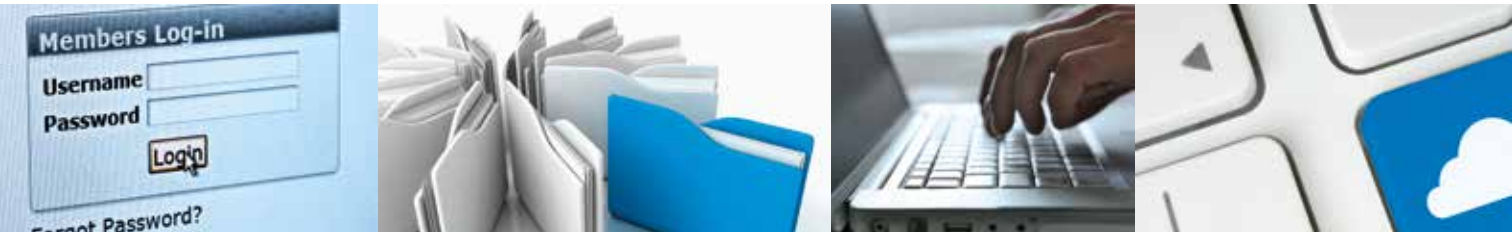
DATATILSYNET

Datatilsynets årsberetning 2012

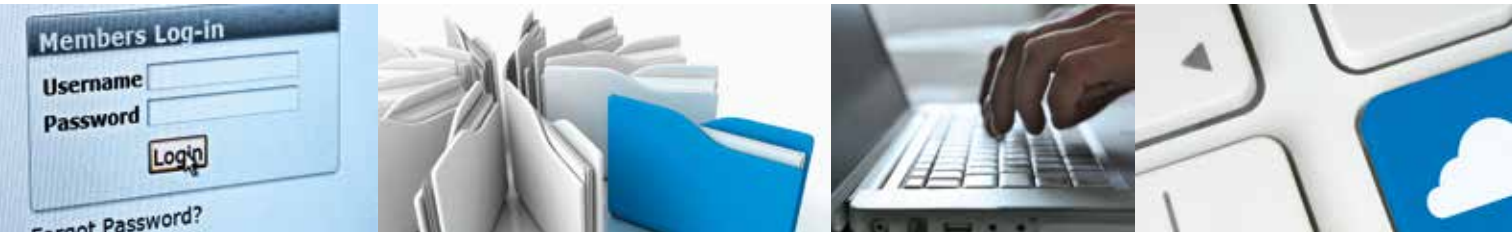
Udgiver: Datatilsynet
Tryk og layout: Rosendahls - Schultz Grafisk
Beretningen er sat med Meta
Oplag: 300
September 2013
ISSN nr: 1601-5657
ISBN nr: 978-87-992871-4-7

Datatilsynets årsberetning 2012



Indhold



Til Folketinget

2012 har i høj grad stået i fremtidens tegn for Datatilsynet.

EU-Kommissionen offentliggjorde i 2012 sit udspil til nye regler om beskyttelse af personoplysninger i EU. Reformpakken indeholder et forslag til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og den fri udveksling af sådanne oplysninger. Forordningen vil skulle afløse det generelle databeskyttelsesdirektiv, som persondataloven implementerer.

I lyset af den teknologiske udvikling og globaliseringen er der efter Datatilsynets opfattelse god grund til at overveje reguleringen af databeskyttelsesområdet, således at borgerne sikres et højt beskyttelsesniveau samtidig med, at fordelene ved nye digitale løsninger og services kan høstes.

På positivsiden er det helt klart, at borgernes retsstilling i det nye forordningsudkast styrkes med mere åbenhed og større indflydelse.

For virksomheder og organisationer er der større krav om at tage ansvar for databeskyttelse. Der strammes op med nye forpligtelser for at øge fokus på databeskyttelse. Samtidig med, at der sker en smidiggørelse og harmonisering af visse regler.

Som datatilsyn får vi styrkede beføjelser — det hilser vi velkommen.

Alligevel er Datatilsynet umiddelbart skeptisk over for valget af en forordning i stedet for et direktiv.

Forordning kan være et godt valg på områder med grænseoverskridende ydelser, men måske ikke som et generelt instrument på alle områder. Der er meget store forskelle landene imellem — historisk og kulturelt betinget. Så her er der brug for en nærmere analyse af, hvad det betyder for danskerne — f.eks. når vi tænker i forhold til den offentlige sektors måde at gøre tingene på.

Med en forordning falder den danske persondatalov helt bort, dvs. også de ganske fornuftige særregler, som vi har haft i Danmark i mange år, f.eks. om kreditoplysningsbureauer og om behandling af persondata til forskning og statistik. Disse regler har ikke givet anledning til problemer. Samtidig indføres der særlige beslutningsprocedurer i sager, som berører borgere i flere EU-lande, og EU-kommissionen får større kompetence.

Der vil gå flere år, før en ny regulering af databeskyttelsesområdet kan træde i kraft. Datatilsynet har derfor i 2012 først og fremmest koncentreret sig om de aktuelle opgaver for tilsynet. Det er en løbende udfordring for Datatilsynet at behandle de mange sager, som tilsynet modtager.

