DATATILSYNET

Datatilsynets årsberetning 2011

Datatilsynets årsberetning 2011

Udgiver: Datatilsynet
Tryk og layout: Rosendahls-Schultz Grafisk
Beretningen er sat med Meta
Oplag: 300
Oktober 2012
ISSN nr: 1601-5657
ISBN nr: 978-87-992871-3-0




Indhold

Til Folketinget

Datatilsynet har igen i 2011 haft et spændende og udfordrende år. Persondatabeskyttelse er et vigtigt aspekt i forbindelse med den teknologiske udvikling, som hele tiden medfører flere digitale løsninger og processer. Brugen af internettet er en helt integreret del af dagligdagen for de fleste, og der opstår stadig nye måder at anvende internettet på.

Denne udvikling gør, at Datatilsynet konstant bliver udfordret. Det er vigtigt, at tilsynet hele tiden holder sig ajour med, hvad der rører sig i samfundet, og samtidig gør sig overvejelser om, hvad det giver af problemstillinger inden for databeskyttelse.

Datatilsynet har generelt en positiv indstilling over for brug af nye teknologier. Men Datatilsynet ser det også som en væsentlig opgave at sætte fokus på, at den teknologiske udvikling kan indebære en øget risiko for vores grundlæggende ret til privatliv og databeskyttelse.

Et nyt emne, som har fyldt meget i tilsynet i 2011, er cloud computing. Muligheden for, at offentlige myndigheder og private virksomheder kan opbevare data i "skyen", giver anledning til en række spørgsmål. Datatilsynet var en af de første tilsynsmyndigheder i Europa, som tog fat på problemstillingen omkring cloud computing.

Det var også i 2011, at Datatilsynet for første gang var såkaldt "lead authority" på en dansk virksomheds bindende virksomhedsregler (Binding Corporate Rules - BCR). Bindende virksomhedsregler giver mulighed for, at virksomheder inden for en koncern kan overføre personoplysninger mellem hinanden, uanset at der herved sker overførsel af oplysninger til tredjelande, dvs. lande uden for EU/EØS.

På den negative side har Datatilsynet igen i 2011 kunnet konstatere, at der sker mange datasikkerhedsbrister, f.eks. i form af ikke-tilsigtede offentliggørelser af personoplysninger på internettet. Datatilsynet ser med alvor på disse sager og reagerer straks, når tilsynet bliver opmærksom på sådanne sikkerhedsbrister. Det gælder om at lære af sådanne hændelser, således at de i videst muligt omfang kan undgås fremover. Og når en sikkerhedsbrist alligevel er sket, er det vigtigt hurtigt at få begrænset eventuelle skadevirkninger for de berørte personer.

Med disse ord – og i nyt design – afgiver Datatilsynet hermed sin årsberetning for 2011.

København, oktober 2012

Henrik Waaben
Formand for Datarådet

Janni Christoffersen
Direktør

Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2011 afgives i medfør af persondatalovens § 65, hvorefter tilsynet afgiver en årlig beretning om sin virksomhed til Folketinget. Beretningen indeholder en omtale af væsentlige aktiviteter for Datatilsynet i 2011, herunder tilsynets inspektioner (kontrolbesøg).

På Datatilsynets hjemmeside www.datatilsynet.dk offentliggør tilsynet løbende udtalelser og afgørelser i sager, som vurderes at være af generel interesse. Datatilsynet kan således henvise til sin hjemmeside for yderligere oplysninger.

Datatilsynets virksomhed i 2011

Datatilsynets opgaver

Datatilsynet er den centrale uafhængige myndighed, der fører tilsyn med, at reglerne i persondataloven overholdes. Tilsynet med domstolene ligger dog under Domstolsstyrelsen.

Persondataloven:

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger. Loven er senest ændret ved lov nr. 422 af 10. maj 2011.

Tilsynet med persondataloven indebærer et stort antal forskelligartede opgaver. Datatilsynet har i 2011 bl.a. haft følgende opgaver:

- Information, rådgivning og vejledning, bl.a. i form af generelle retningslinjer
- Behandling af klager fra borgere
- Udtalelser om forslag til love og bekendtgørelser mv.
- Udtalelser om anmeldelser fra offentlige myndigheder
- Tilladelser til virksomheder mv.
- Tilladelser til forskere
- Bidrag til besvarelse af spørgsmål fra Folketinget
- Sager på Datatilsynets eget initiativ (egen drift-sager), herunder inspektioner hos offentlige myndigheder, private virksomheder, forskere mv.
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsynsmyndigheder
- Deltagelse i arbejdsgrupper, udvalg mv. og oplæg på konferencer o.l.




Retningslinjer for fratrådte medarbejderes e-mail-konti

I 2011 har Datatilsynet bl.a. fastsat generelle retningslinjer for arbejdsgiveres behandling af e-mail-konti efter medarbejdernes fratræden. Retningslinjerne indebærer bl.a., at når en medarbejder har forladt arbejdspladsen og ikke længere kan få adgang til sin personlige e-mail-konto på arbejdspladsen, må e-mail-kontoen kun holdes aktiv i en periode, der er så kort som muligt. Den aktive e-mail-konto må kun benyttes til modtagelse af e-mail, og der skal sættes et auto-svar på e-mail-kontoen med besked om medarbejderens fratræden og eventuel anden relevant information.

Retningslinjerne kan læses i deres fulde længde på Datatilsynets hjemmeside.

Påbud om at ophøre med offentliggørelse af oplysninger om politisk overbevisning

Datatilsynet tog i 2011 af egen drift en sag op om en privat sammenslutnings offentliggørelse af oplysninger om bl.a. politisk tilhørsforhold.

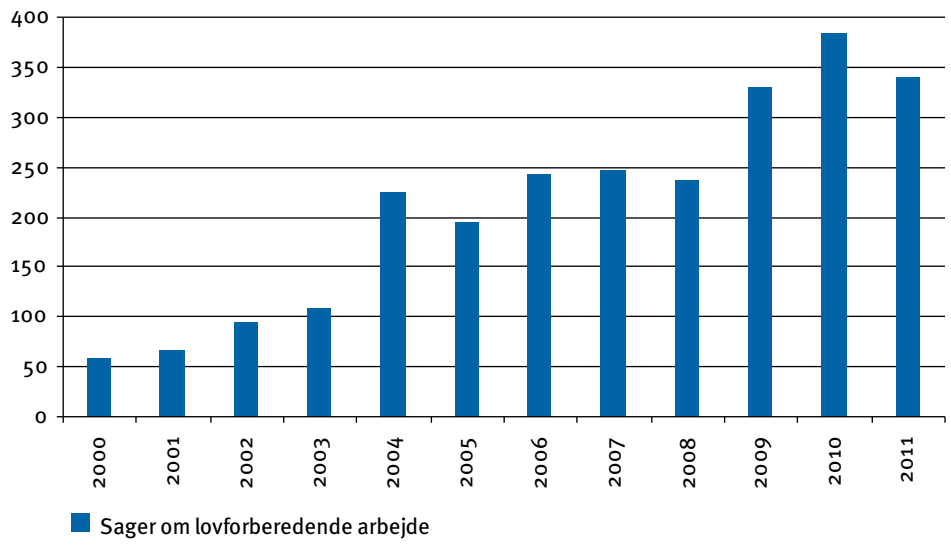
I en over 100 sider lang rapport på en hjemmeside var offentliggjort navne, billeder og andre oplysninger om en lang række personer, der ifølge rapporten angiveligt var medlemmer eller tidligere medlemmer af en politisk organisation. Datatilsynet meddelte den dataansvarlige for offentliggørelsen påbud om at stoppe offentliggørelsen af oplysninger om politisk overbevisning samt billeder på den pågældende hjemmeside. Det var Datatilsynets vurdering, at der ikke var den fornødne hjemmel til offentliggørelse af oplysningerne om politisk overbevisning i persondatalovens § 7, stk. 2.

Idet den dataansvarlige ikke fulgte Datatilsynets påbud, gav tilsynet den 21. september 2011 databehandleren (serviceudbyderen) påbud om at fjerne oplysningerne. Databehandleren fulgte tilsynets påbud.

Høringer over lovforslag mv.

I 2011 registrerede Datatilsynet 339 nye høringssager i forbindelse med lovforslag, bekendtgørelser mv. Dette er et fald på 11 % i forhold til 2010 (383 i 2010), hvilket skyldes, at lovgivningsarbejdet i Folketinget og centraladministration blev sat i stå i forbindelse med folketingsvalget i september 2011.

Datatilsynet skal efter persondatalovens § 57 afgive udtalelse ved udarbejdelse af generelle retsforskrifter, f.eks. forslag til love, bekendtgørelser og direktiver, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger






Datatilsynet kritisk over for lovforslag

Datatilsynet behandlede i 2011 Pensionsstyrelsens forslag til lov om ændring af lov om aktiv socialpolitik mv. (bedre kontrol med udbetaling af offentlige forsørgelsesudgifter).

Datatilsynet afgav to høringssvar, bidrog til besvarelse af spørgsmål fra Folketingets Arbejdsmarkedsudvalg og deltog tillige i møder om lovforslaget. Tilsynet deltog endvidere i Folketingets Arbejdsmarkedsudvalgs offentlige høring om lovforslaget.

Datatilsynet havde en række konkrete betænkeligheder i forhold til beskyttelsen af de involverede borgeres privatliv. Tilsynet pegede bl.a. på spørgsmål om forudsigeligheden for borgerne ved såkaldte "lufthavnstilsyn" og myndighedernes adgang til oplysninger i indkomstregisteret. Tilsynet havde endvidere betænkeligheder i forhold til adgangen for Pensionsstyrelsen til at indhente oplysninger fra pengeinstitutter om hævninger og indsættelser foretaget i udlandet.

Social- og Integrationsministeriet anmodede i 2011 om Datatilsynets bemærkninger til et lovforslag om sagsbehandling og administration i Udbetaling Danmark. Datatilsynet afgav i december et omfattende høringssvar, hvori tilsynet bl.a. pegede på, at lovforslagets konsekvente fravigelse af persondataloven § 8, stk. 3, gav anledning til principielle overvejelser om bestemmelsens fortsatte berettigelse. Tilsynet pegede endvidere på, at nødvendighedsbetingelsen i persondatalovens § 5 skulle overvejes nøje i forbindelse med udvekslingen af oplysninger mellem Udbetaling Danmark og kommunerne. Endelig havde tilsynet en række bemærkninger omkring datasikkerhed, når oplysninger udveksles.

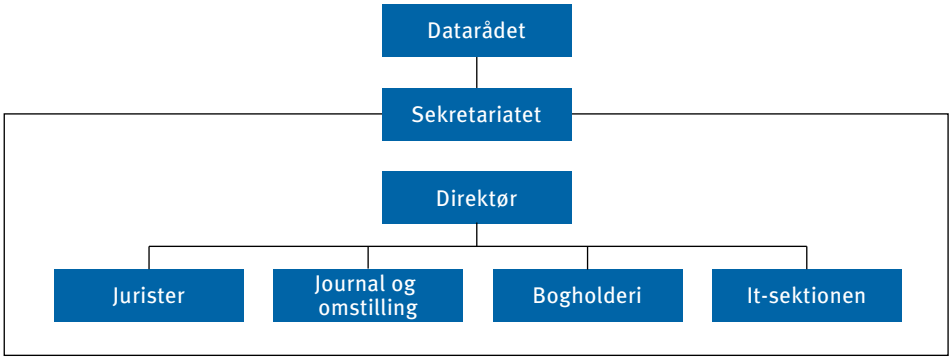
Om Udbetaling Danmark

Myndigheden Udbetaling Danmark overtager i løbet af 2012 og foråret 2013 opgaver fra kommunerne på områderne familieydelser (børne- og ægtefællebidrag, børnetilskud, børne- og ungeydelse), barselsdagpenge, boligstøtte, folkepension og førtidspension. Det er offentlige ydelser, som kommunen hidtil har taget sig af. Kommunen vil dog fortsat have ansvar for enkelte opgaver. F.eks. skal kommunen fortsat afgøre, om borgeren er berettiget til førtidspension, men det er Udbetaling Danmark, der skal udbetale den.

