tilgodeset med forslaget, vil kunne tilgodeses ved at stille anonymiserede oplysninger til rådighed for lægerne.

Hvis der var påtænkt en udvidelse af anvendelsen af overbliksbilleder, forudsatte tilsynet, at den generelle slettefrist på 2 år i Medicinprofilen også vil finde anvendelse for oplysninger, der indgår i overbliksbillederne.

Datatilsynet forudsatte, at kravet om logning også iagttages i forbindelse med overbliksbilleder, således at anvendelsen af oplysninger om den registrerede i overbliksbilleder er omfattet af den registreredes direkte elektroniske adgang til indsigt. Dette gælder også oplysninger om, hos hvem overbliksbilledet er anvendt.

De vedtagne lovændringer

Apotekerlovens § 11, stk. 4, fik følgende formulering:

”Lægemiddelstyrelsen kan til Sundhedsstyrelsen videregive alle oplysninger om ordination af afhængighedsskabende og antipsykotiske lægemidler, herunder oplysninger, der identificerer receptudstederen ved personnummer, ydernummer eller lignende, og oplysninger, der identificerer patienten ved personnummer, med henblik på Sundhedsstyrelsens vurdering af konkrete receptudstederes ordinationer.”

Af de endelige bemærkninger til lovforslagets punkt 3.2. vedrørende apotekerlovens § 11, stk. 4, fremgår det, at i forbindelse med udarbejdelse af et nyt register i Sundhedsstyrelsen er det hensigten at koordinere slettefristen i styrelsens nye register med slettefristen i Den Personlige Elektroniske Medicinprofil (PEM) således, at slettefristen i begge situationer er to år.

Sundhedslovens § 157, stk. 2, 2. pkt. fik følgende formulering:

”Alment praktiserende læger kan tillige benytte registeret til at finde egne patienter, der behandles uhensigtsmæssigt med lægemidler. Praktiserende speciallæger kan tillige benytte registeret til at finde patienter, som speciallægen har ordineret et eller flere lægemidler til, og som behandles uhensigtsmæssigt med lægemidler.”

Af de endelige bemærkningerne til den ændrede sundhedslovs § 157, stk. 2, 2. pkt. fremgår, at adgangen til overbliksbilleder dog vil være begrænset til de patienter, der er blevet behandlet af den praktiserende speciallæge inden for de sidste to år, da der gælder en slettefrist på to år for Medicinprofilen, jf. § 14 i bekendtgørelse nr. 990 af den 2. oktober 2006 om Lægemiddelstyrelsens register over Personlige Elektroniske Medicinprofiler.

Forslag til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse

Justitsministeriet anmodede om Datatilsynets bemærkninger til et forslag til en EU-rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse.

Datatilsynet bemærkede, at forslaget til rammeafgørelsen efter Datatilsynets opfattelse rejste væsentlige spørgsmål i relation til databeskyttelse.

De angivne formål med forslaget – at forebygge og bekæmpe terrorhandlinger og organiseret kriminalitet – var selvsagt saglige og anerkendelsesværdige.

Rammeafgørelsen ville imidlertid føre til indsamling og langvarig opbevaring af store mængder oplysninger vedrørende de omhandlede passagerer. Rammeafgørelsens formålsbestemmelser gav endvidere vide rammer for behandlingen af disse oplysninger, som også i stort omfang ville kunne udveksles mellem medlemsstaterne.

En nærmere begrundelse for, at indsamlingen og den efterfølgende analyse af passageroplysninger rent faktisk kunne bidrage til forebyggelse eller bekæmpelse af terrorhandlinger og organiseret kriminalitet fremgik ikke, og anvendelsen af PNR-oplysninger ville kunne føre til en uretmæssig mistænkeliggørelse af uskyldige mennesker.

Datatilsynet måtte på den baggrund stille sig tvivlende over for, om der var den fornødne proportionalitet mellem den behandling af passageroplysninger og opfyldelsen af de formål, der var beskrevet i forslaget. Datatilsynet henviste i den forbindelse også til en udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse.

Under henvisning til grundlæggende databeskyttelsesretlige principper om proportionalitet og nødvendighed fandt Datatilsynet derfor, at forslaget gav anledning til væsentlige betænkeligheder i forhold til beskyttelsen af de registreredes personers privatliv.

Datatilsynet fremhævede navnlig hensynet til, at man som almindelig borger kan foretage en rejse, uden at der sker en systematisk registrering, kortlægning og overvågning heraf.

På den baggrund var det Datatilsynets sammenfattende vurdering, at forslaget til rammeafgørelsen kun burde gennemføres, hvis vægtige samfundsmæssige hensyn talte herfor. Som påpeget ovenfor fandt Datatilsynet, at navnlig spørgsmålet om indgrebets proportionalitet i forhold til de registrerede personer burde give anledning til særlig overvejelse.

Det måtte efter Datatilsynets opfattelse bero på en politisk vurdering, om de samfundsmæssige hensyn, som forslaget tilsigtede at varetage, havde en sådan helt særlig karakter, at dette skulle gennemføres i sin daværende form.

Efter forslagets artikel 3, stk. 5, måtte PNR-oplysninger om passagerer kun behandles af medlemsstaternes passageroplysningsenheder og kompetente myndigheder for at forebygge eller bekæmpe terrorhandlinger og organiseret kriminalitet.

Især henvisningen til organiseret kriminalitet, som var defineret i forslagets artikel 2, litra i, gav efter Datatilsynets opfattelse vide rammer for anvendelsen af PNR-oplysninger.

Tilsynet henviste i den forbindelse til, at luftfartslovens § 148 a, stk. 2, alene foreskriver udlevering af passageroplysninger til PET til brug for forebyggelse og efterforskning af overtrædelse af straffelovens bestemmelser om forbrydelser

mod statens selvstændighed og sikkerhed (kapitel 12) og forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv. (kapitel 13).

Rammeafgørelsen ville medføre en opbevaring i 13 år af oplysninger om alle passagerer på fly, der var planlagt til at indflyve på mindst én EU-medlemsstats område, og som kom fra et tredjeland, eller som var planlagt til at lette fra mindst én EU-medlemsstats område med endeligt bestemmelsessted i et tredjeland, jf. forslagets artikel 9, stk. 1-3.

Datatilsynet fandt, at der var tale om en meget lang opbevaringsperiode, når henses til, at registreringen ville ske uden konkret begrundelse i den enkelte passagers forhold.

Af forslagets præambelbetragtning 9 fremgik, at det tidsrum, hvori de kompetente nationale myndigheder skulle opbevare PNR-oplysninger, burde stå i passende forhold til formålet hermed, nemlig at forebygge og bekæmpe terrorhandlinger og organiseret kriminalitet. Det anførtes endvidere, at på grund af oplysningernes art og anvendelsen af disse var det vigtigt, at de blev gemt tilstrækkeligt længe til, at de ville kunne anvendes til at udvikle risikoindikatorer og fastslå rejse- og adfærdsmønstre.

Datatilsynet fandt dog ikke, at det med disse bemærkninger i tilstrækkelig grad var begrundet, hvorfor en opbevaringsperiode på 13 år var nødvendig og forholdsmæssig.

Datatilsynet noterede sig i den forbindelse også, at det af Kommissionens høring af berørte parter, bl.a. fremgik, at der blandt disse var bred enighed om, at for at systemet kunne være effektivt, skulle oplysningerne opbevares i fem år, medmindre de blev anvendt til en strafferetlig undersøgelse eller efterretningsaktiviteter.

Datatilsynet fandt derfor, at opbevaringsperioden i hvert fald ikke burde overstige fem år. Tilsynet henviste endvidere til, at luftfartslovens § 148 a, stk. 1, alene foreskriver en etårig opbevaringsperiode.

Datatilsynet fandt, at der burde fastsættes klare regler om overførsel af passageroplysningerne til tredjelande, herunder om overførsel i forbindelse med anmodninger om gensidig adgang til PNR-oplysninger.