I 2012 har Datatilsynet som en del af en effektiviseringsproces fået indført nye regler, som begrænser antallet af sager om tilladelser fra Datatilsynet, f.eks. på lægemiddel- og forskningsområdet. Der er i 2012 desuden blevet gennemført en ændring af persondataloven, som medfører, at tilsynet ikke længere skal give tilladelse til selve overførslen af personoplysninger til usikre tredjelande, når en overførsel sker på grundlag af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser, som er godkendt af EU-Kommissionen. Ændringen trådte i kraft den 1. januar 2013.

København, september 2013

Henrik Waaben
Formand for Datarådet

Janni Christoffersen
Direktør

Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2012 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 2012, 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 2012

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. 1245 af 18. december 2012.

I tilknytning til persondataloven har Justitsministeriet udstedt en række bekendtgørelser. Datatilsynet har desuden lavet en række vejledninger vedrørende loven.

Tilsynet med persondataloven indebærer et stort antal forskelligartede opgaver. Datatilsynet har i 2012 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.

Rådgivning og vejledning

Det er forudsat i de almindelige bemærkninger til persondataloven, at Datatilsynet i første række bør tage sigte på at kunne udøve sin virksomhed gennem generelle retningslinjer og ved en serviceorienteret rådgivning og vejledning.

Dette sikres bl.a. gennem tilsynets hjemmeside, hvor tilsynet offentliggør relevant praksis. Datatilsynet har endvidere udarbejdet informationspjecer og forskellige vejledninger om persondataloven.

På hjemmesiden offentliggør tilsynet også de generelle retningslinjer, som tilsynet fastsætter. I 2012 har Datatilsynet bl.a. fastsat krav til sundhedsvidenskabelige forskningsprojekter og kliniske forsøg med lægemidler. Dette område blev i 2012 undtaget fra kravet om anmeldelse til og tilladelse fra Datatilsynet (se nærmere om undtagelserne nedenfor i afsnittet Nye fritagelser fra anmeldelses- og tilladelseskravet i den private sektor).

Datatilsynet arrangerede sammen med Danske Advokater, Dansk Industri og Københavns Universitet en persondatakonference den 14. november 2012 på Nationalmuseet. Konferencens fokus var EU-Kommissionens forslag til ny forordning på databeskyttelsesområdet. Datatilsynet bidrog med flere oplæg på konferencen, der havde 300 deltagere. I 2012 har Datatilsynet endvidere deltaget med 20 indlæg på møder, konferencer mv. Som eksempler kan nævnes, at Datatilsynet har holdt oplæg for Dansk Industri om whistleblowersager og for foreningen Ansættelsesadvokater om persondataloven og HR-området. Tilsynet prioriterer sådanne opgaver for at informere om persondataloven og tilsynets praksis, men også for at tilsynet kan opnå større viden om, hvilke konkrete problemstillinger der er aktuelle på de forskellige områder af samfundslivet.

Datatilsynet markerede også den årlige databeskyttelsesdag[1] den 28. januar 2012 ved at holde oplæg på tre konferencer: "Databeskyttelsesdagen 2012", Ældresagens konference "Danmark går online – er der plads til alle?" og Dansk IT's konference "IT-sikkerhed 2012".

Datatilsynet modtager fortsat et meget stort antal telefoniske henvendelser. Det er en vigtig del af tilsynets arbejde at yde telefonrådgivning, som kan give hurtig hjælp og sparring til borgere, dataansvarlige mv. med persondataretlige problemstillinger.

1 Den 28. januar er fastsat til at være Europæisk Databeskyttelsesdag. Databeskyttelsesdagen er et initiativ fra Europa-rådet, og dagen støttes af EU-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.

På baggrund af tilsynets kvartalsvise stikprøvetællinger anslås antallet af telefoniske henvendelser til tilsynet i 2012 at ligge på ca. 17.000 opkald og dermed på lidt lavere niveau end i 2011 (ca. 18.000 opkald).

Datatilsynet giver desuden vejledning på baggrund af skriftlige forespørgsler om persondataloven. Nedenfor ses et eksempel på en sådan sag. Sagen blev behandlet på et møde i Datarådet.

Transmission af gudstjenester

Ribe Stift rettede i 2012 henvendelse med spørgsmål om, hvorvidt Datatilsynet i forhold til persondataloven så noget til hinder for direkte transmission og visning på skærme af gudstjenester og forskellige former for kirkelige handlinger.

Formålet med transmissionen er at give personer, der er forhindret i at være fysisk til stede i kirken, mulighed for at følge kirkelige handlinger. Det vil ved indgangen til den pågældende kirke tydeligt blive angivet ved skiltning, at der foretages transmission fra kirken.

Datatilsynet lagde i sin udtalelse af 17. januar 2013 til grund, at det er menighedsrådene, der i forhold til persondataloven er ansvarlige for den behandling af personoplysninger, der finder sted i forbindelse med transmission af gudstjenester og visning på skærme i kirken. Efter persondataloven[2] er det derfor i første række op til menighedsrådet konkret at foretage en afvejning af den interesse, der forfølges med den påtænkte behandling, i forhold til de hensyn, som på den anden side skal tages til de personer, der berøres.

I denne vurdering kan menighedsrådet efter Datatilsynets opfattelse inddrage forskellige hensyn. Det kan tillægges vægt, at der er offentlig adgang for alle til kirken, og at der kun påtænkes transmission til en begrænset modtagerkreds ud over de tilstedeværende. For så vidt angår visning på skærme i kirken er der alene tale om en anden form for formidling af den information, som kirkegængere allerede har adgang til ved at være til stede under gudstjenesten.