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 persondataloven 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 seks 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 forretningsordenen for Datarådet og kan findes på Datatilsynets hjemmeside.




Datarådets medlemmer (pr. 31. december 2011)

Formand, højesteretsdommer Henrik Waaben
Næstformand, advokat Janne Glæsel
Professor, dr.jur. Peter Blume
Overlæge, afdelingschef Hans Henrik Storm
Direktør Rasmus Kjeldahl
Kommunaldirektør Niels Johannesen
Chefkonsulent Henning Mortensen

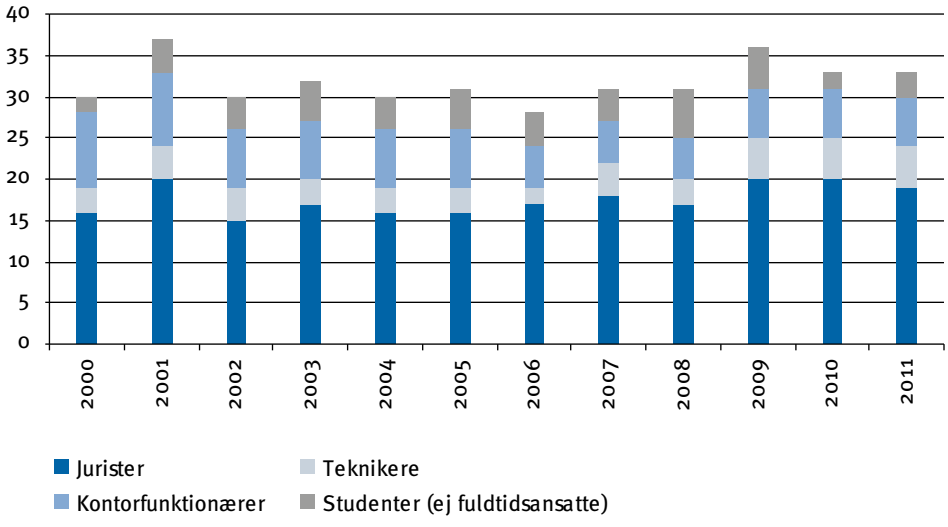
Medlemmerne beskikkes for 4 år ad gangen. De er personligt udpeget i kraft af deres sagkundskab inden for bestemte sagsområder og er ikke repræsentanter for bestemte interesseorganisationer el.lign.

Sekretariatet

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

Datatilsynets bevillingsmæssige forhold mv. fremgår af Datatilsynets årsrapport 2011. Årsrapporten for 2011 er offentliggjort på tilsynets hjemmeside.

Personalesammensætning






Datatilsynets medarbejdere (pr. 31. december 2011)

Direktør, cand.jur. Janni Christoffersen
Kontorchef, cand.jur. Lena Andersen
It-chef, civilingeniør, HD, Sten Hansen
Chefkonsulent, cand.jur. Jakob Lundsager
Chefkonsulent, cand.jur. Lene Engedal Kragelund
Specialkonsulent, cand.jur. Maiken Christensen Breüner
Specialkonsulent, mag.art. Camilla Daasnes
It-sikkerhedskonsulent, exam. ESL, CISSP Henrik Blumensaath Bjarnholt
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
Kontorfuldmægtig Helle Jensen
Kontorfuldmægtig Pernille Jensen
Kontorfuldmægtig Anne-Marie Müller
Kontorfuldmægtig Suzanne Stenkvist
Overassistent Vibeke Lund Larsen
Overassistent Mette Maj Leilund
Assistent Camilla Knutsdotter Hallingby (orlov)
It-medarbejder Eva Caspersen
It-medarbejder Flemming Nielsen
Fuldmægtig, cand.jur. Trine Cseh-Lessel
Fuldmægtig, cand.jur. Marianne Jansteen Eskesen
Fuldmægtig, cand.jur. Mette Hansen (orlov)
Fuldmægtig, cand.jur. Robert Padilla Bang Jensen
Fuldmægtig, cand.jur. Lasse May Jørgensen
Fuldmægtig, cand.jur. Henrik Rubæk Jørgensen
Fuldmægtig, cand.jur. Christine Landsgaard
Fuldmægtig, cand.jur. Iben Segel Larsen
Fuldmægtig, cand.jur. Louise Black Mogensen
Fuldmægtig, cand.jur. Anna Alexandra Pontoppidan
Fuldmægtig, cand.jur. Kristian Gyde Poulsen
Fuldmægtig, cand.jur. Maja Blomquist Rasmussen
Fuldmægtig, cand.jur. Dana Safin
Fuldmægtig, cand.jur. Anne Mette Riis Steinø
Stud.jur. Frederik Rechenbach Enelund
Stud.jur. Desiré Dyveke Palsbøll
Stud.jur. Kirsten Marie Petersen

Databeskyttelsesdag 2011

Den 28. januar er fastsat til at være Europæisk Databeskyttelsesdag. Databeskyttelsesdagen er et initiativ fra Europarådet, og dagen støttes af Europa-Kommissionen og de europæiske datatilsyn.

Databeskyttelsesdagen er en anledning til at gøre en særlig indsats for at øge borgernes bevidsthed om deres rettigheder efter persondataloven.

I 2011 markede Datatilsynet databeskyttelsesdagen ved at have en stand i Frederiksberg Centret, hvor centrets kunder kunne stille spørgsmål og få vejledning om deres rettigheder efter persondataloven. Datatilsynet havde i anledning af databeskyttelsesdagen udarbejdet to pjecer. "Sociale netværk og internettet – Hvad skal du være opmærksom på?" er en kortfattet introduktion til, hvad man kan og ikke kan offentliggøre om andre personer i sociale netværk, chatfora mv. "Kend din ret til indsigt" er en kortfattet beskrivelse af reglerne om indsigt – en af de rettigheder, som borgerne har efter persondataloven.

Du kan udskrive Datatilsynets pjecer "Sociale netværk og internettet – Hvad skal du være opmærksom på?" og "Kend din ret til indsigt" på tilsynets hjemmeside under Publikationer

De besøgende havde også mulighed for at tage testen "Test din viden om beskyttelse af personoplysninger", som var særligt udarbejdet til lejligheden. Testen består af 10 spørgsmål. Efter besvarelsen får man de rigtige svar. Samtidig kan man se, hvor rigtigt man har svaret i forhold til andre, der har udfyldt testen.

"Test din viden om beskyttelse af personoplysninger" er tilgængelig på Datatilsynets hjemmeside under punktet Borger.

Eksempel på spørgsmål fra testen:
Må din arbejdsgiver lægge et billede af dig på sin hjemmeside?
1. Ja, det har en arbejdsgiver altid ret til
2. Nej, det vil aldrig være i overensstemmelse med persondataloven
3. Ja, men det kræver dit udtrykkelige samtykke

(Det rigtige svar er 3)

Statistiske oplysninger

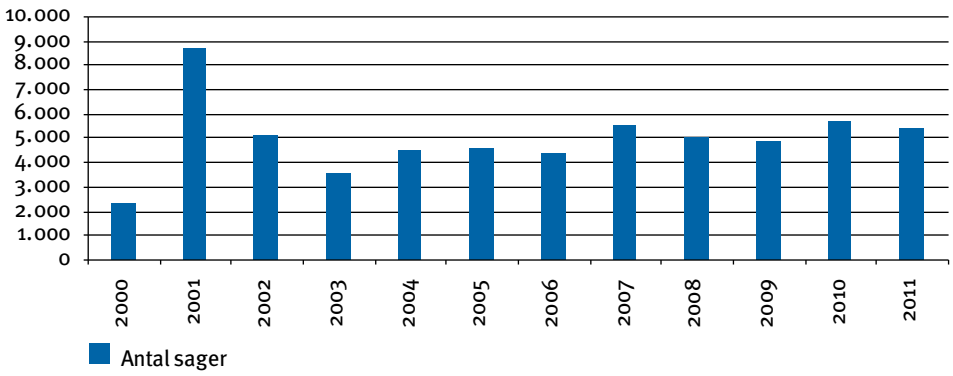
Her er oplysninger om antallet af nye sager i Datatilsynets journalsystem i 2011. Tallene omfatter sager, som er oprettet i løbet af 2011. En del af Datatilsynets sagsbehandling er imidlertid en fortsættelse af eksisterende sager. Dette er for eksempel tilfældet, når en anmeldelse ændres, eller en tilladelse forlænges. Disse sager er af praktiske årsager ikke medtaget i statistikken.

Datatilsynet registrerede 5.442 nye sager i 2011.

Nyoprettede sager 1. januar 2011 til 31. december 2011:

Datatilsynets egen administration mv.	189
Lovforberedende arbejde	339
Forespørgsler og klager vedrørende private	1.235
Forespørgsler og klager vedrørende offentlige myndigheder	730
Anmeldelser for den private sektor	2.165
Anmeldelser for den offentlige sektor	437
Sager på Datatilsynets eget initiativ (egen drift-sager)	96
Sikkerhedsspørgsmål	51
Internationale sager	176
Datatilsynets kompetence efter anden lovgivning	24
I alt	5.442

Der er et svagt fald i antallet af nyoprettede sager i 2011 set i forhold til 2010. I 2010 var tallet 5.665 nyoprettede sager, dvs. der er et fald på 4 %. Fra 2009 til 2010 var der en stigning på 17 %.



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

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 1.235 nye sager om forespørgsler og klager vedrørende private dataansvarlige.

Sagerne havde følgende fordeling på forskellige virksomhedstyper:

Almindelige virksomheder	164
Den finansielle sektor	57
Fagforeninger, a-kasser, pensionskasser mv.	30
Telesektoren	256
Foreninger og organisationer	120
Sundhedssektoren (medicinalfirmaer, klinikker, læger mv.)	33
Kreditoplysningsbureauer	120
Advarselsregistre	29
Stillingsbesættende virksomheder	11
Ansøgninger om tilladelser	142
Diverse	269
Sager af generel karakter	1
Edb-servicebureauer	3

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2011[1], var:

Klager	11 %
Forespørgsler	76 %
Ikke kategoriserede	13 %

1 I lighed med Datatilsynets Årsberetning 2010 er disse tal for 2011 ikke opgjort på grundlag af sager, som er oprettet i 2011, men på grundlag af sager, som Datatilsynet har færdigbehandlet i 2011. Heriblandt er sager oprettet i 2011 og 2010 samt enkelte sager fra tidligere år. Opgørelsesmetoden skyldes et ønske om at opgøre tallene på en måde, så de ikke ændrer sig afhængig af, hvornår man opgør dem.




Forespørgsler og klager vedrørende offentlige myndigheder

Datatilsynet registrerede i alt 730 nye sager om forespørgsler og klager vedrørende offentlige myndigheder.

Sagerne var fordelt således:

Statslige myndigheder	250
Regioner	34
Primærkommuner	206
Ansøgning om tilladelser	229
Diverse	11

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2011[2], var:

Klager	9 %
Forespørgsler	54 %
Ikke kategoriserede	37 %

2 Se note 1

Anmeldelser

Anmeldelser for den private sektor

Datatilsynet registrerede i alt 2.165 nye sager om anmeldelser for den private sektor. Fordelingen af sagerne var:

Forskning og statistik	1.376
Privates behandling af oplysninger om rent private forhold	480
Advarselsregistre	9
Spærrelister	5
Kreditoplysningsbureauer	3
Stillingsbesættende virksomheder	30
Edb-servicebureauer	14
Diverse sager af generel karakter	248

Anmeldelser for den offentlige forvaltning

Datatilsynet registrerede i alt 437 nye sager om anmeldelser for den offentlige sektor. Fordelingen af sagerne var:

Fællesanmeldelser	6
Kommuner	94
Regioner	0
Statslige myndigheder	267
Tilslutninger, kommuner	70
Tilslutninger, regioner	0
Tilslutninger, statslige myndigheder	0
Diverse/sager af generel karakter	0




Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 96 nye sager oprettet på tilsynets eget initiativ. Fordelingen af sagerne var:

Inspektion og kontrol vedrørende private	37
Inspektion og kontrol vedrørende offentlige myndigheder	23
Sager rejst på grundlag af presseomtale og lign.	36
Diverse/sager af generel karakter	0

Internationale sager

Datatilsynet registrerede i alt 176 nye internationale sager. Fordelingen af sagerne var:

Forespørgsler fra udlandet	67
Nordisk tilsynssamarbejde	5
Europarådet	1
EU	83
Datakommissærsamarbejdet	13
OECD	1
Diverse /sager af generel karakter	6

Persondataloven – i stadig udvikling

Persondataloven trådte i kraft den 1. juli 2000. Siden da er loven blevet ændret seks gange. Også i 2011 er der sket en ændring. Den 1. juli 2011 trådte § 26 d om kommuners billedoptagelser i forbindelse med tv-overvågning således i kraft.