Datatilsynet fandt endvidere, at det gav anledning til tvivl, i hvilket omfang anvendelsesområdet for rammeafgørelsen om databeskyttelse ville dække behandlingen af personoplysninger i medfør af det foreliggende forslag til rammeafgørelse.

Ændring af persondataloven (gennemførelse af rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejder og retligt samarbejde i kriminalsager)

Justitsministeriet anmodede Datatilsynet om en udtalelse til udkast til lov om ændring af lov om behandling af personoplysninger (persondataloven) (Gennemførelse af EU-rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager).

Det fremgik af det fremsendte materiale, at Folketinget ved folketingsbeslutning af 10. juni 2008 havde meddelt sit samtykke til gennemførelse af EU-rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, jf. grundlovens § 19, stk. 1. Rammeafgørelsen var baggrunden for det omhandlede udkast til lovforslag.

Der blev foreslået indsat en ny bemyndigelsesbestemmelse i persondataloven, hvorefter justitsministeren vil kunne fastsætte nærmere administrative bestemmelser om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for Den Europæiske Union.

Datatilsynet noterede sig, at den foreslåede bemyndigelsesbestemmelse alene giver justitsministeren adgang til (inden for rammeafgørelsens anvendelsesområde) at fastsætte regler, som i overensstemmelse med rammeafgørelsen indebærer en yderligere styrkelse af databeskyttelsen, når det gælder udveksling af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for EU.

Indsættelse af en bemyndigelsesbestemmelse, som foreslået i lovudkastet, gav ikke i sig selv Datatilsynet anledning til bemærkninger.

På udvalgte punkter havde Justitsministeriet redegjort for sine foreløbige overvejelser om gennemførelsen af rammeafgørelsen, men det var i øvrigt anført, at Justitsministeriet vil tage endelig stilling i forbindelse med udformningen af selve bekendtgørelsen, og at et udkast til bekendtgørelsen vil blive forelagt for Datatilsynet til udtalelse, jf. persondatalovens § 57.

Det fremgik af bemærkningerne til lovforslaget, at de regler, som vil blive fastsat i henhold til den foreslåede bemyndigelsesbestemmelse, også vil omfatte databeskyttelse i forbindelse med danske myndigheders politimæssige og strafferetlige samarbejde med de tredjelande, der deltager i Schengen-samarbejdet (for tiden Island, Norge, Schweiz og Liechtenstein), jf. i den forbindelse udtrykket "mv." i den foreslåede nye § 72 a.

Datatilsynet gik ud fra, at der med denne bemærkning sigtes til politimæssigt og strafferetligt samarbejde **ud over det**, som foregår med bl.a. disse lande inden for Schengen-konventionen. Datatilsynet lagde således til grund, at samarbejdet inden for bl.a. Schengen og Europol ikke berøres af rammeafgørelsen, men fortsat reguleres af de særlige bestemmelser på disse områder. Datatilsynet

henviste herved til præampelbetragtning (39), hvoraf fremgår, at adskillige EU-retsakter indeholder specifikke bestemmelser om beskyttelse af personoplysninger, og at navnlig bestemmelserne om Europols, Eurojusts, Schengeninformationssystemets (SIS) og toldinformationssystemets (CIS) funktionsmåde samt de bestemmelser der giver medlemsstaternes myndigheder direkte adgang til datasystemer i visse andre medlemsstater, ikke bør berøres af rammeafgørelsen.

For at skabe klarhed over anvendelsesområdet for rammeafgørelsen foreslog Datatilsynet, at det i bemærkningerne til lovforslaget blev præciseret, hvorledes forholdet til bestemmelserne om Europol, Eurojust, Schengen-informationssystemet (SIS) og toldinformationssystemet (CIS) er.

Det fremgår af rammeafgørelsens artikel 2, litra h), at de "kompetente myndigheder" i medlemsstaterne er politi, toldvæsen, retslige myndigheder og andre kompetente myndigheder, der i henhold til national lov har beføjelse til at behandle personoplysninger inden for denne rammeafgørelses anvendelsesområde.

Det fulgte af de generelle bemærkninger, afsnit 4.2.2.4., at rammeafgørelsen indeholder særlige regler om adgangen for danske myndigheder (dvs. politi, anklagemyndighed, kriminalforsorg og domstole) til at viderebehandle personoplysninger, som modtages fra eller stilles til rådighed af myndigheder i andre medlemsstater.

Det stod ikke umiddelbart Datatilsynet klart, om oplistningen af de pågældende danske myndigheder er udtømmende. Tilsynet fandt det hensigtsmæssigt, at det af lovforslaget kom til at fremgå, hvilke danske myndigheder der er "kompetente myndigheder" og derved kan behandle personoplysninger i medfør af de foreslåede regler.

For så vidt angår behandling af oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssigt tilhørsforhold samt oplysninger om helbredsforhold eller seksuelle forhold, anførte Justitsministeriet, at rammeafgørelsen (i princippet) fastsætter strengere betingelser for, hvornår danske myndigheder kan behandle sådanne personoplysninger, end hvad der i dag følger af persondatalovens § 7.

Justitsministeriet bemærkede dog, at det i praksis formentlig ikke vil være muligt at angive nogen væsentlig forskel på kriterierne "nødvendigt" og "strengt nødvendigt". Det gælder således bl.a. i relation til politiets mv. adgang til at behandle de nævnte typer af følsomme personoplysninger med henblik på kriminalitetsbekæmpelse, f.eks. i forbindelse med opklaring af et politisk motiveret mord.

Datatilsynet henledte i den forbindelse opmærksomheden på den særlige bestemmelse i persondatalovens § 7, stk. 8, hvoraf det følger, at der for den offentlige forvaltning ikke må føres edb-registre med oplysninger om politiske forhold, som ikke er offentligt tilgængelige.

De begrænsninger, som følger af § 7, stk. 8, vil efter tilsynets vurdering navnlig være aktuelle i forbindelse med, at de kompetente myndigheder efter rammeafgørelsens artikel 10 er forpligtet til at registrere, hvilke oplysninger der er blevet videregivet til udenlandske myndigheder.

Dette indebærer efter Datatilsynets vurdering, at der i forbindelse med behandling af sager om politisk motiveret kriminalitet registreres oplysninger om politiske forhold omfattet af § 7, stk. 8, i forbindelse med førelsen af den påkrævede fortegnelse over, hvilke oplysninger der videregives.

Datatilsynet anbefalede på denne baggrund, at Justitsministeriet overvejer bestemmelsen i persondatalovens § 7, stk. 8, i forhold til de oplysninger, der registreres som følge af rammeafgørelsen.

Det fremgik bl.a. af afsnit 4.2.4.4. i lovforslagets bemærkninger, at den registrerede i medfør af rammeafgørelsens artikel 18 har ret til at forvente, at den dataansvarlige myndighed overholder sine forpligtelser vedrørende berigtigelse, sletning og blokering (eller at der eventuelt sker "referenceangivelse"). Den registrerede skal kunne gøre denne rettighed gældende direkte over for den dataansvarlige *eller* gennem den nationale tilsynsmyndighed.

Det fremgik endvidere, at gennemførelsen af rammeafgørelsens artikel 18 i dansk ret efter Justitsministeriets opfattelse må antages at nødvendiggøre en ændring af den gældende retstilstand. Der fremgik dog ikke yderligere herom, idet de nærmere regler vil blive fastsat i den bekendtgørelse, som Justitsministeriet vil udstede.

Datatilsynet ville finde det hensigtsmæssigt, at det af selve lovforslaget kom til at fremgå, hvorledes den registrerede skal udøve sine rettigheder. Datatilsynet ville dermed også få mulighed for at vurdere, hvorvidt tilsynet påføres opgaver ud over de nuværende, samt hvilket omfang sådanne nye opgaver måtte have.