Datatilsynets umiddelbare vurdering var, at persondataloven ikke er til hinder for, at menighedsrådet beslutter at foretage transmission af live-billeder af kirkegængere, der deltager i gudstjeneste, herunder i nadverhandlinger, til andre konkrete lokaliteter, herunder plejehjem, ligesom live-billeder vil kunne vises på skærme i kirken.

2 § 6, stk. 1, nr. 7, og § 5

Det var imidlertid Datatilsynets opfattelse, at det vil være velbegrundet at sikre kirkegængere en mulighed for at vælge, om de ønsker at deltage i en sådan transmission[3]. Eventuelt ved, at områder af kirken ikke omfattes af transmissionen af live-billeder, eller ved, at der gennemføres gudstjenester uden transmission. Under alle omstændigheder bør der meget klart informeres om, hvornår og hvordan der sker transmission, således at man har mulighed for at fravælge at deltage i gudstjenester, herunder nadverhandlinger, hvor der foretages transmission af live-billeder.

Ved dåbshandlinger må der som minimum gives klar og tydelig information til faddere og dåbsvidner forud for transmissionen. I forhold til den døbte (for små børn ved forældremyndighedsindehaver) fandt Datatilsynet, at det må anses for nødvendigt at indhente udtrykkelig accept til transmission af live-billeder af selve dåbshandlingen til andre lokaliteter[4].

For så vidt angår ansatte i kirken var det Datatilsynets opfattelse, at disse bør høres, inden det besluttes at foretage live-transmission til andre lokaliteter[5].

Klagesagsbehandling

I klagesagerne træffer Datatilsynet afgørelse om, hvorvidt en behandling af personoplysninger er sket 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 2012 har tilsynet registreret en stigning på 8 % i antallet af nye sager (forespørgsler og klager) vedrørende private virksomheder mv. (fra 1.235 i 2011 til 1.332 i 2012). I forhold til offentlige myndigheder har antallet af sager i 2011 og 2012 været det samme (730).

Nedenfor ses et eksempel på en klagesag, som Datatilsynet behandlede i 2012. Sagen blev behandlet på et møde i Datarådet.

3 Jf. persondatalovens § 5 og § 6, stk. 1, nr. 7
4 Jf. persondatalovens § 7, stk. 2, nr. 1
5 Datatilsynet har ikke kompetence til at vurdere eventuelle ansættelsesretlige spørgsmål i denne sammenhæng

Offentliggørelse af personoplysninger på hjemmeside

En kommune klagede på vegne af tre ansatte, kommunens borgmester og en plejefamilie tilknyttet kommunen til Datatilsynet over registrering på en hjemmeside.

Det fremgik af hjemmesiden, at hjemmesiden havde til formål at lave en registrering af bl.a. advokater, kommunale ansatte, plejefamilier, politi og politikere, der efter borgernes mening har overtrådt loven, samt hvis en borger føler sig uretfærdigt behandlet.

Om en af personerne havde der tidligere også været anført oplysninger om (arbejds) email-adresse, fødselsdato, og at vedkommende havde fået konstateret en angivet sygdom. Desuden fremgik oplysninger om navn, adresse, telefonnummer, CVR-nummer og opstartsdato for et selskab, som personen ifølge det angivne var involveret i. Der var desuden angivet link til CVR vedrørende selskabet og link til en artikel omkring et lån i selskabet – et lån som på hjemmesiden var angivet som værende ulovligt. Datatilsynet konstaterede, at disse oplysninger nu var slettet fra hjemmesiden.

Om plejefamilien fremgik på hjemmesiden oplysninger om navn, adresse, telefonnummer, og at der var tale om en plejefamilie.

Ved hver enkelt af de pågældende personer var der derudover anført "overskrifter"/ "etiketter" i form af "Pligtforsømmelse", "Magtmisbrug", Pligtforsømmelse, Trusler m.v.", "Trusler, Chikane, tavshedspligten m.v." eller "[...] er blevet registreret på [...] for Pligtforsømmelse. Samt for brud på tavshedspligten som er overtrædelse af Straffelovens § 152 stk. 1. og stk. 2".

Datatilsynet udtalte i sin afgørelse af 12. juni 2012, at persondataloven bl.a. gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling. Det fremgår af lovens § 1, stk. 1. Loven finder dog ikke anvendelse, hvis det vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10. Det fremgår udtrykkeligt af persondatalovens § 2, stk. 2.

Datatilsynet fandt, at hensynet til informations- og ytringsfriheden måtte føre til, at der ikke efter persondataloven var grundlag for, at tilsynet foretog noget i sagen, jf. lovens § 2, stk. 2.

Datatilsynet lagde i den forbindelse vægt på, at hjemmesidens tema var forholdet mellem borgere og beslutningstagere/myndighedspersoner, at hjemmesiden var præget af subjektive vurderinger og værdiladede ytringer, og at de påklagede oplysninger indgik som

en del af meningstilkendegivelserne, hvilket også måtte stå brugere af hjemmesiden klart.

Datatilsynet havde ikke herved taget stilling til, om offentliggørelsen af oplysninger på hjemmesiden stred imod anden lovgivning, herunder straffelovens kapitel 27 om freds- og æreskrænkelser. Tilsynet har ikke kompetence til at foretage vurderingen heraf.

Det blev tilføjet, at tilsynet for så vidt angår den tidligere omtale af en persons specifikke helbredsforhold på hjemmesiden havde lagt til grund, at der måtte antages at være tale om oplysninger, som allerede var offentliggjort af den pågældende person selv.