Ikke kun ændringerne af selve loven gør, at der løbende sker en udvikling inden for det persondataretlige område. Også samfundsudviklingen i øvrigt, herunder den teknologiske udvikling, gør, at persondatalovens anvendelsesområde hele tiden udvides.

Biometri

Et af de områder, som er blevet mere og mere relevant er biometri, f.eks. i form af fingeraftryk.

Biometrisk teknologi anvendes i stigende omfang til personidentifikation i forbindelse med adgangs- og sikringssystemer. Pr. 1. januar 2012 skal alle nye pas have lagret fingeraftryk i passets chip. Dette vil gøre det vanskeligere at forfalske og misbruge pas.

Hvad er biometri?

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

De biometriske teknikker bygger f.eks. på elektronisk genkendelse af ansigt, øjne (iris), fingre (fingeraftryk), stemme, hænder, vener og gangart. Dette omfatter også genkendelse af såkaldte templates baseret på biometriske data, f.eks. en matematisk værdi af en borgers fingeraftryk.




Tidsregistrering af aktiverede borgere ved brug af fingeraftryk

Datatilsynet udtalte sig i 2011 om en kommunes brug af aktiverede borgeres fingeraftryk (templates) til tidsregistrering.

Datatilsynet fandt i sin udtalelse af 14. september 2011, at kommunens behandling af oplysninger om aktiverede borgeres møde- og sluttid var nødvendig af hensyn til udførelsen af kommunens opgaver. Endvidere fandt Datatilsynet ikke grundlag for at modsætte sig, at tidsregistreringen skete ved hjælp af fingeraftryk og templates. Behandlingen måtte således antages at ske i overensstemmelse med persondatalovens § 6, stk. 1, nr. 6, om myndighedsudøvelse.

Datatilsynet lagde vægt på det oplyste om, at registreringen havde til formål at kunne dokumentere borgernes fremmødetid, som dannede grundlag for udmåling af kontanthjælp, at systemet var pålideligt og præcist, samt at systemet var ukompliceret, idet det ikke krævede, at koder eller magnetkort skulle huskes. Herudover lagde tilsynet vægt på, at systemet hindrede omgåelse af registrering af mødetid, at der efter det oplyste alene registreredes en matematisk værdi af borgerens fingeraftryk (en template), og at det således ikke var det egentlige fingeraftryk, der registreredes i databasen.

Første højesteretsdom om persondataloven

Spørgsmål om fortolkning af persondataloven er i de forløbne år blevet vurderet af byretten og landsretten i enkelte konkrete retssager. Det er imidlertid i 2011, at Højesteret for første gang har vurderet en problemstilling vedrørende persondataloven.

Højesterets dom af 27. maj 2011 om videregivelse af oplysninger om jobansøger

A havde tidligere været ansat i kommunen K1. Under sygefraværssamtaler i K1 var A blevet konfronteret af sin leder B med mistanke om alkoholmisbrug, hvilket A benægtede. A søgte efterfølgende en stilling i kommunen K2. Under en samtale med D i kommunen K2 gav A tilladelse til, at D kunne indhente referenceoplysninger hos kommunen K1. D kontaktede herefter telefonisk K1 og talte med B, som bl.a. oplyste D om mistanken om alkoholmisbrug.

A anlagde herefter sag ved domstolene mod K1 og K2 med påstand om tilkendelse af en kompensation med henvisning til, at kommunerne havde overtrådt forvaltningsloven, helbredsoplysningsloven og persondataloven.

Højesteret fandt, at oplysninger om misbrug af nydelsesmidler, herunder alkohol, ikke kunne anses for helbredsoplysninger i helbredsoplysningslovens forstand, og at helbredsoplysningsloven derfor ikke fandt anvendelse i sagen.

For så vidt angår persondataloven blev det af Højesteret lagt til grund, at oplysningen om mistanken om alkoholmisbrug på tidspunktet for videregivelsen blev behandlet elektronisk i kommunen K1. Uanset at det måtte lægges til grund, at B under telefonsamtalen med D videregav de omhandlede oplysninger ud fra sin hukommelse, fandt Højesteret, at persondataloven fandt anvendelse. Dette gjaldt, selv om oplysningerne også fandtes på papir i A's personalesag[3]. Desuden fandt Højesteret, at der ikke forelå samtykke til den pågældende videregivelse af en følsom personoplysning, og at videregivelsen dermed var i strid med persondatalovens § 7, stk. 1. Derimod fandt Højesteret det ikke godtgjort, at K1 under sagsforløbet havde tilsidesat sin oplysningspligt over for A efter persondatalovens § 28 og § 29.

Højesteret fandt det ikke godtgjort, at A ville have opnået ansættelse i K2, hvis oplysningerne om mistanke om alkoholmisbrug ikke var blevet videregivet. A havde derfor ikke krav på erstatning som følge af den retsstridige videregivelse af oplysninger fra K1 til K2. K1 blev derimod pålagt at betale en godtgørelse på 25.000 kr. for tort til A i medfør af erstatningsansvarslovens § 26 som følge af den retsstridige videregivelse.

Hvad angår forvaltningsloven fandt Højesteret ikke tilstrækkeligt grundlag for at fastslå, at K2 havde indhentet oplysninger om A i strid med forvaltningslovens § 29, stk. 1 (om ansøgningssager). Derimod havde K2 overtrådt forvaltningslovens § 19 ved ikke at have hørt A over oplysningerne om det mulige alkoholmisbrug, inden den traf beslutning om ikke at tilbyde A ansættelse. Imidlertid lagde Højesteret til grund, at den manglende partshøring ikke havde betydning for K2' beslutning, og at der derfor ikke var grundlag for at pålægge K2 at betale erstatning eller godtgørelse til A herfor.

3 Videregivelsen fandt sted før ændringen af persondataloven i 2009, hvorefter manuel videregivelse mellem forvaltningsmyndigheder er omfattet af loven, jf. § 1, stk. 3




Første anvendelse af persondatalovens § 7, stk. 7

Det blev også i 2011, at Datatilsynet for første gang afgjorde en sag efter persondatalovens § 7, stk. 7. Efter denne bestemmelse kan undtagelse fra forbuddet i stk. 1 mod behandling af følsomme oplysninger om f.eks. helbredsforhold gøres, hvis behandlingen af de følsomme personoplysninger sker af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser. Datatilsynet skal give tilladelse hertil og underrette EU-Kommissionen herom.

Rådgivningscenters behandling af følsomme oplysninger om pårørende

Datatilsynet havde modtaget en anmeldelse fra et privat rådgivningscenter, som behandlede og rådgav børn og unge (klienter), hvis forældre var alvorligt syge eller døde. I forbindelse med behandlingen og rådgivningen behandlede centret følsomme oplysninger om de klienter, der kontaktede rådgivningscentret. Derudover behandlede centret oplysninger om de pårørendes helbredsmæssige forhold.

Datatilsynet udtalte i sit svar af 21. november 2011, at behandling af følsomme oplysninger om klienterne – f.eks. oplysninger om helbredsforhold og væsentlige sociale problemer – kun kunne ske med udtrykkeligt samtykke, jf. persondatalovens § 7, stk. 2, nr. 1, og § 8, stk. 4.

Hvad angår oplysninger om klienternes pårørende lagde Datatilsynet til grund, at ikke ville være praktisk muligt for rådgivningscentret i alle tilfælde at stille krav om udtrykkeligt samtykke fra disse. Tilsynet var imidlertid indstillet på at give tilladelse til indsamling og registrering af oplysninger om helbredsmæssige forhold om rådgivningscentrets klienters pårørende efter den særlige bestemmelse i persondatalovens § 7, stk. 7.

Datatilsynet fandt således, at der i dette konkrete tilfælde var knyttet en så vigtig samfundsmæssig interesse til rådgivningcentrets virksomhed, at der burde gives tilladelse til, at rådgivningscentret kunne indsamle og registrere oplysninger om klienternes pårørendes helbredsmæssige forhold i det omfang, indsamlingen og registreringen var nødvendig for behandling og rådgivning af barnet eller den unge. Datatilsynet lagde herved vægt på formålet med og indholdet af rådgivningscentrets virksomhed og på det oplyste om, at oplysninger om forælderens/søskendes sygdomsforløb, som det bliver oplevet af barnet/den unge, er af helt afgørende betydning for at kunne foretage en faglig vurdering af, hvilken behandling der skal iværksættes. Rådgivningscentret havde videre anført, at det var rådgivningscentrets erfaring, at det er nødvendigt med en vis detaljeringsgrad i for-

hold til dokumentationen af sygdomsforløbet, og at det ikke er tilstrækkeligt blot at skelne mellem, om barnets/den unges forælder er syg eller død.

Rådgivningscentret har efterfølgende modtaget tilladelse til behandlingen af følsomme oplysninger.

Datatilsynets kompetence

Et område, som jævnligt giver Datatilsynet anledning til overvejelser, er tilsynets kompetence i henhold til persondataloven, når den pågældende behandling af personoplysninger i et eller andet omfang også er reguleret i anden lovgivning end persondataloven. Det kan f.eks. være ved videregivelse af oplysninger i forbindelse med partshøring eller aktindsigt efter forvaltningslovens regler eller ved indsamling af oplysninger på det sociale område. I sådanne sager er Datatilsynet tilbageholdende med at gå ind i sagen, idet disse sager ofte vil kræve en vurdering af anden lovgivning end persondataloven. Datatilsynet vil således ofte henvise til den relevante klageinstans på området.

Datatilsynets kompetence til berigtigelse efter persondatalovens § 37

Datatilsynet har i 2011 behandlet to klagesager om berigtigelse af oplysninger hos Udlændingeservice. Begge sager drejede sig om berigtigelse af oplysninger om fødselsdato og den ene desuden om berigtigelse af fødselssted.

Datatilsynet udtalte i sine afgørelser af 6. december 2011, at det var tilsynets opfattelse, at tilsynet efter persondatalovens § 37 ikke havde mulighed for at efterprøve udlændingemyndighedernes afgørelser om fastlæggelse af klagernes fødselsdato og fødselssted.

Datatilsynet lagde vægt på, at fastlæggelsen af klagernes identitet, herunder fødselsdato og fødselssted, var central for klagernes retsstilling efter udlændingelovgivningen, og at afgørelserne herom derfor havde karakter af en egentlig materiel prøvelse, som det var udlændingemyndighedernes kompetence at foretage som led i behandlingen af klagernes sager efter udlændingelovgivningen. Persondatalovens § 37 tilsigter efter Datatilsynets opfattelse ikke at give tilsynet kompetence til at vurdere indholdsmæssige spørgsmål, der er reguleret af anden lovgivning som eksempelvis udlændingelovgivningen.

Tv-overvågning

Persondataloven regulerer den behandling af personoplysninger, som tv-overvågning indebærer. Loven gælder for virksomheder, organisationer og offentlige myndigheder.

Når det gælder selve afgrænsningen af, hvilke områder der må overvåges, er det som regel tv-overvågningsloven, som er det relevante regelsæt.

Kommunernes tv-overvågning

I 2011 vedtog Folketinget ændringer i tv-overvågningsloven og persondataloven. Forinden havde der været en høringsrunde, hvor bl.a. Datatilsynet havde fremsat bemærkninger og udtrykt generel betænkelighed ved forslaget. Ændringerne trådte i kraft den 1. juli 2011.