For så vidt angår behandlingssikkerheden anførtes det bl.a. i bemærkningerne, afsnit 4.2.5., at rammeafgørelsens bestemmelser om behandlingssikkerhed i artikel 21 og 22 i vidt omfang svarer til reglerne i persondatalovens kapitel 11 med tilhørende bekendtgørelser.

Det anførtes imidlertid endvidere, at der formentlig vil være behov for visse ændringer af de administrativt fastsatte regler om behandlingssikkerhed.

Det stod ikke umiddelbart Datatilsynet klart, hvilke administrativt fastsatte regler Justitsministeriet finder behov for at ændre, og hvorledes det vil påvirke Datatilsynets tilsynsopgaver.

Datatilsynet foreslog endvidere, at Justitsministeriet i det videre arbejde overvejer forholdet mellem den foreslåede bekendtgørelse og den regulering, som følger af kriminalregisterbekendtgørelsen. Kriminalregisterbekendtgørelsen indeholder således bestemmelser om indsigt, videregivelse af oplysninger til udenlandske myndigheder samt behandlingssikkerhed.

Med hensyn til det nærmere indhold i den foreslåede bekendtgørelse måtte Datatilsynet forbeholde sin stillingtagen i forbindelse med høringen over et udkast dertil.

Det anførtes i bemærkningerne, afsnit 5, at lovforslaget ikke skønnes at have økonomiske eller administrative konsekvenser for det offentlige af betydning.

Under henvisning til, at det i lovforslaget understreges, at rammeafgørelsen indebærer en styrkelse af databeskyttelsen, og at der er tale om et helt særskilt regelsæt, som skal administreres, udtrykte Datatilsynet som sin forventning, at tilsynet tilføres yderligere ressourcer. Datatilsynet lagde derfor afgørende vægt på, at tilsynets ressourcemæssige situation indgik i de videre overvejelser om gennemførelse af rammeafgørelsen.

Da rækkevidden af rammeafgørelsen endnu ikke var afklaret på en række punkter, jf. ovenfor, fandt Datatilsynet det på daværende tidspunkt vanskeligt at vurdere det nærmere omfang af rammeafgørelsens konsekvenser for tilsynet. Datatilsynet tog derfor forbehold for en nærmere drøftelse i det videre forløb af spørgsmålet om ressourcer.

Internationalt arbejde

Indledning

Som beskrevet i tidligere årsberetninger, senest i Datatilsynets Årsberetning for 2007, har der siden 1979 – men især fra 1989 – udviklet sig et omfattende regelsæt på databeskyttelsesområdet, som har fået stadig større betydning for Datatilsynets arbejde. På Datatilsynets hjemmeside er de regelsæt, som nærmere vil blive omtalt, tilgængelige via link under "Internationalt".

Den væsentligste ældre konvention på området er Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, som trådte i kraft i 1985. Forud herfor var i september 1980 fremkommet OECDs internationalt dækkende Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, som indeholder en række hovedprincipper for persondatabeskyttelse, og som har størst betydning for de lande, der ikke har ratificeret Europarådskonventionen.

Særligt afgørende har dog været udviklingen inden for EU med vedtagelse af direktiver gældende for det indre marked (søjle I-området), bl.a. det generelle databeskyttelsesdirektiv, men også – afledt af det stigende europæiske samarbejde mellem kontrollerende myndigheder i de enkelte EU-medlemsstater (politi, toldvæsen og asylmyndigheder) – vedtagelse af en række konventioner, som efterhånden er blevet inddraget under EU, og som er omfattet af Amsterdamtraktatens 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 myndighedskontrol.

Folketinget meddelte ved folketingsbeslutning af 10. juni 2008 sit samtykke til gennemførelse af EU-rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, jf. grundlovens § 19, stk. 1.

Den 27. november 2008 blev Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager vedtaget. Formålet med rammeafgørelsen er at sikre en høj grad af beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder, herunder navnlig deres ret til privatlivets fred for så vidt angår behandlingen af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, jf. afsnit VI i traktaten om Den Europæiske Union, og samtidig sikre en høj grad af offentlig sikkerhed.

Af rammeafgørelsen artikel 2 følger, at medlemsstaterne i overensstemmelse med denne rammeafgørelse beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder og navnlig deres ret til privatlivets fred, når personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner:

a) videregives eller er videregivet eller stilles til rådighed eller er stillet til rådighed mellem medlemsstater
b) videregives eller er videregivet eller stilles til rådighed eller er stillet til rådighed af medlemsstater for myndigheder eller informationssystemer, der er oprettet på grundlag af afsnit VI i traktaten om Den Europæiske Union, eller
c) videregives eller er videregivet eller stilles til rådighed eller er stillet til rådighed for de kompetente myndigheder i medlemsstaterne af myndigheder eller informationssystemer, der er oprettet på grundlag af traktaten om Den Europæiske Union eller traktaten om oprettelse af Det Europæiske Fællesskab.

På baggrund af rammeafgørelsen blev der indsat en bemyndigelsesbestemmelse i persondatalovens § 72 a, hvorefter justitsministeren vil kunne fastsætte nærmere administrative bestemmelser om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for Den Europæiske Union. Datatilsynets bemærkninger til ændringen er beskrevet under udtalelser over lovforslag.

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

Nedenfor gives en kort beskrivelse af det formelle grundlag for tilsynets aktiviteter på det internationale område, suppleret med oplysninger om de væsentligste sager, som tilsynet har beskæftiget sig med i 2008 og 2009. 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 TP-D) og Databeskyttelsesekspertgruppen (CJ-PD) på grund af manglende økonomiske ressourcer har TP-D fortsat CJ-PDs arbejde.

TP-D 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. Danmark har underskrevet tillægsprotokollen.

Datatilsynet deltog i foråret 2008 og i efteråret 2009 i Den Rådgivende Komité TP-D´s plenarmøde.

Europarådets hjemmeside kan findes via et link fra Datatilsynets hjemmeside.

Den Europæiske Union

Europol-konventionen

Euopol-samarbejdet var oprindeligt baseret på konventionen af 26. juli 1995 om oprettelse af en europæisk politienhed (Europol-konventionen). Danmark gennemførte konventionen ved lov nr. 415 af 10. juni 1997, som trådte i kraft den 1. juli 1999. Senere blev der gennemført ændringer af konventionen ved lov nr. 1435 af 22. december 2004, der bl.a. gennemførte 3 protokoller til ændring af Europol-konventionen. Det drejer sig om Rådets retsakt af 30. november 2000 (EFT 2000 C 358/1), Rådets retsakt af 28. november 2002 (EFT 2002 C 312/1) samt Rådets retsakt af 27. november 2003 (EUT 2004 nr. 2/3). Gennemførelsen af de 2 første protokoller trådte i kraft den 29. marts 2007, mens ikrafttrædelsesdatoen for den 3. protokol var den 18. april 2007, jf. bekendtgørelse nr. 165 af 8. februar 2007.

Senest er der gennemført ændringer i retsgrundlaget i form af Rådets afgørelse af 6. april 2009 om oprettelse af en europæisk politienhed (Europol). Formålet med forslaget er at erstatte den nuværende Europol-konvention med en rådsafgørelse. Dette vil medføre en række ændringer med hensyn til Europols organisering, finansiering, mandat, databeskyttelse mv. Forslaget betyder ændringer i Europol-loven. Rådsafgørelsen træder i kraft 1. januar 2010 og er gennemført i Danmark ved lov nr. 1261 af 16. december 2009 (europol-loven).

Europol-loven gennemfører Rådsafgørelsen om Den Europæiske Politienhed (Europol) i Danmark. Europol er et EU-samarbejde, der især beskæftiger sig med den grove og grænseoverskridende kriminalitet i EU - f.eks. organiseret kriminalitet og terrorisme. Europol skal bl.a. støtte de enkelte landes myndigheder i deres samarbejde over grænserne.