Høringer over lovforslag mv.

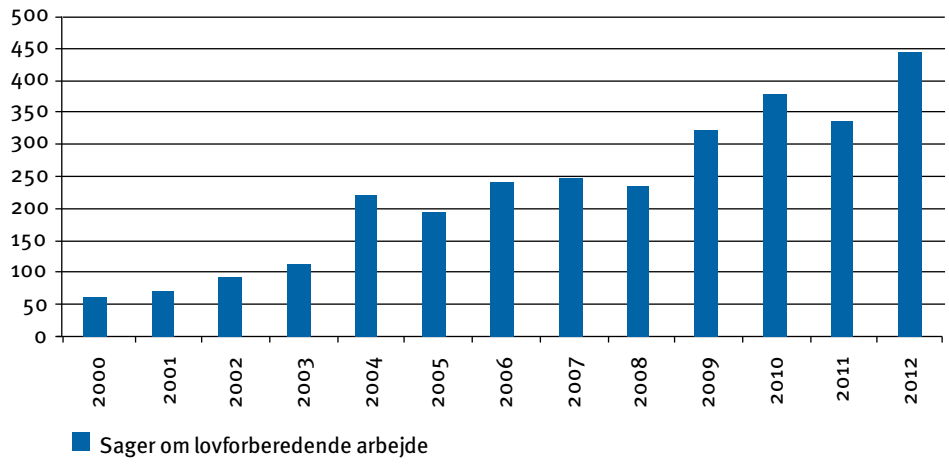
I 2012 registrerede Datatilsynet 444 nye høringssager i forbindelse med lovforslag, bekendtgørelser mv. Dette er en stigning på 31 % i forhold til 2011 (339 i 2011).

Som det fremgår af grafen nedenfor, er der en markant stigende tendens på området. I 2000 registrerede Datatilsynet således kun 59 nye sager om udtalelser til lovforslag mv. Der er således tale om en mangedobling af sagsantallet fra 2000 til 2012.

Datatilsynet oplever, at disse høringssager ofte er særdeles ressourcekrævende. Hertil kommer, at der ofte er fastsat meget korter svarfrister.

I sine udtalelser forholder Datatilsynet sig til de eventuelle databeskyttelsesretlige problemstillinger i det foreliggende lovforslag mv. Datatilsynet anser sine udtalelser som et væsentligt bidrag i lovgivningsprocessen, dels fordi tilsynet besidder en ekspertviden om databeskyttelse, dels fordi tilsynet efter persondataloven udøver sine funktioner i fuld uafhængighed. Tilsynet prioriterer derfor opgaven højt.

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



Nye fritagelser fra anmeldelses- og tilladelseskravet i den private sektor

I den private sektor indebærer persondataloven i en række tilfælde krav om anmeldelse til og tilladelse fra Datatilsynet, når der sker behandling af følsomme personoplysninger.

Håndtering af anmeldelser – navnlig fra den private sektor – har siden persondatalovens ikrafttræden optaget en ganske stor del af tilsynets ressourcer. Der har ikke været tegn på en stagnering i antallet af nye anmeldelser – tværtimod.

I 2012 er der derfor – på Datatilsynets initiativ – gennemført en ændring af undtagelsesbekendtgørelsen[6], således at flere områder i den private sektor er blevet fritaget fra anmeldelsespligten/tilladelseskravet. Ændringerne gælder fra den 15. maj 2012.

Undtagelserne gælder nu for:

- behandling af oplysninger om ansattes fagforeningsmæssige tilhørsforhold i forbindelse med aftaler om kontingentindeholdelse
- virksomheder omfattet af lov om finansiel virksomhed
- kliniske forsøg med lægemidler omfattet af lov om lægemidler
- kliniske afprøvninger af medicinsk udstyr omfattet af lov om medicinsk udstyr
- sundhedsvidenskabelige forskningsprojekter omfattet af lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter
- pligtmæssig sikkerhedsovervågning af lægemidler og medicinsk udstyr efter lov om lægemidler eller lov om medicinsk udstyr
- kontaktbureauer og hjemmesider om dating
- studerendes projekt- og specialeopgaver mv.
- virksomheders behandling af oplysninger fra et centralt privat register med oplysninger om restaurationsforbud

På Datatilsynets hjemmeside er det præciseret, i hvilke tilfælde og under hvilke betingelser undtagelserne finder anvendelse.

Selv om der ikke gælder en anmeldelsespligt til Datatilsynet, skal persondatalovens regler om, hvornår personoplysninger kan indsamles, registreres mv., fortsat overholdes. Det samme gælder regler i relevant lovgivning på de berørte sagsområder.

6 Bekendtgørelse nr. 534 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig (ændret ved bekendtgørelse nr. 202 af 22. marts 2001 og bekendtgørelse nr. 410 af 9. maj 2012)

Bortfald af anmeldelsespligten ændrer heller ikke på de forpligtelser, som persondataloven pålægger virksomheder og andre dataansvarlige i forhold til personer, om hvem der behandles oplysninger. Det gælder bl.a. oplysningspligt, indsigtsret og retten til at gøre indsigelse. Borgernes adgang til at klage til Datatilsynet over behandling af personoplysninger omfattet af persondataloven er også uændret. Datatilsynet har desuden fortsat mulighed for at tage sager op af egen drift. Til gengæld har Datatilsynet ikke længere inspektionskompetence på områderne.

Datatilsynet har i 2012 udformet informationsmateriale til de berørte sektorer og dataansvarlige.