Med ændringerne har kommunerne fået en øget adgang til at foretage tv-overvågning i det offentlige rum. Kommunerne kan tv-overvåge som led i en generel tryghedsskabende indsats i nær tilknytning til boligområder, som i henhold til en polititilladelse bliver tv-overvåget af en almen boligorganisation eller andre organisationer eller foreninger, der repræsenterer husstandene i boligområdet.

Det er en betingelse, at tv-overvågningen fremmer trygheden for borgerne, som færdes i området, f.eks. fordi området bliver præget af uro og hærværk.

Det er endvidere en betingelse, at den utryghed, som overvågningen skal bekæmpe, skyldes kriminalitet eller andre utryghedsskabende former for adfærd, der udspringer af de samme forhold, som har ført til, at politiet har givet boligorganisationen tilladelse til tv-overvågning.

Kommunerne skal inden iværksættelse af tv-overvågning efter den nye regel drøfte behovet for overvågningen med politiet, som kan bidrage med synspunkter, f.eks. med hensyn til, hvor der især kan være behov for en særlig tryghedsskabende indsats.

Persondatalovens regler gælder generelt for kommunernes håndtering af personoplysninger i forbindelse med tv-overvågning. Det indebærer bl.a., at lovens krav om information til de personer, der overvåges, skal opfyldes. Endvidere indebærer persondatalovens krav

om behandlingssikkerhed, at de personoplysninger, der indgår i optagelserne, skal være beskyttet mod misbrug og mod, at de kommer til uvedkommendes kendskab.

I persondatalovens § 26 d er der desuden fastsat særlige retningslinjer for kommunens behandling af optagelser fra tv-overvågning i medfør af den nye bestemmelse i tv-overvågningslovens § 2 a.

Denne regel indebærer bl.a., at en kommune kun må anvende eller gennemse de nævnte optagelser, hvis det sker med henblik på at fremme trygheden for personer, som færdes i området, eller hvis der er samtykke fra samtlige personer på optagelserne.

De nye regler i tv-overvågningsloven og persondataloven

Tv-overvågningsloven:
§ 2 a. En kommunalbestyrelse kan efter drøftelse med politidirektøren med henblik på at fremme trygheden foretage tv-overvågning af offentlig gade, vej, plads eller lignende område, som benyttes til almindelig færdsel, og som ligger i nær tilknytning til et område, der tv-overvåges i medfør af § 2, stk. 2.

Persondataloven:
§ 26 d. En kommune må kun behandle billedoptagelser med personoplysninger, der optages i forbindelse med tv-overvågning omfattet af § 2 a i lov om tv-overvågning, hvis
1) den registrerede har givet sit udtrykkelige samtykke til behandlingen eller
2) behandlingen sker med henblik på at fremme trygheden for personer, som færdes i det tv-overvågede område.
Stk. 2. Optagelser som nævnt i stk. 1 må videregives i de tilfælde, der er nævnt i § 26 a, stk. 1.
Stk. 3. Optagelser som nævnt i stk. 1 skal slettes, senest 30 dage efter at optagelserne er foretaget.

Tv-overvågningsinspektioner hos kommuner i 2011

Datatilsynet har mulighed for at foretage inspektioner (kontrolbesøg) hos alle offentlige myndigheder og private dataansvarlige, der behandler personoplysninger i forbindelse med tv-overvågning.

I efteråret 2011 har Datatilsynet bl.a. gennemført en række inspektioner i Greve. Her besøgte tilsynet en række butikker samt Greve Kommune.

Datatilsynet var i 2011 på fem kommuneinspektioner målrettet tv-overvågning. Ingen af de fem kommuner havde gjort brug af de nye regler om tv-overvågning i det offentlige rum.

Hos to af de inspicerede kommuner udtalte Datatilsynet kritik og underrettede kommunaldirektørerne i de pågældende kommuner om, at kommunerne havde overtrådt persondataloven. Nogle af overtrædelserne var bl.a. manglende sikkerhedsregler vedrørende tv-overvågning, opbevaring af optagelser fra tv-overvågning i mere end 30 dage og manglende information til medarbejdere, faste brugere, børn og forældre, der færdes på områder, hvor kommunen foretager tv-overvågning.

Læs mere om tv-overvågning

På Datatilsynets hjemmeside kan du læse om dine rettigheder i forbindelse med tv-overvågning. Du finder teksterne om rettighederne under punktet Borger ⇢ Tv-overvågning.

Der findes også underpunkter om tv-overvågning under punkterne Offentlig og Erhverv. Her kan du bl.a. læse om persondatalovens krav om datasikkerhed i forbindelse med tv-overvågning.

Datatilsynet offentliggør også sine afgørelser om tv-overvågning på hjemmesiden. Disse kan du finde under punktet Afgørelser.

I øvrigt har Datatilsynet i samarbejde med Justitsministeriet udformet en pjece om tv-overvågning. Den kan læses på tilsynets hjemmeside under Publikationer.

Advarselsregistre

Anmeldelse og tilladelse

Hvis en privat dataansvarlig ønsker at behandle oplysninger med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret person eller virksomhed mv., skal der foretages anmeldelse heraf til Datatilsynet. Den dataansvarlig skal derudover have en tilladelse fra Datatilsynet. Det følger af persondatalovens § 50, stk. 1, nr. 2.

Ved Datatilsynets vurdering af, om en ansøgning om tilladelse til oprettelse af et advarselsregister kan imødekommes, lægger tilsynet vægt på, om oprettelsen af advarselsregistret tjener anerkendelsesværdige interesser. Herudover foretager Datatilsynet en vurdering af, om den anmeldte behandling af oplysninger i forbindelse med advarselsregistret i øvrigt opfylder persondatalovens krav.

I Datatilsynets praksis, som er en videreførelse af Registertilsynets praksis, er det fast antaget, at de restriktive betingelser for behandling af oplysninger om strafbare forhold i den private sektor i persondatalovens § 8, stk. 4 og 5, ikke giver mulighed for registrering og videregivelse af oplysninger om strafbare forhold i forbindelse med førelsen af et advarselsregister.

Datatilsynet har i 2011 behandlet en række sager vedrørende oprettelse af advarselsregistre.

Oplysninger om virksomheder mv. i advarselsregistre

Persondataloven gælder som udgangspunkt kun for oplysninger om personer. Det fremgår af lovens § 1, stk. 1-3. Men når der er tale om advarselsregistre, gælder loven også for oplysninger om virksomheder, foreninger mv. Det fremgår af lovens § 1, stk. 4.

Tilladelse og vilkår

Datatilsynet fastsætter vilkår i forbindelse med en tilladelse til at føre et advarselsregister. Det er vilkår om, hvornår der må ske registrering i advarselsregistret. Herudover fastsætter Datatilsynet en række standardmæssige vilkår om oplysningspligt, indsigtsret, sletning og sikkerhed. Eksempler på vilkår for advarselsregistre kan ses på Datatilsynets hjemmeside under punktet Erhverv ⋯› Advarselsregistre.

Klage til Datatilsynet

En person eller virksomhed mv., som er blevet registreret i et advarselsregister, kan klage til Datatilsynet, hvis vedkommende mener, at der er sket behandling i strid med tilsynets tilladelse, f.eks. hvis der ikke er sket den nødvendige sletning, eller hvis der sker behandling af urigtige oplysninger. Den registrerede skal dog i første omgang rette henvendelse til den dataansvarlige herom.

Frivillig registrering for at undgå gældssætning og evt. identitetstyveri ikke et advarselsregister

Datatilsynet modtog i slutningen af 2010 en forespørgsel vedrørende etablering af et register, som havde til formål – via en frivillig registrering baseret på et udtrykkeligt samtykke – at "advare" andre imod umiddelbart at indgå i kreditforhold med de registrerede.

Det fremgik af henvendelsen, at den dataansvarlige ønskede at registrere oplysninger om 1) personer, som af den ene eller anden grund ønskede at gøre potentielle kreditgivere opmærksomme på, at disse ikke umiddelbart skulle sige ja til at give vedkommende kredit, og 2) personer, som havde mistet et identitetspapir og i den forbindelse var bekymret for, at det ville blive misbrugt. Det fremgik endvidere, at der i visse tilfælde skulle registreres og videregives oplysninger om årsag til registrering i registret.

Datatilsynet udtalte den 16. august 2011, at der ved vurderingen af, om en behandling kan anses for at være et advarselsregister, skal lægges vægt på, om registret er oprettet med henblik på videregivelse, og om videregivelsen sker med henblik på at advare mod forretningsforbindelser med eller ansættelsesforhold til de registrerede. Tilsynet udtalte endvidere, at den typiske behandling i form af et advarselsregister er et register, der er oprettet af en forening eller en brancheorganisation med henblik på at videregive oplys-

ninger til foreningens eller brancheorganisationens medlemmer om medlemmernes forretningsforbindelser og disses betalingsevne.

Datatilsynet udtalte herefter, at den påtænkte registrering og videregivelse af oplysninger om frivillig registrering samt årsag hertil efter tilsynets opfattelse ikke udgjorde et advarselsregister efter persondatalovens § 50, stk. 1, nr. 2. Datatilsynet lagde herved vægt på, at der var tale om frivillige registreringer, at en registrering ikke nødvendigvis var udtryk for, at den registrerede var "dårlig betaler", samt at det måtte antages at være i de registreredes interesse, at de pågældende oplysninger blev videregivet til potentielle kreditorer.

Datatilsynet foretog herefter en vurdering af, om den påtænkte registrering og videregivelse af oplysninger ville kunne finde sted inden for persondatalovens rammer. Datatilsynet udtalte, at registrering og videregivelse af oplysninger om frivillig registrering kunne ske på baggrund af udtrykkeligt samtykke, jf. persondatalovens § 6, stk. 1, nr. 1. For så vidt angik oplysninger om årsag til registrering var det Datatilsynets opfattelse, at oplysninger om mistede identitetspapirer og frygt for misbrug heraf kunne registreres og videregives på baggrund af udtrykkeligt samtykke. Tilsynet fandt derimod, at oplysninger om øvrige årsager til frivillig registrering ikke kunne registreres og videregives på baggrund af udtrykkeligt samtykke. Tilsynet henviste herved til de grundlæggende krav i persondataloven om god databehandlingsskik, saglighed og proportionalitet.

Liste over advarselsregistre

En liste over virksomheder, der har tilladelse til at føre advarselsregister, kan findes på Datatilsynets hjemmeside. Listen findes ved i Fortegnelsen på tilsynets hjemmeside at søge i rubrikken journalnummer og skrive "-43-".

Register over lejere, der har misligholdt lejemål eller lejeaftale

Datatilsynet blev i 2011 gennem omtale i medierne opmærksom på, at Sammenslutningen af Private Udlejere (SAPU) førte en liste over "dårlige" lejere.

Datatilsynet sendte i den anledning et påbud til SAPU om at stoppe indsamling og videregivelse af oplysninger om lejere samt om at slette alle oplysninger om strafbare forhold. Påbuddet var bl.a. begrundet med, at der ikke var foretaget anmeldelse til og indhentet

tilladelse fra Datatilsynet, og at SAPU ikke havde hjemmel til at behandle oplysninger om strafbare forhold.

SAPU indsendte efterfølgende en anmeldelse vedrørende registret over "dårlige" lejere (betegnet SAPU Listen) til Datatilsynet. Af anmeldelsen fremgik bl.a., at formålet med advarselsregistret var at advare private udlejere mod personer eller virksomheder, der tidligere havde misligholdt lejemål eller lejeaftale.