Målet med Rådsafgørelsen er at skabe en mere tidssvarende lovgivning. Rigspolitiet er stadig den nationale enhed, jf. Rådsafgørelsens artikel 8, jf. europol-lovens § 2, og Datatilsynet er fortsat den nationale kontrolinstans, jf. Rådsafgørelsens artikel 33, jf. europol-lovens § 3. Europa-Parlamentets kontrol med Europol styrkes med Rådsafgørelsen.

Rådsafgørelsen erstatter Europol-konventionen, jf. Rådsafgørelsens artikel 1.

Datatilsynet har haft lovudkast vedrørende Den Europæiske Politienhed i høring, og dette gav ikke anledning til særlige bemærkninger. Datatilsynet bemærkede dog, at der siden 1995 er foretaget flere ændringer af retsgrundlaget for Europol, hvorved der lægges op til et intensiveret samarbejde inden for et stadig bredere kompetenceområde og dermed også til øget udveksling af personoplysninger. Datatilsynet fandt det i den forbindelse ikke muligt inden for de nuværende bevillingsmæssige rammer at afsætte yderligere ressourcer til tilsyn med Europol-området. Datatilsynet anmodede i øvrigt om at blive inddraget i drøftelser om nye tiltag i forbindelse med gennemførelse af rådsafgørelsen, f.eks. hvis andre myndigheder skal have direkte kontakt til Europol eller adgang til at søge i Europols informationssystem.

Efter Justitsministeriets opfattelse vil Datatilsynet – som national kontrolinstans – ikke med rådsafgørelsen blive pålagt yderligere kontrolopgaver i forhold til, hvad der er gældende i dag efter Europol-konventionen. Justitsministeriet vil imidlertid være opmærksom på udviklingen og vil i givet fald træffe de nødvendige foranstaltninger med henblik på at sikre, at Datatilsynet kan udføre den fornødne kontrol indenfor Europol-området. Justitsministeriet har ikke fundet, at der er behov for at ændre den eksisterende ordning, hvorefter alene Rigspolitiet har direkte kontakt med Europol. Hvis der imidlertid senere viser sig behov herfor, vil Justitsministeriet drøfte dette spørgsmål nærmere med de berørte parter, herunder i fornødent omfang med Datatilsynet.

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: Der føres tilsyn med den europæiske politienhed Europol, som fysisk er placeret i Haag, og hvis virksomhed formelt påbegyndtes den 1. juli 1999. Dette tilsyn varetages af Den Fælles Kontrolinstans, og hertil knytter sig Det Fælles Klageudvalg, jf. Europol-konventionens artikel 24 (Rådsafgørelsens artikel 34), som skal behandle konkrete klager. Datatilsynet er repræsenteret ved 2 medlemmer i Den Fælles Kontrolinstans, hvoraf 1 medlem er indtrådt i Det Fælles Klageudvalg.

Den Fælles Kontrolinstans har i 2008 afholdt 4 møder, hvor man bl.a. har drøftet det nye retsgrundlag for Europol, it-projekter i regi af Europol, en oplysningsbrochure og kontrolinstansens 3. aktivitetsrapport (perioden november 2004 til oktober 2006).

Den Fælles Kontrolinstans har igen i 2009 afholdt 4 møder, hvor man udover det nye retsgrundlag for Europol bl.a. har drøftet inspektionen af Europol, der blev foretaget den 3.-6. marts 2009. Der fandtes generelt ingen særlige persondataretlige problemer under inspektionen. Der blev endvidere drøftet operationelle aftaler med tredjelande, som Europol ønsker at indgå i et samarbejde med.

Udtalelserne fra Den Fælles Kontrolinstans kan findes på kontrolinstansens hjemmeside http://europoljsb.consilium.europa.eu/default.

Det Fælles Klageudvalg har i 2008 afholdt 4 møder og 2 møder i 2009. Klageudvalgets afgørelser kan findes på Den Fælles Kontrolinstans' hjemmeside.

Den Fælles kontrolinstans for Europol har udgivet den fjerde aktivitetsrapport for den fælles kontrolinstans vedrørende årene 2006-2008. Rapporten kan findes på Datatilsynets hjemmeside under Internationalt.

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, lov nr. 448 af 9. juni 2004 og senest ved lov nr. 521 af 6. juni 2007.

Retsgrundlaget for anden generation af Schengen-informationssystemet (SIS II) kom på plads i 2007 med Rådets vedtagelse den 12. juni 2007 af rådsafgørelsen om oprettelse, drift og brug af SIS II. Forordningen om oprettelse, drift og brug af SIS II samt forordningen om adgang til SIS II for de tjenester i medlemsstaterne, der har ansvaret for udstedelse af registreringsattester for motorkøretøjer, vedtog Rådet allerede den 20. november 2006.

Ved lov nr. 521 af 6. juni 2007 er justitsministeren bl.a. bemyndiget til at fastsætte ikrafttrædelsestidspunktet (§ 2, stk. 2) for lovens bestemmelse om, at bestemmelserne i rådsafgørelsen og forordningen om oprettelse, drift og brug af anden generation af SIS II gælder i Danmark. Justitsministeren har endnu ikke fastsat et sådant ikrafttrædelsestidspunkt.

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 Datatilsynet deltaget i møderne som medlem.

Den Fælles Tilsynsmyndighed Schengen har i 2008 afholdt 4 møder. Tilsynsmyndigheden har i samarbejde med Schengen-landene bl.a. foretaget visse fælles undersøgelser af landenes brug af artiklerne 97 og 98 i Schengen-konventionen. De endelige rapporter herom blev vedtaget den 13. oktober 2009. Tilsynsmyndigheden har i 2008 desuden bl.a. haft fokus på spørgsmål om samarbejdet mellem de nationale datatilsyn.

Den Fælles Tilsynsmyndighed Schengen har i 2009 afholdt 3 møder. Tilsynsmyndigheden har i samarbejde med Schengen-landene bl.a. haft fokus på opfølgende undersøgelser af landenes brug af artiklerne 96 og 99.

I forbindelse med Datatilsynets opfølgende undersøgelse af den danske brug af Schengen-konventionens art. 96 og 99 foretog tilsynet i oktober 2009 en stikprøvekontrol af de danske indberetninger.

Tilsynsmyndigheden har i samarbejde med Schengen-landene udarbejdet *a guide for exercising the right of acces*, som er oversat til alle officielle sprog. Tilsynsmyndigheden har i 2009 desuden haft fokus på den planlagte overgang til SIS II.

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. Konventionen trådte i kraft den 23. december 2005.

Arbejdsopgaver: I henhold til konventionens artikel 17 skal medlemsstaterne udpege en national tilsynsmyndighed med ansvar for beskyttelse af personoplysninger. Datatilsynet er af Skatteministeriet blevet anmodet om at påtage sig opgaven som national tilsynsmyndighed, og tilsynet har givet ministeriet tilsagn herom.

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.

Den Fælles Tilsynsmyndighed Toldinformationssystemet har i 2008 afholdt 4 møder og har bl.a. drøftet udviklingen af en audit model, som kan anvendes ved undersøgelse af datasikkerheden i medlemsstaterne.

Den Fælles Tilsynsmyndighed Toldinformationssystemet har i 2009 afholdt 3 møder og har bl.a. haft fokus på evaluering af medlemsstaternes brug af CIS. Tilsynsmyndigheden har udarbejdet et selvevalueringsskema, der skal sendes til de nationale myndigheder i 2010.

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
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 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 blev ophævet 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 nævnte 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: 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.

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 er imidlertid blevet tilknyttet Eurodac-systemet på mellemstatsligt grundlag.

Formålet med Eurodac-forordningen er at fastlægge regler for oprettelse af en elektronisk database af fingeraftryk af asylansøgere og visse andre personer til brug ved anvendelsen af Dublin-konventionen, der 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 er i overensstemmelse med Eurodac-forordningen.