I forlængelse af ændringen pr. 15. maj 2012 har Datatilsynet kunnet konstatere et betydeligt fald i antallet af sager om anmeldelser for den private sektor i forhold til 2011. Således registrerede Datatilsynet i 2011 2.165 nye sager om anmeldelser for den private sektor, mens tallet i 2012 var 1.734, dvs. et fald på 20 %. Faldet skyldes først og fremmest, at der på området forskning og statistik er sket et fald fra 1.376 sager i 2011 til 982 i 2012 – et fald på 29 %.

Ændringerne er endnu ikke slået helt igennem, men tilsynet forventer, at der også fremover vil være et faldende antal anmeldelser fra private dataansvarlige.

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.

Dataradet

Dataradet består af en formand og af seks andre medlemmer, der er udpeget af justitsministeren. Dataradet 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 Dataradet og kan findes på Datatilsynets hjemmeside.

Dataradets medlemmer (pr. 31. december 2012)

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

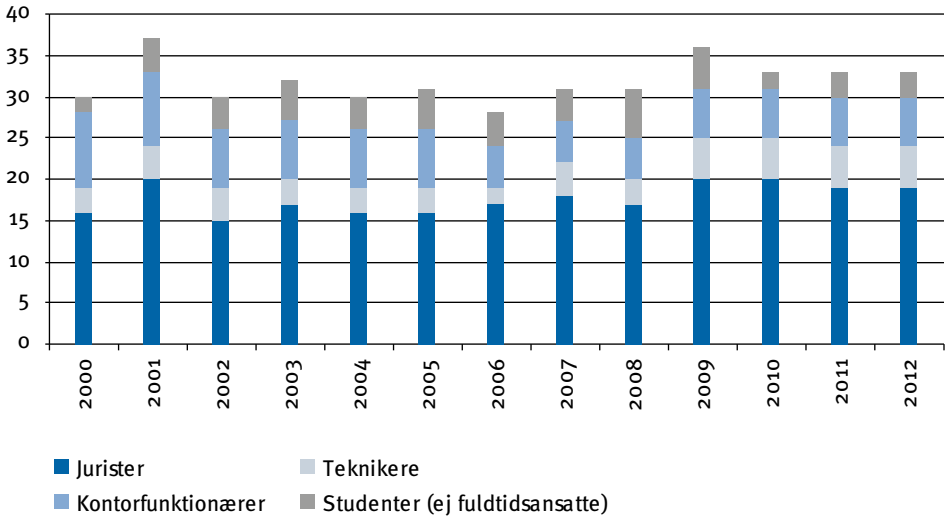
Medlemmerne beskikkes for 4 år ad gangen. De er personligt udpeget i kraft af deres sagkundskab inden for bestemte sagsområder og er ikke repræsentanter for bestemte interesseorganisationer el.lign.

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 2012. Årsrapporten er offentliggjort på tilsynets hjemmeside.

Personalesammensætning





Datatilsynets medarbejdere (pr. 31. december 2012)

Direktør, cand.jur. Janni Christoffersen
Kontorchef, cand.jur. Lena Andersen
Kommitteret, cand.jur. Birgit Kleis
It-chef, civilingeniør, HD, Sten Hansen
Chefkonsulent, cand.jur. Maiken Christensen Breüner
Chefkonsulent, cand.jur. Lene Engedal Kragelund
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
Kontorfuldmægtig Mette Maj Leilund
Assistent Camilla Knutsdotter Hallingby
It-medarbejder Eva Caspersen
It-medarbejder Flemming Nielsen
Fuldmægtig, cand.jur. Maiken Bøgelund Bek
Fuldmægtig, cand.jur. Trine Cseh-Lessel
Fuldmægtig, cand.jur. Kasper Frederiksen
Fuldmægtig, cand.jur. Helle Ginnerup-Nielsen
Fuldmægtig, cand.jur. Christian Vinter Hagstrøm
Fuldmægtig, cand.jur. Mette Hansen
Fuldmægtig, cand.jur. Robert Padilla Bang Jensen
Fuldmægtig, cand.jur. Lasse May Jørgensen
Fuldmægtig, cand.jur. Christine Landsgaard (orlov)
Fuldmægtig, cand.jur. Martin Nybye-Petersen
Fuldmægtig, cand.jur. André Dybdal Pape
Fuldmægtig, cand.jur. Kristian Gyde Poulsen
Fuldmægtig, cand.jur. Maja Blomquist Rasmussen (orlov)
Fuldmægtig, cand.jur. Dana Safin
Fuldmægtig, cand.jur. Anne Mette Riis Steinø (orlov)
Stud.jur. Laura Hvass Jørgensen
Stud.jur. Ole Lyngvåg
Stud.jur. Inneke Wolthoorn

Statistiske oplysninger

Her er oplysninger om antallet af nye sager i Datatilsynets journalsystem i 2012. Tallene omfatter sager, som er oprettet i løbet af 2012. 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.