Datatilsynet udtalte den 1. december 2011, at tilsynet var indstillet på at meddele tilladelse til advarselsregistret på nærmere angivne vilkår. Af de beskrevne vilkår fremgik bl.a., *at* der – under nærmere angivne omstændigheder – alene måtte ske behandling af oplysninger om 1) ophævelse af lejemål på grund af for sen betaling af leje, 2) misligholdelse af lejemåls stand, 3) manglende vedligeholdelse af lejemål og 4) manglende oplysning af den adresse, den tidligere lejer var flyttet til, i tilfælde hvor der var et økonomisk mellemværende mellem lejer og udlejer, og fordringen ikke var bestridt, *at* der ikke måtte ske behandling af oplysninger om ophævelse af lejemål på grund af for sen betaling af leje, hvis berettigelsen af ophævelsen var bestridt, *at* der alene måtte ske behandling af oplysninger om misligholdelse eller manglende vedligeholdelse af lejemål, såfremt der forelå en endelig afgørelse fra Huslejenævnet, ankenævnet i Københavns Kommune eller Boligretten (eller højere instans), der fastslog, at der forelå en misligholdelse eller manglende vedligeholdelse som nævnt i tilsynets vilkår, og lejeren nægtede at følge denne afgørelse, samt *at* der alene måtte registreres og videregives summariske oplysninger om, hvorvidt indberetningen tilhørte ovennævnte kategori 1, 2, 3 eller 4.

Binding Corporate Rules (BCR)

Bindende virksomhedsregler

Hvis en dataansvarlig vil overføre oplysninger til tredjelande, der ikke sikrer et tilstrækkeligt beskyttelsesniveau, skal den dataansvarlige som udgangspunkt indhente Datatilsynets tilladelse hertil.

Hvad er et tredjeland?

Et tredjeland er en stat, som ikke indgår i Det Europæiske Fællesskab eller er et af de såkaldte EØS-lande. Dette betyder, at f.eks. Norge og Island ikke er tredjelande, men USA og Indien er.

Datatilsynet kan give tilladelse til, at der overføres oplysninger til tredjelande, som ikke sikrer et tilstrækkeligt beskyttelsesniveau, hvis den dataansvarlige yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder. Dette kan f.eks. gøres ved anvendelse af de såkaldt bindende virksomhedsregler (BCR).

BCR er regler, der vedtages for en koncern, som har virksomheder i flere lande, herunder tredjelande. Reglerne skal være bindende for samtlige enheder og virksomheder i koncernen og kan således ikke anvendes som hjemmel for overførsel af oplysninger til virksomheder, som ikke er en del af koncernen.

Når bindende virksomhedsregler skal godkendes, anvendes en særlig procedure, der er fastsat af Artikel 29-gruppen (læs mere om Artikel 29-gruppen under afsnittet Internationalt samarbejde). Proceduren går ud på, at de bindende virksomhedsregler i første omgang udelukkende fremsendes til databeskyttelsesmyndigheden i det EU-land, hvor koncernens europæiske hovedkvarter ligger. Herefter koordinerer den pågældende myndighed – den såkaldte "lead authority" – godkendelse fra de øvrige implicerede EU-lande.

Når reglerne er godkendt af databeskyttelsesmyndighederne i de EU-lande, hvorfra koncernen ønsker at overføre oplysninger, kan der i princippet frit overføres oplysninger mellem koncernens virksomheder, hvis disse lever op til kravene i de bindende virksomheds-

regler samt reglerne i databeskyttelseslovgivningen i øvrigt. I Danmark er det et krav efter persondatalovens § 27, stk. 4, at virksomheden får Datatilsynets tilladelse til at overføre oplysningerne på baggrund af de bindende virksomhedsregler. De bindende virksomhedsregler skaber udelukkende hjemmel til at føre oplysningerne ud af EU's område til et tredjeland. Der skal således fortsat være hjemmel til f.eks. selve det at *videregive* oplysningerne, jf. persondatalovens § 27, stk. 5.

Datatilsynets arbejde med BCR i 2011

I 2011 kunne Datatilsynet for første gang som "lead authority" for en dansk virksomhed færdiggøre proceduren med at få godkendt en BCR.

Arbejdet med den første danske BCR startede allerede i 2009, da Novo Nordisk A/S pegede på Datatilsynet som koordinerende myndighed for virksomhedens BCR.

Det stod hurtigt klart for Datatilsynet, at processen med at udarbejde og efterfølgende få godkendt de bindende virksomhedsregler i de øvrige EU-lande ville være mere omfattende end først antaget. Det var således først i slutningen af 2011, at godkendelsesproceduren for den første danske BCR endelig kunne afsluttes.

Arbejdet med Novo Nordisk A/S' bindende virksomhedsregler har været en lærerig proces for Datatilsynet. Tilsynet har via samarbejdet med Novo Nordisk A/S og de øvrige EU-landes databeskyttelsesmyndigheder tilegnet sig en større viden om bl.a. de forskellige hensyn, som henholdsvis de private virksomheder og de forskellige databeskyttelsesmyndigheder mener, at en BCR skal varetage.

Datatilsynet er efterfølgende blevet kontaktet af andre danske virksomheder, der ligesom Novo Nordisk A/S ønsker en mere smidig udveksling af personoplysninger inden for deres koncern.

Internationalt BCR-samarbejde

Datatilsynet har også i 2011 deltaget i den såkaldte BCR Subgroup, der er en arbejdsgruppe under Artikel 29-gruppen. Undergruppen har i 2011 haft 3 møder, hvor aktuelle problemstillinger i BCR-sammenhæng er blevet diskuteret. Der har endvidere været afholdt 1 undervisningsseminar for medlemmer af undergruppen med henblik på at skabe større viden om BCR.

Læs mere

På Datatilsynets hjemmeside under punktet Erhverv ⇢ Tredjelande ⇢ Binding Corporate Rules (BCR) findes links til Artikel 29-gruppens udtalelser (de såkaldte "working papers") om BCR. Endvidere findes link til et eksempel på Datatilsynets tilladelse til overførsel af personoplysninger på grundlag af en BCR.

Kreditoplysning

Klager over registrering

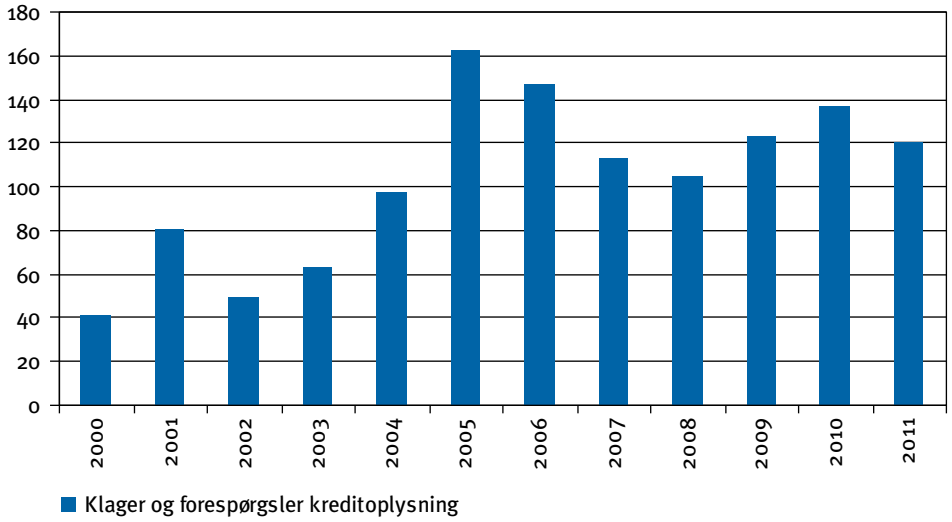
Registrering hos kreditoplysningsbureauer er et område, hvor Datatilsynet modtager mange klager. Klagerne vedrører både private personer og virksomheder.

Persondataloven gælder også for oplysninger om virksomheder, hvis behandlingen af oplysninger udføres for et kreditoplysningsbureau. Det fremgår af lovens § 1, stk. 4.

De fleste sager vedrørende kreditoplysning er klager over indberetninger fra private virksomheder. Offentlige myndigheder kan også indberette til kreditoplysningsbureauer efter særlige regler i persondatalovens kapitel 5.

Antallet af henvendelser på kreditoplysningsområdet svinger noget fra år til år, men tendensen er et stigende antal sager for Datatilsynet på dette område.

Klager og forespørgsler kreditoplysning



Nye problemstillinger på kreditoplysningsområdet

Reglerne for kreditoplysningsbureauer er stort set en videreførelse af de regler, der var gældende før persondatalovens ikrafttræden. Datatilsynet har på denne baggrund en omfattende praksis. Nye problemstillinger dukker dog fortsat op.

Betalingspåkrav

I 2011 har Datatilsynet bl.a. taget stilling til indberetning til kreditoplysningsbureauer fra finansielle virksomheder på baggrund af et betalingspåkrav.

Finanstilsynet har fastsat retningslinjer for pengeinstitutters indberetning til kreditoplysningsbureauer. De særlige retningslinjer finder bl.a. anvendelse på pengeinstitutter, realkreditinstitutter og forsikringsselskaber.

Af disse retningslinjer fremgår bl.a., at hvis kreditor har et grundlag for tvangsfuldbyrdelse efter retsplejelovens § 478, f.eks. lånedokumenter, visse gældsbreve og pantebreve, og kan gå direkte i fogedretten, må indberetning til et kreditoplysningsbureau først finde sted, når der har været afholdt møde i fogedretten, og der er sket tilførsel (registrering) til fogedprotokollen.

I forbindelse med en konkret klagesag hørte Datatilsynet Finanstilsynet om, hvornår der kan ske videregivelse til et kreditoplysningsbureau på baggrund af behandlingen af et betalingspåkrav i retten.

Finanstilsynet fandt, at der er tale om en berettiget videregivelse efter lov om finansiel virksomheds § 117, stk. 1, når et pengeinstitut videregiver oplysning om en kundes gældsforhold til et kreditoplysningsbureau i en situation, hvor et betalingspåkrav af fogedretten er givet påtegning om, at der ikke rettidigt er modtaget indsigelser mod kravet.

Der kan derfor ske indberetning til et kreditoplysningsbureau af krav – der i øvrigt opfylder kravene for indberetning – hvis der er givet påtegning om, at fogedretten ikke har modtaget indsigelser mod et betalingspåkrav. Dette er også tilfældet ved indberetning fra ikke finansielle virksomheder.

Hvad er et betalingskrav?

Et betalingspåkrav er et dokument, som kreditor kan indlevere til fogedretten, når vedkommende ønsker at starte en forenklet inkassoproces mod en skyldner. Når fogedretten modtager et betalingspåkrav, sendes dette til forkyndelse for skyldner. Hvis skyldner ikke reagerer indenfor 14 dage efter forkyndelsen, påtegner fogedretten påkravet, hvorved det får samme bindende virkning som en dom.

Rekonstruktion

Ved en ændring af konkursloven, der trådte i kraft den 1. april 2011, blev der indført regler om rekonstruktion af insolvente selskaber. Samtidig ophævedes konkurslovens kapital 12 om betalingsstandsning.

I modsætning til reglerne om betalingsstandsning offentliggøres oplysning om rekonstruktion i Statstidende i forbindelse med skifterettens indkaldelse af fordringshaverne til møde.

På baggrund af de nye regler har Datatilsynet vurderet, at en oplysning om rekonstruktion, der er offentliggjort i Statstidende, kan registreres af kreditoplysningsbureauer i op til 5 år.

I den forbindelse har Datatilsynet udsendt et brev af 5. januar 2012 til samtlige kreditoplysningsbureauer, hvor der redegøres for, hvornår der kan ske registrering af en oplysning om rekonstruktion, og hvornår der skal ske sletning. Brevet kan læses på Datatilsynets hjemmeside under punktet Afgørelser.

Internationalt samarbejde

Europol

Tilsynet med Europol

Europol, der fysisk er placeret i Haag i Holland, har til opgave at beskæftige sig med grov, grænseoverskridende kriminalitet, f.eks. terrorisme og organiseret kriminalitet.

Til det formål tilflyder der løbende Europol oplysninger fra medlemsstaterne om bl.a. forbrydelser, hændelser og mistænkte, hvor der er grænseoverskridende elementer, og hvor forbrydelsen har en grov karakter.

I Danmark er det Rigspolitiet, der er udpeget som national enhed, mens Datatilsynet er national kontrolinstans. Som national enhed er Rigspolitiet bindeled mellem danske myndigheder og Europol. Datatilsynet har opgaven med at føre tilsynet med Rigspolitiets varetagelse af opgaver efter Rådets afgørelse af 9. april 2009 om oprettelse af Den Europæiske Politienhed (Europol).