Af udlændingelovens § 58 c, stk. 3, 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.

I 2008 blev der i Eurodac afholdt 3 møder, hvor der bl.a. var fokus på udarbejdelsen af to spørgeskemaer, der omhandler (1) information til de registrerede i Eurodac-systemet og (2) procedurerne for at finde ud af, hvorvidt en asylansøger opfylder det aldersmæssige krav for registrering i Eurodac.

I 2009 blev der i Eurodac afholdt 3 møder, hvor den 2. inspektionsrapport bl.a. blev drøftet. Inspektionsrapporten blev vedtaget den 24. juni 2009. Rapporten er offentliggjort på EDPS' hjemmeside: http://www.edps.europa.eu/EDPSWEB/edps/Home/Supervision/Eurodac.

Det generelle databeskyttelsesdirektiv
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 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 kommitéprocedure, 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 fra den eller de tilsynsmyndigheder, som hver medlemsstat har udpeget, af en repræsentant fra den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og –organisationerne, samt af en repræsentant fra Kommissionen. Kommissionen (Generaldirektoratet for Frihed, Sikkerhed og Retfærdighed) er sekretariat for gruppen.

Artikel 29-gruppen har i 2008 og 2009 afholdt 3 to-dagsmøder og 2 en-dagsmøder. Datatilsynet har desuden deltaget i to underarbejdsgrupper, "Technology Subgroup", som særligt arbejder med beskyttelse af personoplysninger i forbindelse med anvendelse af internet og anden ny teknologi, samt "BCR" undergruppen som arbejder med Binding Corporate Rules (BCR).

Artikel 29-gruppen har i 2008 og 2009 vedtaget en række henstillinger, udtalelser mv.

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-institutionerne
Forordningens navn: EU-Parlamentets og Rådets forordning (EU) 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 (EU-Tidende nr. L 8 af 12/1/2001, s.1).

Ikrafttrædelse: Ifølge artikel 51 træder forordningen i kraft på 20. dagen efter offentliggørelsen den 12. januar 2001 i EU-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" 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, jf. 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.

Senest ved Europaparlamentet og Rådets afgørelse af 14. januar 2009 blev nederlænderen Peter Johan Hustinx udpeget til europæisk tilsynsførende for databeskyttelse for en femårig periode.

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

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

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

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

Arbejdsopgaver: I henhold til Eurojust-afgørelsens artikel 23 oprettes der en fælles kontrolinstans til overvågning af Eurojusts aktiviteter med henblik på at sikre, at disse aktiviteter finder sted i overensstemmelse med Eurojust-afgørelsens bestemmelser vedrørende datasikkerhed. Forretningsordenen for den fælles kontrolinstans blev vedtaget i 2004 og ændret i 2009. Instansen har siden 2004 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.

EU-datakommissærernes arbejde

Alle EUs medlemsstater har nu lovgivning om persondatabeskyttelse. Der er i Datatilsynets årsberetning 1996, side 18-20, redegjort for samarbejdet mellem EU-datatilsynene, der dog i nogen grad har ændret indhold, efter at der afholdes regelmæssige møder i Artikel 29-gruppen. Samarbejdet foregår fortsat ved afholdelse af en årlig konference samt et møde, som afholdes i forbindelse med den årlige internationale konference. I 2008 blev den årlige EU-datatilsynskonference afholdt i Rom af det italienske datatilsyn, og i 2009 blev konferencen holdt i Edinburgh af det engelske datatilsyn. På konferencerne blev en række spørgsmål af fælles interesse drøftet, bl.a. beskyttelse af personoplysninger ved kontrol ved EU´s grænser og aftale mellem EU-lande og tredjelande på området for politi- og retlig samarbejde.

Datatilsynet har i 2008 og 2009 deltaget i 8 møder i arbejdsgruppen Working Party on Police and Justice (WPPJ). Denne arbejdsgruppe undersøger udviklingen inden for det strafferetlige område med særlig fokus på databeskyttelsesretlige problemstillinger. WPPJ forbereder forslag, udkast til skrivelser mv. til konferencerne med henblik på fremsendelse til EU-institutioner og andre interessenter.

WPPJ har i 2008 haft særlig fokus på søjleproblematikken i relation til Lissabontraktaten. WPPJ har i 2009 udover søjleproblematikken bl.a. haft fokus på den

teknologiske udvikling i relation til biometri og anvendelsen heraf inden for det strafferetlige område.

International konference for databeskyttelsesmyndigheder mv.

Det 30. årlige internationale møde for datatilsynsmyndighederne blev i oktober 2008 afholdt i Strasbourg, Frankrig. På konferencen blev der vedtaget flere resolutioner bl.a. en om databeskyttelse hos sociale netværk og en om børns online privacy. I november 2009 blev det 31. møde afholdt i Madrid, Spanien, her blev bl.a. vedtaget en resolution om internationale standarder for beskyttelse af personoplysninger og privacy. Resolutionerne findes på Datatilsynets hjemmeside under Internationalt, Konferencer.

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, som den omtales, 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

Datatilsynet deltog i 2008 i det fællesnordiske sagsbehandlermøde, som blev holdt i Stockholm. På mødet udvekslede deltagerne erfaringer om såvel generelle som konkrete spørgsmål, bl.a. tv-overvågning, internettet og digital forvaltning. Datatilsynet deltog også i 2009 i det fællesnordiske sagsbehandlermøde, der foregik på Færøerne. På mødet blev bl.a. sociale netværk og overvågning behandlet.

Der afholdes nordisk datachefmøde hvert andet år. Der var ikke et møde i 2008. Datatilsynet deltog i 2009 i det nordiske datachefmøde i Stockholm. På mødet blev en række emner drøftet, bl.a. sociale netværk, beskyttelse af personoplysninger på arbejdspladsen, nye lovgivningstendenser og børn og unges adfærd på internettet mv.

Sikkerhedsspørgsmål

Persondatalovens krav til datasikkerhed

I medfør af persondatalovens § 41, stk. 5, 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 på tilsynets hjemmeside: 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 ligeledes på Datatilsynets hjemmeside. Både bekendtgørelsen og vejledningen retter sig mod behandling af personoplysninger, som foretages for den offentlige forvaltning. For oplysninger, der behandles i den private sektor, gælder umiddelbart persondatalovens § 41, stk. 3.

Som nævnt tidligere fastsatte Datatilsynet i 2008 nye sikkerhedskrav i relation til private virksomheders overførsel af personoplysninger via internettet. Ved fastsættelsen af kravene og anbefalingerne skelnes der mellem kommunikation via hjemmesider og kommunikation via e-mail.

Datatilsynet stiller herefter udtrykkeligt krav om kryptering ved overførsel af følsomme oplysninger og oplysning om personnummer via hjemmesider samt i tilfælde, hvor behandlingen af personoplysninger i den private sektor sker efter tilladelse med vilkår om konkrete sikkerhedsforanstaltninger ved transmission over internet.

I en række andre situationer anbefaler Datatilsynet, at personoplysninger beskyttes, når de overføres via internet.

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

Datatilsynet har med bekymring konstateret en stigning i antallet af sikkerhedsbrister hos både private virksomheder og offentlige myndigheder i forbindelse med behandling af personoplysninger. En række sikkerhedsbrister på flere danske universiteter, hvorved bl.a. personnumre, navne og i visse tilfælde

helbredsoplysninger er offentliggjort, har været særligt bekymrende og givet Datatilsynet anledning til at udtale kritik.

Universiteters utilsigtede offentliggørelse af personoplysninger på internet og intranet

I 2008 og 2009 erfarede Datatilsynet, at danske universiteter i flere tilfælde ved fejl ikke havde overholdt kravene i persondatalovens § 41, stk. 3, i forbindelse med offentliggørelse af personoplysninger på internettet eller intranet.
Det følger af lovens § 41, stk. 3, 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.