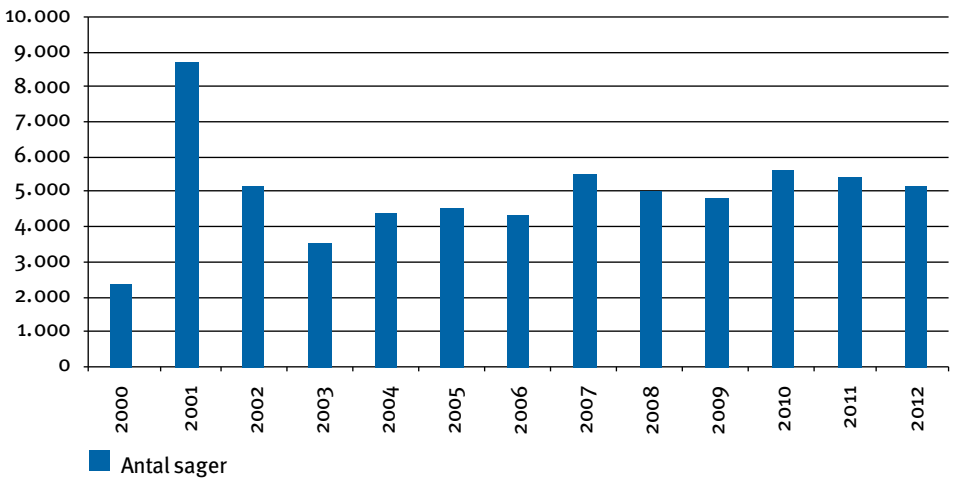
Datatilsynet registrerede 5.166 nye sager i 2012.

Nyoprettede sager 1. januar 2012 til 31. december 2012:

Datatilsynets egen administration mv.	262
Lovforberedende arbejde	444
Forespørgsler og klager vedrørende private	1.332
Forespørgsler og klager vedrørende offentlige myndigheder	730
Anmeldelser for den private sektor	1.734
Anmeldelser for den offentlige sektor	297
Sager på Datatilsynets eget initiativ (egen drift-sager)	118
Sikkerhedsspørgsmål	26
Internationale sager	191
Datatilsynets kompetence efter anden lovgivning	32
I alt	5.166

Der er et mindre fald i antallet af nyoprettede sager i 2012 set i forhold til 2011. I 2011 var tallet 5.442 nyoprettede sager, dvs. der er et fald på 5 %[7]. Faldet i sager skal ses i lyset af, at Datatilsynet pr. 15. maj 2012 har fået indført nye fritagelser fra anmeldelses- og tilladelseskravet i den private sektor (se nærmere herom ovenfor i afsnittet Nye fritagelser fra anmeldelses- og tilladelseskravet i den private sektor). Datatilsynet har således i 2012 modtaget 394 færre sager om anmeldelser på forsknings- og statistikområdet end i 2011 (1.376 sager i 2011, 982 sager i 2012).

7 Faldet i antallet af sager er i Datatilsynets årsrapport for 2012 fejlagtigt anført til 9 %



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

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 1.332 nye sager om forespørgsler og klager vedrørende private dataansvarlige.

Sagerne havde følgende fordeling på forskellige virksomhedstyper:

Almindelige virksomheder	172
Den finansielle sektor	60
Fagforeninger, a-kasser, pensionskasser mv.	8
Telesektoren	81
Foreninger og organisationer	119
Sundhedssektoren (medicinalfirmaer, klinikker, læger mv.)	22
Kreditoplysningsbureauer	121
Advarselsregistre	21
Stillingsbesættende virksomheder	8
Ansøgninger om tilladelser	183
Internet, sociale netværk, cloud mv.	263
Tv-overvågning	47
Private forskere	24
Diverse	203
Sager af generel karakter	0

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2012[8], var:

Klager	9 %
Forespørgsler	75 %
Ikke kategoriserede	16 %

8 I lighed med Datatilsynets Årsberetning 2011 er disse tal for 2012 ikke opgjort på grundlag af sager, som er oprettet i 2012, men på grundlag af sager, som Datatilsynet har færdigbehandlet i 2012. Heriblandt er sager oprettet i 2012 og 2011 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	223
Regioner	40
Primærkommuner	207
Ansøgning om tilladelser	250
Diverse	10

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2012[9], var:

Klager	11 %
Forespørgsler	51 %
Ikke kategoriserede	38 %

9 Se note 1

Anmeldelser

Anmeldelser for den private sektor

Datatilsynet registrerede i alt 1.734 nye sager om anmeldelser for den private sektor. Fordelingen af sagerne var:

Forskning og statistik	982
Privates behandling af oplysninger om rent private forhold	511
Advarselsregistre	1
Spærrelister	37
Kreditoplysningsbureauer	3
Stillingsbesættende virksomheder	27
Edb-servicebureauer	12
Diverse sager af generel karakter	161

Anmeldelser for den offentlige forvaltning

Datatilsynet registrerede i alt 297 nye sager om anmeldelser for den offentlige sektor. Fordelingen af sagerne var:

Fællesanmeldelser	0
Kommuner	52
Regioner	5
Statslige myndigheder	219
Tilslutninger, kommuner	21
Tilslutninger, regioner	0
Tilslutninger, statslige myndigheder	0
Diverse/sager af generel karakter	0

Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 118 nye sager oprettet på tilsynets eget initiativ. Fordelingen af sagerne var:

Inspektion og kontrol vedrørende private	29
Inspektion og kontrol vedrørende offentlige myndigheder	24
Sager rejst på grundlag af presseomtale og lign.	44
Diverse/sager af generel karakter	0
Online-undersøgelser	21

Internationale sager

Datatilsynet registrerede i alt 191 nye internationale sager. Fordelingen af sagerne var:

Forespørgsler fra udlandet	86
Nordisk tilsynssamarbejde	6
Europarådet	6
EU	75
Datakommissærsamarbejdet	10
OECD	1
Diverse /sager af generel karakter	7




10 år med databeskyttelse

– interview med Datatilsynets direktør Janni Christoffersen

Du har i 2012 haft 10-års jubilæum som direktør i Datatilsynet. Bliver det ved med at være spændende og udfordrende?
Ja, for der sker hele tiden rigtig meget på databeskyttelsesområdet. Den teknologiske udvikling med internettet og udviklingen i teknologier – cloud, biometri, intelligent tv-overvågning, mobile devices – har været enorm igennem de sidste 10 år.