I forhold til tilsynet med Europols behandling af personoplysninger er der efter rådsafgørelsens art. 34 oprettet Den Fælles Kontrolinstans. Datatilsynet er repræsenteret med to medlemmer i Den Fælles Kontrolinstans, hvoraf ét medlem ligeledes er indtrådt i Det Fælles Klageudvalg. Det Fælles Klageudvalg behandler konkrete klager over Europols behandling af oplysninger, f.eks. manglende indsigt hos Europol.

I Den Fælles Kontrolinstans har der i 2011 været afholdt fem møder, hvor man bl.a. har drøftet resultatet af kontrolinstansens første inspektion målrettet Europols rolle i TFTP-aftalen mellem USA og EU. I marts 2011 afgav Den Fælles Kontrolinstans en udtalelse om inspektionen, hvor kontrolinstansen konkluderede, at den betydelige anvendelse af mundtligt formidlede oplysninger mellem de amerikanske myndigheder og Europol umuliggjorde både intern revision ved den lokale databeskyttelsesofficer og ekstern kontrol ved Den Fælles Kontrolinstans.

Udtalelserne fra Den Fælles Kontrolinstans kan findes via link fra Datatilsynets hjemmeside under punktet Internationalt ⇢ Europol.

Det Fællesklageudvalg har i 2011 afholdt fire møder. Klageudvalget har i 2011 truffet afgørelse i to klagesager, der også findes omtalt på kontrolinstansens hjemmeside.

Schengen

Schengenevaluering på databeskyttelsesområdet

Danmark er i 2011 blevet evalueret bl.a. på databeskyttelsesområdet i forhold til de krav, som Schengenreglerne opstiller. Evalueringen blev varetaget af databeskyttelseseksperter fra en række af EU's medlemsstater.

Evalueringen fandt sted i oktober 2011, men selve processen startede allerede i sommeren 2010 med besvarelse af et spørgeskema. Datatilsynet stod for afholdelsen af evalueringen, hvor Udenrigsministeriet, Udlændingeservice, Rigspolitiet samt CSC Danmark A/S som databehandler for Rigspolitiet også var involveret. Efter evalueringen skal Datatilsynet følge op på de anbefalinger/bemærkninger, som evalueringsholdet er kommet med.

Om Schengen-konventionen

Konvention om gennemførelse af Schengen-aftalen af 14. juni 1985 mellem regeringerne i Den Økonomiske Union Benelux, Forbundsrepublikken Tyskland og Den Franske Republik om gradvis ophævelse af kontrollen med de fælles grænser.

Konventionen har til formål at etablere fri personbevægelighed over de indre grænser samt at styrke indsatsen mod international kriminalitet og illegal indvandring. Til opfyldelse af formålene skal der bl.a. ske udveksling af oplysninger og erfaringer til brug for de enkelte landes bekæmpelse af kriminalitet.

Folketinget bemyndigede ved lov nr. 418 af 10. juni 1997 om Danmarks tiltrædelse af Schengenkonventionen (Schengenloven) regeringen til at ratificere tiltrædelsesaftalen på Danmarks vegne, og ratifikationen fandt sted den 23. september 1997.

Inspektion af Rigspolitiet

Datatilsynet har i 2011 gennemført en inspektion hos Rigspolitiet i forhold til myndighedens rolle efter Schengenreglerne. Ved inspektionen gennemgik tilsynet bl.a. Rigspolitiets procedurer for håndteringen af specifikke indberetningstyper. Derudover foretog Datatilsynet en fysisk besigtigelse af de faciliteter, som Rigspolitiets særlige afdeling, der bl.a. indberetter til Schengen-informationssystemet (SIS), har til rådighed.

I medfør af § 2, stk. 2, i Schengenloven er Rigspolitiet udpeget som central myndighed efter Schengen-konventionens artikel 108, stk. 1. Rigspolitiet er i medfør af denne artikel ansvarlig for den nationale del af Schengen-informationssystemet, herunder danske indberetninger efter artiklerne 95-100.

Efter samme lovs § 2, stk. 3, er Datatilsynet udpeget som tilsynsmyndighed efter Schengen-konventionens artikel 114 og 128. Datatilsynet har således bl.a. til opgave i overensstemmelse med national lovgivning at føre et uafhængigt tilsyn med databasen i den nationale del af Schengen-informationssystemet samt at kontrollere, at behandlingen og anvendelsen af de oplysninger, der er optaget i Schengen-informationssystemet, ikke krænker de berørte personers rettigheder.

JSA Schengen

Den Fælles Tilsynsmyndighed Schengen (JSA Schengen) fører bl.a. tilsyn med Schengen-informationssystemets tekniske støttefunktion (C.SIS), som fysisk er placeret i Strasbourg.

I JSA Schengen, hvor Datatilsynet er repræsenteret med to medlemmer, er der i 2011 blevet afholdt fire møder. Her har man bl.a. diskuteret udviklingen af et nyt computersystem til Schengen-informationssystemet samt tilrettelæggelsen af to undersøgelser, hvoraf den ene er en opfølgning på en tidligere gennemført undersøgelse vedrørende Schengen-konventionens artikel 99 (vedrørende diskret overvågning / målrettet kontrol).

Hvad er Schengen-informationssystemet?

Schengen-informationssystemet (SIS) er et fælles edb-baseret informationssystem, som skal sikre en hurtig og sikker udveksling af oplysninger mellem Schengen-landene. Systemet består af en national del i hvert Schengen-land (N.SIS) og en central teknisk støttefunktion (C.SIS), som ligger i Strasbourg. Myndighederne i Schengen-landene kan trække på oplysningerne i SIS i forbindelse med udførelsen af politimæssige opgaver og administrationen af udlændingelovgivningen. Medlemslandene kan til SIS bl.a. foretage indberetning af personer, der ønskes udleveret, og uønskede udlændinge, der nægtes indrejse.

Læs mere om SIS på Datatilsynets hjemmeside under punktet Internationalt ⇢ Schengen.

Told-informationssystemet

Told-informationssystemet (CIS) har til formål at 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.

Datatilsynet er af Skatteministeriet blevet anmodet om påtage sig opgaven som national tilsynsmyndighed vedrørende SKATs brug af Told-informationssystemet. Som national tilsynsmyndighed deltager Datatilsynet også i Den Fællestilsynsmyndighed Toldinformationssystemet. Denne myndighed fører tilsyn med en central database, som er oprettet i EU-regi i Bruxelles, med terminaladgang for samtlige medlemsstaters myndigheder.

Der er i 2011 blevet afholdt fire møder i Den Fælles Kontrolinstans Told-informations-systemet, hvor man bl.a. har drøftet udarbejdelsen af en håndbog til et nyt europæisk sagsbehandlingssystem på skatteområdet (FIDE) og forholdet til ny EU-lovgivning i form af Rådets rammeafgørelse 2008/977/RIA.

Rådets rammeafgørelse

Rådets rammeafgørelse 2008/977/RIA om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager er implementeret i dansk ret ved bekendtgørelse nr. 1287 af 25. november 2010. Rammeafgørelsen er nærmere omtalt i Datatilsynets årsberetning 2008-2009, side 38.

Eurodac

Efter udlændingelovens regler fører Datatilsynet tilsyn med behandlingen og anvendelsen af de oplysninger, der er videregivet og modtaget efter reglerne i Eurodac-forordningen. På denne baggrund deltager Datatilsynet også i møder med andre nationale databeskyttelsesmyndigheder samt Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). Disse møder sker i gruppen Eurodac Supervision Coordination Group (ESCG). EDPS fører tilsynet med den centrale Eurodacenhed, mens de enkelte, deltagende medlemsstater fører tilsyn med de fingeraftryk, de selv indfører i Eurodac.

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.

Datatilsynet har i 2011 bidraget til en rapport om sletning af fingeraftryk (advance deletion), der er udarbejdet af EDPS. Rapporten er offentliggjort på EDPS' hjemmeside, hvortil der er link fra Datatilsynets hjemmeside under punktet Internationalt ⇢ EDPS.

I 2011 blev der i ESCG afholdt 2 møder, hvor man bl.a. drøftede en skabelon til gennemførelse af nationale sikkerhedsinspektioner af Eurodac-systemet. Under møderne orienterer Kommissionen gruppen om tekniske og lovgivningsmæssige tiltag, der vedrører Eurodac, ligesom gruppen får mulighed for at stille Kommissionens repræsentanter spørgsmål.

Om Eurodac

Eurodac består af en central enhed, der er oprettet i Europa-Kommissionen, og som driver en central edb-database med fingeraftryksoplysninger, samt de elektroniske midler til videregivelse mellem medlemsstaterne og den centrale database. Gennem databasen kan myndighederne i en medlemsstat tjekke, om en asylansøger tidligere har søgt asyl i en anden medlemsstat.

Visum-informationssystemet (VIS)

I 2011 startede udrulningen af det nye europæiske system til behandling af visumansøgninger ved repræsentationerne – VIS. Således har alle EU-repræsentationer i Nordafrika i efteråret 2011 implementeret det nye system, der har været undervejs siden juni 2002.

Ved Rådets beslutning af 8. juni 2004 om indførelse af visuminformationssystemet (VIS) blev det, jf. artikel 1, besluttet, at der indføres et system (VIS) til udveksling af visumoplysninger mellem medlemsstaterne, som skal give kompetente nationale myndigheder mulighed for at indlæse og opdatere visumdata og konsultere dem elektronisk. Siden er kommet bl.a. Europa-parlamentets og Rådets forordning af 9. juli 2008 om visum-informationssystemet og udveksling af oplysningerne mellem medlemsstaterne om visa til kortvarigt ophold (VIS-forordningen).

VIS består af en central enhed (C-VIS) samt nationale adgangspunkter (DK-VIS i Danmark). VIS-databasen indeholder oplysninger om visumansøgere og andre relevante personer, bl.a. pårørende og arbejdsgivere, samt visumansøgerens fingeraftryk.

For så vidt angår medlemsstaternes behandling af personoplysninger i VIS gælder national databeskyttelseslovgivning (persondataloven i Danmark), hvorimod C-VIS er underlagt de regler, der gælder for Den Europæiske Unions institutioner, jf. Europa-parlamentets og Rådets forordning (EF) 2001/45 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger.

Artikel 29-gruppen

Artikel 29-gruppen er nedsat i henhold til artikel 29 i det generelle databeskyttelsesdirektiv [4] . Gruppen er uafhængig og rådgiver EU-Kommissionen om persondataretlige emner. Den består af repræsentanter fra de nationale databeskyttelsesmyndigheder i EU (samt andre europæiske lande, der har status som observatører), en repræsentant fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) samt en repræsentant fra Kommissionen. Det danske datatilsyn repræsenteres sædvanligvis af tilsynets direktør.

Artikel 29-gruppen har i 2011 afholdt 6 møder i Bruxelles. I 2011 har et af de vigtigste emner været den fremtidige regulering af databeskyttelsesområdet i EU.

Artikel 29-gruppens arbejdsprogram og pressemeddelelser om afholdte møder er tilgængelige på gruppens hjemmeside, hvortil der er link fra Datatilsynets hjemmeside under punktet Internationalt ⇢ Artikel 29-gruppen.

Der er nedsat flere arbejdsgrupper (subgroups) under Artikel 29-gruppen. Datatilsynet har deltaget i fem af disse underarbejdsgrupper:

- Technology Subgroup, som særligt arbejder med beskyttelse af personoplysninger i forbindelse med anvendelse af internet og ny teknologi
- BCR Subgroup, som arbejder med Binding Corporate Rules (BCR)
- Health Data Subgroup, som har arbejdet med epSOS (European Patients Smart Open Services) vedrørende elektronisk udveksling af patientoplysninger i EU
- BTLE Subgroup (Borders Travel Law-Enforcement), som arbejder med spørgsmål om beskyttelse af personoplysninger i forhold til retshåndhævelse og aktiviteter vedrørende rejsende, f.eks. flypassagerer
- Financial Matters Subgroup, som særligt arbejder med beskyttelse af personoplysninger i relation til den finansielle sektor, herunder TFTP-aftalen med USA

4 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

I 2011 har Artikel 29-gruppen vedtaget en række henstillinger, udtalelser mv. Således har gruppen bl.a. lavet udtalelser om geolocations services on smartphones og om begrebet samtykke. Der er link til disse dokumenter på Datatilsynets hjemmeside under punktet Internationalt ⇢ Artikel 29-gruppen.