Nedenfor er kort omtalt fem sager, hvor utilsigtet offentliggørelse af personoplysninger fandt sted:

1. Danmarks Tekniske Universitets (DTU) havde ved en fejl på sin hjemmeside offentliggjort en PowerPoint-præsentation indeholdende personoplysninger. PowerPoint-præsentationen indeholdt en indlejret Excel-fil med oplysninger om personnumre og helbredsoplysninger på 10 personer.

Datatilsynet udtalte bl.a., at DTU ikke havde udvist den fornødne omhu, og at DTU dermed ikke havde overholdt kravene i persondatalovens § 41, stk. 3. Datatilsynet fandt det passerede meget beklageligt (Datatilsynets j.nr. 2008-632-0035).

2. IT-Universitetet i København (ITU) havde ved en fejl ikke spærret for offentlig adgang via internettet til et internt system, der holder styr på fejl/mangler i it-systemer på ITU. Ved en yderligere menneskelig fejl indeholdt systemet desuden personnumre og navne på 17 personer, som derved blev eksponeret på internettet.

Datatilsynet udtalte bl.a., at ITU ikke havde udvist den fornødne omhu. ITU havde dermed ikke overholdt kravene i persondatalovens § 41, stk. 3. Datatilsynet fandt det skete kritisabelt og fandt anledning til understrege vigtigheden af, at ITU fremover ved anskaffelse og udvikling af nye it-systemer sikrer sig, at kravene i persondataloven og sikkerhedsbekendtgørelsen iagttages, herunder at der er truffet de fornødne sikkerhedsforanstaltninger (Datatilsynets j.nr. 2009-311-0180).

3. Københavns Universitet havde offentliggjort bl.a. personnumre på 25 studerende på en holdliste, der var frit tilgængelig via internettet. Holdlisten, der indeholdt maskerede personnumre, var lagret som en pdf-fil. Ved konvertering af pdf-filen til et andet format forsvandt maskeringen af personnumrene imidlertid. Forinden havde Datatilsynet den 22. januar 2009 afgivet udtalelse i anledning af en lignende sikkerhedsbrist hos Københavns Universitet.

Datatilsynet udtalte bl.a., at Københavns Universitet ikke havde udvist den fornødne omhu. Universitetet har dermed ikke overholdt kravene i persondatalovens § 41, stk. 3. Datatilsynet fandt i lyset af den forudgående sikkerhedsbrist hos Københavns Universitet det passerede meget beklageligt.

Datatilsynet pegede på muligheden for at begrænse anvendelsen af fortrolige personoplysninger - herunder personnumre - således at disse oplysninger slet ikke er tilgængelige for andre end nogle få centrale medarbejdere og således at der f.eks. anvendes et studienummer, som ikke er identisk med den studerendes personnummer. Herudover foreslog Datatilsynet, at Københavns Universitet overvejer at etablere en teknisk løsning, der holder øje med fortrolige oplysninger (navnlig personnumre) og blokerer for offentliggørelsen af disse.

Datatilsynet rettede efterfølgende henvendelse til Ministeriet for Videnskab, Teknologi og Udvikling i anledning af denne og lignende sager med sikkerhedsbrister på andre universiteter (Datatilsynets j.nr. 2009-632-0046).

4. Copenhagen Business School (CBS) videregav på sit intranet personoplysninger i form af bl.a. fulde navne og personnumre på ca. 110 studerende.

Datatilsynet udtalte bl.a., at CBS ikke har udvist den fornødne omhu. Datatilsynet havde tidligere, i en sag hvor CBS lagde oplysninger om studerendes personnumre på CBS' intranet, udtalt at det dengang passerede var meget beklageligt. I den anledning udtalte CBS, at CBS ville udarbejde en vejledning og en handlingsplan til sikring af, at alle medarbejdere modtager den fornødne instruktion. Dette havde CBS imidlertid ikke gjort.

På denne baggrund fandt Datatilsynet det gentagne brud på persondatalovens § 41, stk. 3 kritisabelt. Datatilsynet rettede efterfølgende henvendelse til Ministeriet for Videnskab, Teknologi og Udvikling i anledning af denne og lignende sager med sikkerhedsbrister på andre universiteter (Datatilsynets j.nr. 2008-216-0253)

5. Aalborg Universitet havde ved en fejl offentliggjort oplysninger om personnumre på studerende på universitetets hjemmeside. Oplysningerne fandtes i en Excel-database, der som sådan var offentliggjort. I dette tilfælde var der således ikke tale om, at oplysningerne lå gemt som en indlejret fil i en PowerPoint-præsentation. Oplysningerne vedrørte 82 studerende, og omfattede personnumre, navne, studieretning, semester, telefonnumre og e-mailadresser. Under Datatilsynets behandling af sagen fandt tilsynet imidlertid ved en søgning i Google yderligere tre offentliggjorte Excel filer indeholdende personoplysninger på Aalborg Universitets hjemmeside. De yderligere tre Excel-filer indeholdt personoplysninger - om i alt ca. 3500 patienter, herunder personnumre, navne og (for nogles vedkommende) helbredsoplysninger.

Datatilsynet udtalte bl.a., at Aalborg Universitet ikke havde udvist den fornødne omhu, og Aalborg Universitet havde dermed ikke overholdt kravene i persondatalovens § 41, stk. 3. Datatilsynet fandt endvidere, at det var en skærpende omstændighed, at de tre yderligere Excel-filer lå offentligt tilgængelige efter, at Datatilsynet havde været i kontakt med Aalborg Universitet om den første offentliggørelse – af oplysninger om 82 studerende – og i den forbindelse havde opfordret universitetet til at foretage en gennemgang af universitetets hjemmesider. Datatilsynet fandt på denne baggrund det passerede meget kritisabelt. Datatilsynet rettede efterfølgende henvendelse til Ministeriet for Videnskab, Teknologi og Udvikling i anledning af denne og lignende sager med sikkerhedsbrister på andre universiteter (Datatilsynets j.nr. 2007-632-0016)

Orientering af Ministeriet for Videnskab, Teknologi og Udvikling om mangelfuld behandlingssikkerhed på universiteter

Datatilsynet rettede den 29. maj 2009 henvendelse til Ministeriet for Videnskab, Teknologi og Udvikling i anledning af, at tilsynet i en række sager havde konstateret alvorlige sikkerhedsbrister på landets universiteter. Datatilsynet orienterede om de ovenfor omtalte gentagelsestilfælde af sikkerhedsbrister i forbindelse med behandlingen af personoplysninger ved Aalborg Universitet, Københavns Universitet og Copenhagen Business School samt den udtalte kritik til universiteterne.

Datatilsynet anmodede Ministeriet for Videnskab, Teknologi og Udvikling om at oplyse, om ministeriet vil tage initiativer med henblik på at sikre, at persondataloven efterleves på ministeriets område (Datatilsynets j.nr. 2007-632-0016, 2008-216-0153 og 2009-632-0046).

Universitets- og Bygningsstyrelsen oplyste i den forbindelse, at styrelsen, som opfølgning på Datatilsynets orientering, ville drøfte de konkrete sager på næstkommende universitetsdirektørmøde samt henstille til, at universiteterne sikrer, at persondataloven overholdes. Styrelsen ville endvidere vurdere, om der skulle rejses tilsynssager. Datatilsynet har noteret sig det af styrelsen oplyste.

Vilkår om sikkerhed ved privat anmeldelse

Under hensyn til karakteren og omfanget af de personoplysninger, som behandles på et privathospital, har Datatilsynet fastsat en række vilkår om sikkerhed.

Datatilsynets tilladelse til et privat hospitals behandling af personoplysninger i forbindelse med patientbehandling blev givet på følgende vilkår:

1. I det omfang behandling, herunder videregivelse, af personoplysninger ikke er reguleret af særregler, herunder navnlig i sundhedsloven og vævslovgivningen, skal behandling af personoplysninger, som foretages af privathospitalet, ske i overensstemmelse med persondatalovens regler.