Tidligere handlede databeskyttelse meget om "bigbrother" i form af staten overfor borgeren. Men nu er det mere komplekst. Der er sket en udvikling, hvor det nu i lige så høj grad er private virksomheder, som foretager overvågning af borgerne. Det kan f.eks. være i form af tv-overvågning i butikker eller en arbejdsgiver, som overvåger sine medarbejderes internetbrug.

Også det, vi som borgere gør med vores personoplysninger imellem os, er i en rivende udvikling. Vi eksponerer vores egne data på sociale netværk på internettet, så vi er medvirkende til at indskrænke vores egen privatsfære. Samtidig bidrager vi også til at indskrænke andres privatsfære, når vi på de sociale netværk skriver om vores venner, familie og bekendte. Vi offentliggør både oplysninger om os selv og om dem, vi møder, i alle mulige sammenhænge.

Den teknologiske udvikling har også ført til, at databeskyttelse ikke altid kun er et nationalt spørgsmål. Med databeskyttelsesdirektivet fra 1995 blev der taget højde for europæiske anliggender. Men ofte vil der være tale om globale anliggender. Og det gør vejene ganske uigennemskuelige.

Hele denne udvikling gør, at de databeskyttelsesforhold, vi tidligere så, nu er blevet en del af et meget mere komplekst billede. Svarene på de persondataretlige spørgsmål kan derfor også være temmelig svære at nå frem til.

Kan du også blive ved med at lære noget, som ikke vedrører persondataret, f.eks. som personaleleder?
Jeg tror, at alle, som har prøvet at have ledelsesansvar, vil sige, at det er en daglig udfordring. Folk er forskellige – det er man nødt til at forholde sig til. Som leder skal man tage hensyn til kollektivet og samtidig til den enkelte medarbejder. Det er en daglig udfordring og glæde. Og det indebærer mange overvejelser om, hvordan man gør det bedst. Med ti-



den bliver man bedre til at kende og forudse forskellige reaktionsmønstre. Men det bliver aldrig rutine.

Personligt synes jeg, at kombinationen af dels at få løst de faglige opgaver dels at tage sig af, at huset og dets medarbejdere fungerer godt, er meget tilfredsstillende. Det er udfordrende at få det hele til at hænge sammen.

Er der nogen ulemper ved at have siddet så længe som direktør det samme sted?
For mig er det ideelle for en organisation, at der også kommer nye øjne til. Der vil altid være en risiko for, at man efter et stykke tid med de samme opgaver kommer ud i "sådan plejer vi at gøre". Så derfor er det vigtigt at være åben over for forslag fra medarbejdere og input fra omverdenen, så man forsøger ikke at gro fast i gamle rutiner.

Hvad er de vigtigste begivenheder, der har haft betydning på det persondataretlige område i løbet af de sidste 10 år?
Først og fremmest har eftervirkningerne efter terrorangrebene 11. september 2001 haft enorm betydning. Der skete en ændring i holdningen og tilgangen til kontrol. Begivenhederne gjorde, at borgernes frygt for terror kom til at overstige deres frygt for overvågning. Som borger har man accepteret en lang række tiltag, der indskrænker den personlige frihed. Det ser vi f.eks. i form af øget tv-overvågning. Et andet eksempel er logningsreglerne på teleområdet, hvor teleselskaber skal registrere og gemme oplysninger om teletrafik. Det er en meget omfattende overvågning, samfundet dermed har accepteret.

Også på andre områder ser man, at der er sket en udvikling i kontrolforanstaltninger, f.eks. på offentlige forsørgelsesydelser. Hvor der tidligere kun var få muligheder for at foretage kontrolsamkøring, ser vi ofte kontrolelementet i lovforslag, Datatilsynet får i høring. Teknologien giver mulighed for det, og fra lovgivers side mener man, at det er et redskab, der skal tages i anvendelse.

Pendanten til kontrolsamkøring i det offentlige er whistleblower-ordninger i det private. I Datatilsynet modtager vi mange anmodninger om tilladelse til whistleblower-ordninger. Vi har givet over 100 tilladelser siden 2007. Og der synes ikke at være tale om en aftagende tendens.

Også fremkomsten af de store sociale netværk har medført talrige nye problemstillinger. Vi får i Datatilsynet dagligt henvendelser om Facebook og andre sociale netværk. Disse henvendelser kan både dreje sig om borgernes egne profiler og indlæg, men også om andre borgeres indlæg.




Hvorfor er persondatabeskyttelse vigtig?
Hvis man ser lidt teoretisk på det, så er persondatabeskyttelse anerkendt som en helt grundlæggende rettighed - retten til privatlivets fred. Denne rettighed er fastslået i Den Europæiske Menneskerettighedskonvention og i de grundlæggende EU-regler. Persondataloven implementerer denne rettighed i relation til persondatabeskyttelse.