WPPJ

Ud over deltagelsen i Artikel 29-gruppen og de fælles kontrolinstanser for særlige europæiske systemer deltager Datatilsynet i møder i arbejdsgruppen Working Party on Police and Justice (WPPJ).

Om WPPJ

WPPJ er nedsat af de europæiske datatilsyn.

Arbejdsgruppen WPPJ undersøger udviklingen inden for det strafferetlige område med særlig fokus på databeskyttelsesretlige problemstillinger. WPPJ forbereder forslag, udkast til skrivelser mv. til datatilsynenes konferencer med henblik på fremsendelse til EU-institutioner og andre interessenter.

I 2011 har WPPJ afholdt 4 møder. Fokus har særligt været på anvendelsen af biometriske data inden for det strafferetlige samarbejde samt implementeringen af Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager.

Eurojust

Eurojust er et EU-organ, som blev oprettet i 2002 for at forbedre de kompetente myndigheders effektivitet inden for EU's medlemsstater, når myndighederne beskæftiger sig med efterforskning og retsforfølgning af alvorlig grænseoverskridende og organiseret kriminalitet. For at udføre sine opgaver behandler Eurojust væsentlige mængder oplysninger, ofte persondata, der relaterer sig til mistænkte, dømte personer, vidner og ofre for forbrydelser.

Datatilsynet er repræsenteret i den Fælles Kontrolinstans (JSB), som er en uafhængig kontrolinstans oprettet i medfør af paragraf 23 i Eurojust-afgørelsen[5], og som kollektivt overvåger Eurojust's aktiviteter, der involverer behandling af persondata, og sikrer, at disse udføres i henhold til Eurojust-afgørelsen. JSB's medlemmer er dommere eller personer, der har tilsvarende uafhængighed (i praksis databeskyttelseskommissærer), og som derfor har væsentlig ekspertise inden for både databeskyttelse og retligt samarbejde.

Der har i 2011 været afholdt ét møde i den fælles kontrolinstans.

Europarådet

Datatilsynet deltager i Europarådets arbejde om databeskyttelse, der har tilknytning til Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.

I 2011 deltog Datatilsynet i et møde, hvor ændring af den ovennævnte konvention samt en rekommandation om behandling af personoplysninger i politisektoren blev diskuteret.

Berlin-gruppen

En international arbejdsgruppe – International Working Group on Data Protection in Telecommunication – blev etableret i 1983 på initiativ af datatilsynsmyndighederne fra en række lande, herunder Danmark.

Sekretariatsfunktionen har siden gruppens etablering været varetaget af Berlins Datatilsyn (Berliner Datenschutzbeauftragter).

Arbejdsgruppen – som kalder sig Berlin-gruppen i daglig tale – beskæftiger sig med registerretlige og databeskyttelsesmæssige anliggender inden for telekommunikation i bred forstand, i de senere år i vid udstrækning vedrørende internettet.

I regi af Berlin-gruppen har Datatilsynet i 2011 i samarbejde med de canadiske, slovenske og berlinske databeskyttelsesmyndigheder arbejdet på et såkaldt working document om

5 Rådets afgørelse af 28. februar 2002 om oprettelse af Eurojust for at styrke bekæmpelsen af grov kriminalitet som ændret ved Rådets afgørelse af 16. december 2008

cloud computing. Dokumentet er offentliggjort i april 2012 som "The Sopot Memorandum".

Berlin-gruppen afrapporterer til den lukkede del af Den Internationale Konference for databeskyttelsesmyndigheder.

Nordisk samarbejde

Datatilsynet var i 2011 vært for det årlige fællesnordiske sagsbehandlermøde for sagsbehandlere – fortrinsvis jurister – fra de nordiske datatilsynsmyndigheder (Norge, Sverige, Finland, Åland, Island, Færøerne og Danmark).

Mødet havde forskellige emner på dagsordenen, bl.a. lovgivningen om og tilsynet med databeskyttelse på sundhedsområdet, betingelserne for at behandle personoplysninger i forskningsøjemed, databeskyttelse i relation til sociale medier og straf for overtrædelse af persondatalovgivningen.

I 2011 deltog Datatilsynet også i det fællesnordiske teknikermøde, som foregik i Norge. Deltagerne var it-sikkerhedskonsulenter og teknikere mv. fra datatilsynsmyndighederne i de nordiske lande. Deltagerne udvekslede erfaringer om konkrete sager, bl.a. om cloud computing, brug af personlig NemID i kommuner, diverse former for overvågning, Schengen-evaluering, apps til mobiltelefoner, biometri, geolokalisering samt dataoverførsler.

Erfaringerne fra de årlige fællesnordiske møder viser, at sagerne i de nordiske lande har mange lighedstræk, og at der ofte kun er kortere tidsforskydninger mellem, hvornår en problemstilling i ét land kan genfindes i de øvrige lande. Derved kan der drages fælles fordel af de baggrundsundersøgelser, som de enkelte datatilsyn foretager – især i de tungere sager om f.eks. cloud computing.

Desuden har Datatilsynet i 2011 deltaget i det nordiske datachefmøde. Mødet blev afholdt i Finland. På mødet blev det bl.a. drøftet, hvilke mål og visioner de nordiske datatilsynsmyndigheder hver især har, og hvordan disse bliver til virkelighed.

Desuden blev fremtidigt samarbejde mellem de nordiske datatilsynsmyndigheder drøftet. Dette mundede konkret ud i, at de nordiske datatilsynsmyndigheder i 2011 har haft et samarbejde om at få oplysninger om Facebooks anvendelse af personoplysninger.

Myndighedernes undersøgelse har karakter af "fact finding", da Facebook er etableret i Irland og dermed som udgangspunkt underlagt den irske databeskyttelseslovgivning.

De nordiske datatilsynsmyndigheders fælles spørgsmål til Facebook er sammenfattet af det norske datatilsyn, som sendte en samlet høring til Facebook. Facebooks svar er offentliggjort på det norske datatilsyns hjemmeside www.datatilsynet.no.




It-sikkerhed

Generelt om it-sikkerhed

Datatilsynet får en del henvendelser fra myndigheder, der ønsker at benytte sig af mulighederne i ny teknologi. Henvendelserne viser, at det kan være svært at vide, hvordan systemet bag løsningen reelt set fungerer, og om det indebærer risici i forhold til behandling af personoplysninger.

I sundhedssektoren og i kommunernes ældrepleje er man i stor stil begyndt at bruge ny teknologi, dels internt mellem parter i sundhedssektoren, dels i løsninger rettet mod borgere – typisk i forbindelse med ældrepleje eller telemedicin. Tilsynet har i den forbindelse modtaget forespørgsler om brug af løsninger, hvor der ikke synes at have været tilstrækkelig fokus på beskyttelse af følsomme personoplysninger.

Et eksempel fra 2011 på et system, som sikkerhedsmæssigt på flere punkter ikke syntes at leve op til de persondataretlige sikkerhedskrav, er Sundhedsstyrelsens online modul til bestilling af dataudtræk fra Landspatientregistret. Datatilsynet fandt, at Sundhedsstyrelsen ikke havde godtgjort, at modulet levede op til persondatalovens og sikkerhedsbekendtgørelsens krav.

Tablet-pc, smartphone, apps og log-in

Tilsynet har modtaget mange henvendelser om alternative metoder til at give adgang til personoplysninger. Disse er kommet fra myndigheder og virksomheder, bl.a. en kommune, e-Boks, Digitaliseringsstyrelsen og private firmaer, som laver løsninger for myndigheder. Mange ønsker at bruge en smartphone og "apps" til at give borgere eller medarbejdere adgang til personoplysninger.

Datatilsynet finder, at der er et aktuelt behov for et sikkerhedsmæssigt forsvarligt log-in til selvbetjeningsløsninger via smartphones og lignende. Tilsynet har derfor i 2011 rejst problemstillingen over for Digitaliseringsstyrelsen og spurgt, om der arbejdes på en fællesoffentlig løsning til log-in til selvbetjeningsløsninger via smartphones og lignende.

Cloud computing

Cloud computing udgør en forholdsvis ny måde at anvende it-ressourcer på. Behandling af personoplysninger i forbindelse med cloud computing giver anledning til en række databeskyttelsesretlige udfordringer.

Hvad er cloud computing?

It-sikkerhedskomiteen derfinerer cloud computing som en model for internetbaseret adgang til en delt pulje af konfigurerbare it-ressourcer (net, servere, datalagre, programmer og services), der hurtigt kan etableres og afvikles med en minimal indsats eller interaktion med tjenesteleverandøren[6]. Et eksempel på en cloud-løsning er software udbudt som en service, der ikke skal installeres eller vedligeholdes på kundens egne systemer, men i stedet ligger hos leverandøren og tilgås via brugerens internetbrowser. Som eksempel herpå kan nævnes e-mailtjenester som gmail og hotmail, som er tjenester, der tilgås af brugeren via en internetbrowser, og hvor data ikke gemmes på brugerens egen computer, men i et datacenter hos cloud-leverandøren (i "skyen").

Datatilsynet var i 2011 en af de første tilsynsmyndigheder i EU, som behandlede og tog stilling til en sag vedrørende behandling af personoplysninger i en cloud-løsning. Sagen vedrørte Odense Kommunes brug af cloud-løsningen Google Apps og er omtalt nedenfor. Datatilsynets udtalelse i denne sag har ifølge tilsynets oplysninger dannet præcedens for en række sager om cloud computing hos andre tilsynsmyndigheder i EU.

Datatilsynets behandling af sagen vedrørende Odense Kommunes brug af Google Apps gav anledning til en række forespørgsler, herunder anmodninger om møder og bistand til udarbejdelse af vejledninger mv., fra både offentlige myndigheder og private virksomheder, der ønskede at blive klogere på persondatalovens krav til behandling af personoplysninger i en cloud-løsning.

Arbejdsgruppe

VK-regeringen nedsatte i 2011 en arbejdsgruppe, som fik til opgave at stille forslag til eventuelle tilpasninger af persondataloven og øvrige relevante love og regler, der unødigt vanskeliggør anvendelsen af cloud-teknologier. Arbejdsgruppens notat er offentliggjort på Justitsministeriets og Digitaliseringsstyrelsens hjemmesider.

6 Se publikationen "Sikkerhed i cloud computing" fra december 2010




Odense Kommunes brug af Google Apps

Odense Kommune havde sendt en anmeldelse til Datatilsynet, hvoraf det bl.a. fremgik, at kommunen ønskede at behandle følsomme personoplysninger om elever og forældre i cloud-løsningen Google Apps.

Odense Kommune ønskede, at lærerne skulle anvende løsningen, når der blev registreret oplysninger om planlægning af undervisningen og evaluering af undervisningsforløb samt de enkelte elevers faglige udvikling. Herudover skulle lærerne foretage notater om klasser og elevers samarbejde og udarbejde skrivelser til forældrene vedrørende deres børn. Løsningen ønskedes endvidere anvendt, når der blev planlagt og inviteret til møder og informeret om undervisningsrelaterede aktiviteter. Ifølge Odense Kommune indgik der bl.a. følsomme oplysninger om helbredsforhold, væsentlige sociale problemer og andre rent private forhold i den anmeldte behandling.

Som sagen forelå, var det Datatilsynets opfattelse, at der på en række punkter var problemer i forhold til kravene i persondataloven og sikkerhedsbekendtgørelsen. De identificerede problemer vedrørte overførsel af oplysninger til tredjelande, utilstrækkelig risikovurdering, krav til brug af databehandler samt en række specifikke problemer vedrørende behandlingssikkerhed (f.eks. sletning, transmission af oplysninger, login, kontrol med afviste adgangsforsøg og logning).