2. Behandling af personoplysninger forudsættes i øvrigt at ske under iagttagelse af gældende lovgivning, herunder navnlig sundhedsloven og vævslovgivningen.

3. Behandling af personoplysninger skal ske under iagttagelse af de i bilag 1 beskrevne sikkerhedsregler.

4. Den enkelte medarbejder 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 bl.a.:

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.

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 it-systemer. 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. Hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal der foreligge en skriftlig aftale, hvoraf det fremgår, at de fastsatte vilkår ligeledes gælder for behandlingen ved databehandleren.

4. Hvis behandling af personoplysninger finder sted på en pc-arbejdsplads uden for den dataansvarliges lokaliteter, skal den dataansvarlige fastsætte særlige retningslinier herfor, så det sikres, at de fastsatte vilkår iagttages.

5. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne. Udtagelige lagringsmedier, sikkerhedskopier af data mv. skal opbevares forsvarligt aflåst og således, at uvedkommende ikke kan få adgang til oplysningerne.

6. Såfremt der er etableret eller etableres en digital selvbetjeningsløsning – f.eks. adgang til at indsende og modtage oplysninger via login på en hjemmeside – skal login baseres på digital signatur.

7. 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. Al transmission af følsomme personoplysninger over internettet skal ske i krypteret form.

8. 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

9. 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

10. 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

11. 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.

12. 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.

13. Sundhedslovens regler om adgang til elektroniske patientjournaler skal iagttages ved autorisation. 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.

14. 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.

15. 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

16. 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.

Biologisk materiale

17. Prøver med biologisk materiale og biologisk materiale i biobanker skal opbevares forsvarligt aflåst, således at uvedkommende ikke har adgang til det, og på en sådan måde, at det sikres, at materialet ikke fortabes, forringes eller hændeligt eller ulovligt tilintetgøres.

18. Biologisk materiale, der er mærket med personnummer eller navn, skal opbevares under iagttagelse af særlige sikkerhedshensyn.

19. Der skal fastsættes interne retningslinier for opbevaring af biologisk materiale. Retningslinierne skal gennemgås mindst én gang om året og ajourføres i fornødent omfang.

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 en region, kan der blive tale om et brev (orientering) til kommunalbestyrelsen eller vedkommende regionsråd. 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, som hovedregel begrænset til de typer af behandlinger,

der er omfattet af tilladelseskravet i lovens § 50 samt til edb-servicevirksomheder, omfattet af anmeldelsespligten i lovens § 53.

Med de nye regler om tv-overvågning, jf. kapitlet om tv-overvågning, har Datatilsynet endvidere fra den 1. juli 2007 haft mulighed for at foretage inspektioner hos alle offentlige myndigheder og private dataansvarlige, der behandler personoplysninger i forbindelse med tv-overvågning. Dette gælder, selv om tv-overvågning er undtaget fra anmeldelsespligten.

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.

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

Logning og sletning
Oplysningspligt, indsigtsbegæringer og samkøring i kontroløjemed
Billeder og andre informationer på 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 forbindelse med inspektioner hos offentlige myndigheder vælger Datatilsynet som oftest at lægge særlig vægt på et mere afgrænset antal emner for at få tid til en mere grundig gennemgang og drøftelse af de enkelte emner.

Efter gennemgang af relevante emner gennemgås ved de inspektioner hos offentlige myndigheder, hvor en af Datatilsynets it-sikkerhedskonsulenter deltager, emner af rent teknisk-sikkerhedsmæssig karakter, herunder dele af de sikkerhedsregler, som myndigheden har fastsat i henhold til sikkerhedsbekendtgørelsens § 5. Ved inspektioner, hvor der ikke deltager en it-sikkerhedskonsulent, fokuseres der 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 it-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, der indeholder 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 sluttes 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.

Ved kommuneinspektionerne i 2008 og 2009 kunne stort set alle 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.

Den ovenfor omtalte procedure ved kommuneinspektioner anvendes i dag rutinemæssigt ved inspektioner hos andre offentlige dataansvarlige, herunder statslige myndigheder.

Datatilsynet har i 2009 også afprøvet en ny form for inspektioner, hvor der er blevet udvalgt et tema, som er blevet behandlet mere indgående. Temainspektionerne – i forhold til de mere generelle inspektioner, hvor mange emner berøres – er foretaget hos 4 kommuner, og temaet har været den registreredes rettigheder. Datatilsynet vil også i fremtiden arbejde videre med denne form for inspektioner.

Datatilsynets observationer ved inspektioner i 2008 og 2009

Nedenfor er en samlet oversigt over udførte inspektioner i 2008 og 2009.

Datatilsynet foretog i 2008 94 inspektioner. En del af inspektionsvirksomheden blev udført ved en koncentreret indsats henholdsvis på Fyn og i Nordjylland.

De koncentrerede indsatser blev gennemført ved, at tilsynet udstationerede nogle medarbejdere to gange i Odense af hver tre dages varighed og en enkelt gang i Aalborg af tre dages varighed. Den ene indsats på Fyn og indsatsen i Nordjylland koncentrerede sig om inspektioner hos virksomheder med tv-overvågning.

I 2009 har Datatilsynet foretaget 83 inspektioner. Også i 2009 blev en del af inspektionsvirksomheden gennemført ved en koncentreret indsats – her ved inspektioner over fem dage i Sønderjylland.

Datatilsynet har flere gange tidligere gennemført denne form for målrettet indsats i et geografisk område. Det er fortsat tilsynets indtryk, at man ved i en periode at koncentrere sig om veldefinerede områder – her geografiske – kan opnå stor opmærksomhed omkring persondatalovens regler, tilsynets opgaver og datasikkerhed generelt.

Det overordnede indtryk efter inspektionerne, gennemført i 2008 og 2009 er at de dataansvarlige generelt er opmærksomme på pligten til at anmelde behandlinger af personoplysninger til Datatilsynet.

Ved tilsynets inspektioner er det typiske billede 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 2008 og 2009 konstatere 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 ansvaret for denne gennemgang, hvilke terminer der er fastsat herfor, og hvornår reglerne senest er revideret.

Tv-overvågnings-inspektioner

Med de nye regler om tv-overvågning har Datatilsynet fra den 1. juli 2007 fået mulighed for at foretage inspektioner hos alle offentlige myndigheder og private dataansvarlige, der behandler personoplysninger i forbindelse med tv-overvågning.

Datatilsynets inspektioner kan foretages såvel varslet som uden varsel. Datatilsynet har indtil videre udelukkende foretaget varslede inspektioner på tv-overvågningsområdet, idet tilsynet finder det mest hensigtsmæssigt, at der er personer til stede, som kan besvare tilsynets spørgsmål. Det bemærkes i den forbindelse, at tilsynets fokus er på efterlevelse af persondatalovens krav til håndtering af optagelser, oplysningspligten, sletningsrutiner og datasikkerhed.

Datatilsynet har udarbejdet et spørgeskema til de dataansvarlige, som bliver udsendt til de udvalgte virksomheder sammen med varslingen og returneret til tilsynet med svar forud for selve inspektionen. Skemaerne er en god indgangsvinkel i forhold til inspektion hos private dataansvarlige og desuden effektiviseres inspektionen, således at der kan gennemføres flere inspektioner på kortere tid.

Datatilsynet har afprøvet forskellige fremgangsmåder med hensyn til varsling af inspektionerne. I en del tilfælde har Datatilsynet rettet henvendelse til private virksomheder og forespurgt, om de foretager tv-overvågning, og derefter udvalgt de virksomheder, som skulle inspiceres. I andre tilfælde har Datatilsynet på forhånd haft kendskab til eller formodning om, at de omhandlede virksomheder foretager tv-overvågning, og har derfor varslet inspektion direkte over for disse.