Det førte til, at Datatilsynet ikke var enig i Odense Kommunes vurdering af, at fortrolige og følsomme oplysninger om elever og forældre kunne behandles i Google Apps. Datatilsynet udtalte dog, at tilsynet gerne modtog sagen til fornyet udtalelse, hvis Odense Kommune arbejdede videre med sagen og søgte efter løsninger på de påpegede problemstillinger.

Læs mere

Datatilsynets udtalelse til Odense Kommune af 3. februar 2011 er tilgængelig på Datatilsynets hjemmeside under punktet Afgørelser.

En engelsk version af udtalelsen er endvidere tilgængelig på hjemmesiden under punktet In English.

Læs også Datatilsynets brev af 11. juli 2011 til en alternativ behandler vedrørende brug af cloud-løsningen Dropbox under punktet Afgørelser.

Datatilsynet på Digitaliseringsmessen

I 2011 var Datatilsynet for første gang repræsenteret på den årlige Digitaliseringsmesse. Messen fandt sted i Odense Congress Center den 29. september.

Om Digitaliseringsmessen

Digitaliseringsmessen arrangeres af KL, Borgerservice Danmark og KIT@ (foreningen af kommunale IT-ansvarlige). Messen sætter fokus på digitale løsninger og effektiviseringsmuligheder i kommuner og er platform for vidensdeling mellem leverandører, udviklere og chefer, ledere og medarbejder i kommunerne.

Op mod 1.400 personer deltog i messen, der fandt sted for 3. år i træk. Messen bød på omkring 80 stande, hvor forskellige udstillere – både offentlige og private – var repræsenteret.

Datatilsynet havde en stand på messen, hvor der var mulighed for, at messedeltagerne kunne teste deres viden om beskyttelse af personoplysninger i kommunerne. Datatilsynet havde således til lejligheden udarbejdet en test, som deltagerne kunne tage online ved tilsynets stand.

Mange lagde vejen forbi Datatilsynets stand med spørgsmål til tilsynets medarbejdere om bl.a. brug af digitale løsninger i kommunerne.

For Datatilsynet blev Digitaliseringsmessen en udbytterig dag med mange gode samtaler, som bekræftede tilsynets formodning om, at kommunerne er opmærksomme på persondatalovens regler, men at det i praksis er en stor udfordring at leve op til persondatalovens krav til sikkerhed ved behandling af personoplysninger.

Datatilsynets test var en multiple choice test med 10 spørgsmål, herunder dette:

Må du som ansat i kommunen tjekke din datters nye kæreste i kommunens systemer?

1. Nej
2. Ja, men kun med samtykke fra min datter
3. Ja, jeg bruger min kollegas login, så det ikke kan ses, at det er mig selv, der har søgt på ham

Hele testen og de rigtige svar er tilgængelig på Datatilsynets hjemmeside under punktet Offentlig ⇢ Test din viden.

(Det rigtige svar er 1)

Datatilsynets inspektioner

Inspektioner i 2011

Datatilsynet var i 2011 på 54 inspektioner. Disse inspektioner var fordelt på offentlige myndigheder, private virksomheder og private forskere.

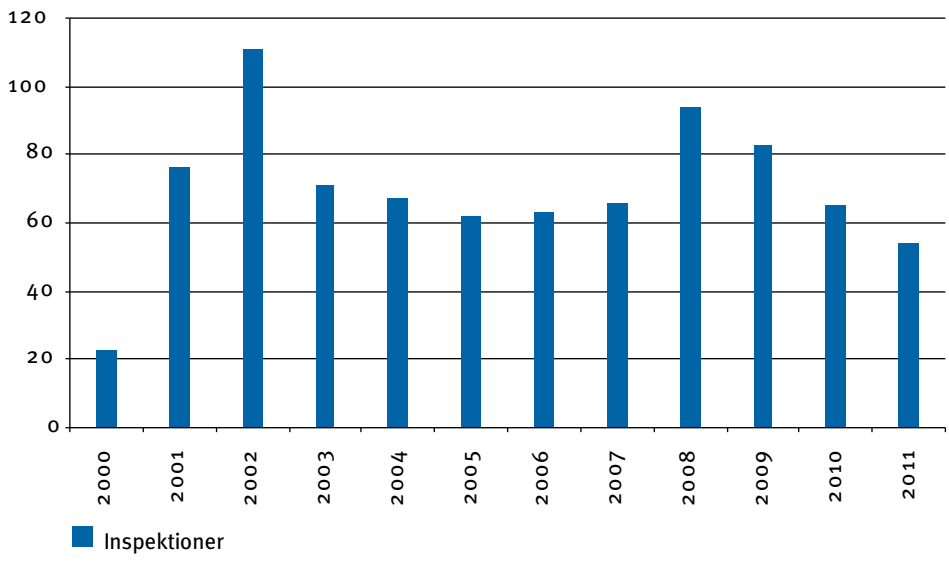
En inspektion indebærer, at typisk 2-3 af Datatilsynets medarbejdere møder op hos den dataansvarlige og får beskrevet den dataansvarliges behandling af personoplysninger.

Af ressourcemæssige årsager har Datatilsynet de seneste to år desværre ikke gennemført så mange inspektioner som tidligere. Tilsynet finder denne udvikling utilfredsstillende, da omfanget af elektronisk databehandling af personoplysninger er stigende i alle dele af samfundet.

Datatilsynets inspektionskompetence

Som led i sin tilsynsvirksomhed har Datatilsynet efter persondatalovens § 62 inspektionsadgang uden retskendelse og kan kræve de nødvendige oplysninger.

Datatilsynets inspektionsadgang i forhold til private virksomheder er ikke ubegrænset. Inspektionsadgangen gælder således kun virksomheder mv., der skal have tilladelse fra Datatilsynet til at behandle personoplysninger, eller hvis der er tale om behandling af personoplysninger i forbindelse med tv-overvågning.



Forløbet af inspektionerne

Når Datatilsynet er på inspektion hos *private dataansvarlige,* tager tilsynet udgangspunkt i de behandlinger, den dataansvarlige har anmeldt til Datatilsynet og fået tilladelse til. Hvis Datatilsynet har stillet vilkår for sin tilladelse, vil disse vilkår normalt være centrale for inspektionen.

I forbindelse med inspektioner hos *offentlige myndigheder* vælger Datatilsynet ofte at lægge særlig vægt på et begrænset antal emner for at få tid til en mere grundig gennemgang og drøftelse af de enkelte emner. Det kan f.eks. være emner som logning og brugernes adgang til myndighedens it-systemer.

Før Datatilsynet tager fra en inspektion, besigtiger tilsynet ofte lokaler, hvor personoplysninger behandles. Tit foretager tilsynet også stikprøver i den dataansvarliges systemer. Tilsynet stiller desuden gerne spørgsmål til de medarbejdere, der konkret behandler personoplysninger eller administrerer it-udstyr.

Formålet med at foretage stikprøver og stille spørgsmål er at undersøge, hvordan de regler og procedurer, som tilsynet har fået præsenteret mundtligt eller skriftligt, efterleves i praksis.

Når Datatilsynet under inspektionen ikke observerer forhold, der skal undersøges nærmere, eller alvorligere overtrædelser af persondataloven, afsluttes inspektionen normalt på stedet.

Hvis Datatilsynet i forbindelse med en inspektion konstaterer, at en myndighed har overtrådt persondataloven, og der er tale om en overtrædelse af en vis alvor, udtaler tilsynet kritik over for myndigheden. Er der tale om en kommune eller en region, kan der blive tale om en orientering af kommunalbestyrelsen eller vedkommende regionsråd. For så vidt angår statslige myndigheder kan det komme på tale at orientere en overordnet myndighed eller den relevante minister.

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.

Særlige fokusområder

I 2011 havde Datatilsynet fokus på virksomheder, der har indført whistleblower-ordninger. Datatilsynet gennemførte således 4 inspektioner på området for at kontrollere, at virksomhederne lever op til den givne tilladelse. Det er første gang, at Datatilsynet har foretaget inspektion af whistleblower-ordninger. Det generelle indtryk fra inspektionerne var positivt. Inspektionerne gav dog anledning til enkelte bemærkninger. F.eks. medførte alle fire inspektioner, at der skulle foretages ændringer i de enkelte virksomheders anmeldelser til Datatilsynet, eksempelvis ændring af den personkreds der indberettede til whistleblowersystemet. Herudover gav kravet om interne sikkerhedsbestemmelser og reglerne om tredjelandsoverførsler Datatilsynet anledning til bemærkninger ved nogle af inspektionerne.

Tilsynet havde i 2011 endvidere fokus på analyseinstitutters behandling af personoplysninger og foretog 6 inspektioner hos en række større analyseinstitutter. Datatilsynet vil i 2012 offentliggøre en informationstekst, som afspejler tilsynets erfaringer fra inspektionerne.

Datatilsynet fortsatte i 2011 arbejdet med at gennemføre inspektioner hos politikredsene og Rigspolitiet. Tilsynet har således særlig fokus på myndigheder, som behandler mange følsomme og fortrolige personoplysninger.

Desuden foretog tilsynet i 2011 en særlig form for inspektion, da vi kontrollerede Brøndby IF's håndtering af karantænelister (hooliganregister) bl.a. i forbindelse med afviklingen af en fodboldkamp. Inspektionen gav ikke Datatilsynet anledning til bemærkninger.

Om hooliganregistre

Efter lov om sikkerhed ved bestemte idrætsbegivenheder kan politiet videregive oplysninger om meddelte karantæner til autoriserede kontrollører. Idrætsklubber, der beskæftiger kontrollørerne er dataansvarlige efter persondataloven, og klubberne skal have en tilladelse til behandlingen af personoplysninger fra Datatilsynet. Lov om sikkerhed ved bestemte idrætsbegivenheder finder indtil videre alene anvendelse i forbindelse med fodboldkampe.

Endelig har Datatilsynet i 2011 for første gang foretaget inspektioner af offentlige myndigheders tv-overvågning. Læs mere om disse inspektioner under afsnittet om tv-overvågning.

Oversigt over udførte inspektioner i 2011

Staten:
Rigspolitiet (Schengen)
Statsfængslet Østjylland
Sydøstjyllands Politi
SKAT (Det Centrale Motorkøretøjsregister)
Forsknings- og Innovationsstyrelsen
Statsforvaltningen Hovedstaden (Beskæftigelsesankenævnet)
Patientombuddet (Dansk Patient Sikkerhedsdatabase)
Midt- og Vestsjællands Politi
Midt- og Vestsjællands Politi (Holbæk lokalstation)

Kommuner:
Sorø Kommune
Høje-Taastrup Kommune (opfølgning)
Københavns Kommune (jobcentret)
Helsingør Kommune
Billund Kommune

Regioner:
Region Hovedstaden (kliniske kvalitetsdatabaser)
Region Midtjylland (EPJ-systemet)

Temainspektioner tv-overvågning – Greve:
Danske Bank (Greve Midtby Center)
Greve Postkontor (Greve Midtby Center)
Guldsmeden (Greve Midtby Center)
Spillehal/videoeksperten (Greve Midtby Center)
Greve Midtby Center (centeradministrationen)
Greve Kommune

Øvrige tv-overvågning:
Butik Rud & Vester
Butik CLICK
Butik CPH Investment Group
Albertslund Kommune
Dragør Kommune
Rødovre Kommune
Vallensbæk Kommune

It-sikkerhed:
Sundhedsstyrelsen (Sundhedsdatanettet)
Privathospitalet Mølholm
Sundhedsstyrelsen (opfølgning)
Region Hovedstaden (datakommunikation med Sundhedsstyrelsen)

Privat forskning og statistik:
Katrine Strandberg-Larsen
Ulveman Explorative A/S
Analyse Danmark A/S
MEGAFON
The Nielsen Company
Gallup
Epinion
Therese Helberg

Alternative behandlere:
Karin Juhlsen
Lise Breusch Klinkby
Urban Health A/S
Daying Klinikken
Susanne Dreyer Olsson

Whistleblower:
Ferring Pharmaceuticals A/S
Novozymes A/S
Lego A/S
TDC A/S

Øvrige private:
Experian A/S (RKI)
Arbejdernes Landsbank (spærreliste)
Brøndby IF (hooliganregister)
Debitor Registret A/S

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