Datatilsynet forventer fortsat at udvikle tilsynets metoder til udvælgelse af de virksomheder, som skal inspiceres.

I 2008 og 2009 har Datatilsynet foretaget et stort antal inspektioner på tv-overvågningsområdet. Der er således foretaget inspektioner inden for bl.a. detailhandlen, restaurationsbranchen og banksektoren. Datatilsynet har udvalgt flere store forretningskæder, koncerner og banker til inspektionsbesøg for at nå så bredt ud som muligt. Imidlertid er også individuelle, mindre forretninger mv. blevet besøgt.

Datatilsynet har gennemført hovedparten af inspektionerne i form af "raids" af 2-3 dages varighed, hvor et geografisk afgrænset område er blevet udvalgt til inspektion – i foråret 2008 Rosengårdcentret i Odense, i efteråret 2008 Aalborg

by, i foråret 2009 Lyngby Storcenter og i efteråret 2009 en række banker i Sønderjylland.

Inspektionerne er gennemført som stikprøvekontroller – dvs. som et rutinemæssigt led i Datatilsynets virksomhed uden konkret anledning i forhold til den enkelte virksomhed.

Af generelle indtryk fra de gennemførte inspektioner af tv-overvågning i 2008 og 2009 kan nævnes, at langt størstedelen af de besigtigede kameraer var digitale, at der typisk blev overvåget hele døgnet i kriminalitetsforebyggende/-opklarende øjemed, og at optagelserne ikke blev opbevaret længere end de tilladte 30 dage. Kunder blev typisk informeret via skiltning, og egne medarbejdere var også informeret om tv-overvågningen – typisk mundtligt, men mange tilkendegav, at man fremover ligeledes ville informere medarbejderne skriftligt. Enkelte af de inspicerede var ikke opmærksomme på at informere ekstern arbejdskraft – f.eks. rengøringspersonale. Typisk var det spørgsmål af teknisk/sikkerhedsmæssig karakter, som betød, at en inspektion ikke kunne afsluttes med det samme.

Datatilsynet kan i øvrigt henvise til redegørelse til Folketinget om erfaringerne med lov om tv-overvågning og lov om behandling af personoplysninger, hvortil tilsynet har bidraget (Retsudvalget 2009-2010, REU alm. del Bilag 129).

Oversigt over udførte inspektioner i 2008:

Staten (17):
Birkerød Gymnasium
Statsadvokaten for Særlig Økonomisk Kriminalitet
Statsadvokaten i Nord- og Østjylland
Arbejdstilsynet
Videnskabsministeriets Department
Naturklagenævnet
Retslægerådet
Direktoratet for Kriminalforsorgen
Velfærdsministeriet
Rigspolitiet, Europol
Fødevarestyrelsen
Personalestyrelsen
Patent- og Varemærkestyrelsen
Fyns Politi
Statsfængslet i Ringe
Aalborg Universitet
Statsforvaltningen i Nordjylland

Kommuner og regioner (12):
Fredensborg
Nyborg
Egedal
Ishøj
Frederikssund
Region Sjælland
Middelfart
Nordfyn
Svendborg
Kerteminde
Holbæk
Brøndby (borgerservice)

Offentlige sygehuse (2):
Frederikssund Hospital
Glostrup Hospital

Offentlig forskning (1):
Østerbroundersøgelsen

Private forskere (9):
Odderprojektet
Liselotte Pedersen
Frank Schiødt, Rigshospitalet

Signe Smith Nielsen
Birgit Petersson
Redi Pecini
Dorthe Bleses
Birthe Søndergaard
Kasper Møller Hansen

Øvrige private (23):
Debitorregisteret
Soliditet A/S
Grafisk Arbejdsgiverforening, Odense
Vallensbæk Zoneterapi
Hanne Birgitte Jensen, Haslev
Guldbrandsen Akupunktur. Ålborg
Lundgaard ApS
Rosengård Center Konto, Odense
Sparekassen Sjælland, Holbæk
Sahva A/S
Pen-Sam
Sydgården, Haderslev
Alm. Brand Forsikring
Experian A/S
Parken Sport & Entertainment
Antipiratgruppen
GF-Forsikring
Faaborg Zoneterapi
Karin List
Lisbeth Kristensen
Merethe Bonnesen Terapi og M assage
Ditte Loft
Åse Andersen

Tv-overvågning(30)
Hautop ApS (7-eleven)
Stenstrup Juveler
Café Norden ApS
Centeradministration (I/S Rosengårdscentret)
Rosengården Apotek (Odense Sct. Knuds Apotek)
Fona (F Group A/S)
Antik Blå A/S
Build-a-bear (Choose Denmark ApS)
Kvickly xtra (Coop Danmark A/S)
Quintess (Axel Kaufmann ApS)
Cinemaxx

Newyorker Danmark ApS
Susanne Markes ApS (DERES)
Video 4
McDonalds
Frederiks I/S
OK
Herman Zinck A/S – Zinck Inspiration
Nordea
Danske Bank
Café Saltlageret
Hr. Nielsen A/S
Stereo Studie
Profil Optik
Hennes & Mauritz
Hansen & Pedersen I/S (Wagner)
Budolfi Apotek
Rubber Duck ApS
Matas
Guldsmed Helbo, Friis ApS

Oversigt over inspektioner i 2009:

Staten(11)
Energistyrelsen
Sikringsstyrelsen
Patientskadeankenævnet
Økonomistyrelsen
Sydsjælland og Lolland Falsters Politi
Syd- og Sønderjyllands Politi
Sønderborg Lokalpoliti
Sikkerhedsstyrelsen
Statsforvaltningen Syddanmark
Nationalmuseet
Rigspolitiet, Schengen

Kommuner og regioner (13)
Odsherred
Lyngby-Taarbæk
Solrød
Kolding
Sønderborg
Aabenraa
Tønder
Haderslev
Esbjerg
Fanø

Vejen
Ballerup
Region Syddanmark

Temainspektioner – registreredes rettigheder (4)
Tårnby Kommune
Køge Kommune
Vallensbæk Kommune
Næstved Kommune

Offentlige sygehuse (3)
Herlev Sygehus
Sygehus Sønderjylland
Sydvestjysk Sygehus

Sikkerhedsinspektioner (3)
Lægemiddelstyrelsen
Sundhed.dk som databehandler for Lægemiddelstyrelsen
Sundhedsstyrelsen

Private forskere(14)
Sven Asger Sørensen
Kasper Iversen
Suzanna Lunding
Kim Rose Olsen
Team Danmark
Jane Greve
Bjarne Laursen
Evy Marie Frantzen
Henrik Enghusen Poulsen
Hanne Kristine Hegaard
Anne Kirstine Møller
Mette Rauhe Mouridsen
Annette Vangsted
Henriette Lipczak

Øvrige private(21)
Arto (Freeway)
WatAgame ApS (GoSupermodel)
Thomson Reuters
Topdanmark
Diners Club
TDC A/S
Uxor ApS

Parken Sport & Entertainment
DFIM
Telekommunikations Industriens advarselsregister
Mercuri Urval A/S
DoktorDating.dk
Akupunktur-klinikken
Annelise Thomsen
Karen Christensen
Else Jakobsen
Klinik for Zoneterapi/B. Bækbo
Mette Pedersen
Dragør Akupunkturklinik
Knudezonen
Kirsten Stenander

Tv-overvågning (14)
Center Ure v/Jens Breum Christiansen
TP Musik Marked ApS
Aktieselskabet TH. Wessel & Vett Magasin Du Nord (Magasin i Lyngby)
Tøjeksperten A/S
Plaza Ure og Smykker A/S
Centerforeningen Lyngby Storcenter
Sydbank A/S - hovedsæde
Sydbank Sønderborg
Danske Bank Tønder
Danske Bank Kolding
Danske Bank Christiansfeld
Nordea Haderslev
Nordea Aabenraa
Nordea Vamdrup