Hvis man ser på det på det mere personlige plan, så har vi nok alle som mennesker nogle oplysninger, som vi gerne vil holde for os selv. Nogle oplysninger vil vi gerne dele med bestemte personer, og nogle oplysninger har vi ikke noget imod at dele med hele verden. Selv her i 2010'erne er min vurdering, at der stadig er oplysninger, som vi gerne vil have højere grad af beskyttelse om og faktisk også tager for givet, at der bliver passet godt på hos myndigheder og virksomheder.

Når vi ser på de mange henvendelser, vi i Datatilsynet modtager fra borgerne, kan vi se, at der er brug for databeskyttelse. Men der kan være meget stor forskel på, hvilket behov borgerne føler for databeskyttelse. De undersøgelser, der med jævne mellemrum bliver lavet på EU-niveau, viser også, at databeskyttelse er vigtigt for os.

Derfor har Datatilsynet en væsentlig rolle – en rolle som bliver mere og mere krævende, efterhånden som de teknologiske muligheder for at indsamle, sammenstille og dele oplysninger bliver større.

Datatilsynet har ca. 35 medarbejdere. Kan Datatilsynet føre et tilstrækkeligt tilsyn med de ressourcer?
Vi vil gerne lave flere inspektioner, end vi gør i dag. Med den udvikling, der har været på mange forskellige områder – stadig mere elektronisk behandling og øget overvågning – ville det være hensigtsmæssigt, hvis vi også kunne udføre flere inspektioner. Men i det daglige tænker vi ikke på, hvad vi ikke kan, men hvad vi kan. I sidste ende er det op til politikerne at beslutte, hvor stort Datatilsynet skal være.

Det er også vigtigt at være opmærksom på, at ansvaret for at håndtere personoplysninger rigtigt og sikkerhedsmæssigt forsvarligt i første omgang påhviler de virksomheder, offentlige myndigheder og personer, som håndterer oplysninger. Dette krav om "accountability" er også noget af det, som forslaget til ny forordning på databeskyttelsesområdet har fokus på.

Helt overordnet må jeg sige, at vi gør det, så godt vi kan. Vi har rigtig travlt. Og vi kan ikke hver dag gå op i, om vi skal være flere eller færre. Vi prøver at udvikle vores metoder og sagsgange – ja, løse vores opgaver bedst muligt med de midler, vi har.

Hvad skal de næste 10 år bruges på?
Der venter en stor udfordring med den forventede ændring af det regelgrundlag, vi fører tilsyn efter. I øjeblikket foregår diskussionerne først og fremmest på EU-niveau. Men det kan føre til store forandringer og under alle omstændigheder en kæmpe opgave med implementering og kommunikation ud til de mange aktører på databeskyttelsesområdet.

På den korte bane har vi naturligvis en løbende udfordring med at være stadig mere effektive, give god service og løse opgaverne på et højt niveau – og samtidig holde os inden for de økonomiske rammer, der er til stede.

Hvor Datatilsynet hidtil har været meget rådgivende og vejledende, vil vi fremover også have mere fokus på tilsyn. Vi vil bl.a. prøve at føre tilsyn på andre måder end vi hidtil har gjort. Som eksempel kan jeg nævne, at vi i 2012 har taget hul på online-undersøgelser, hvor vi udsender spørgeskemaer til de dataansvarlige med spørgsmål relateret til overholdelsen af persondataloven. Disse online-undersøgelser er et godt supplement til de inspektionsbesøg, vi normalt foretager.

Hvad der i øvrigt kommer af udfordringer, må tiden vise. Hvis den teknologiske udvikling bliver ved med at gå lige så stærkt som i de sidste 10 år – hvad den utvivlsomt gør – bliver der rigeligt med spændende opgaver.

Om Janni Christoffersen (f. 1962)

Direktør i Datatilsynet siden 2002.

Startede som nyuddannet cand.jur. (1987) i Civilretsdirektoratet. Har efterfølgende været ansat i Justitsministeriets departement i forskellige stillinger, bl.a. som kontorchef.

Er beskikket som dommer i Tjenestemandsretten. Har desuden været medlem af forskellige komitéer og udvalg, f.eks. Udvalget vedrørende Politiets og Forsvarets Efterretningstjenester og udvalget om offentlige myndigheders offentliggørelse af kontrolresultater. Endvidere har hun været medlem af Flygtningenævnet.

I fritiden dyrker Janni Christoffersen sin særlige interesse for fugle og natur.

Tv-overvågning

Vejledning om tv-overvågning i boligorganisationer

Datatilsynet har i efteråret 2012 offentliggjort en vejledning om boligorganisationers tv-overvågning. Vejledningen er bl.a. udarbejdet på grundlag af de erfaringer, som tilsynet har indhøstet ved gennemførelse af inspektioner hos en række boligorganisationer. Ud over at beskrive reglerne i tv-overvågningsloven og persondataloven i hovedtræk indeholder vejledningen en række konkrete eksempler til illustration heraf. Vejledningen findes på Datatilsynets hjemmeside under punktet Publikationer.

Inspektioner

I foråret 2012 har Datatilsynet gennemført inspektioner af fem boligorganisationers tv-overvågning. Formålet med inspektionerne var at indhente erfaringer omkring de problemstillinger, som forekommer i praksis ved tv-overvågning i boligorganisationer, herunder i forbindelse med eventuel anvendelse af optagelser til andre formål end kriminalitetsbekæmpelse og -forebyggelse. Det generelle indtryk fra inspektionerne var, at de fem boligorganisationer er opmærksomme på persondataloven og har fået professionel bistand til løsningerne. På inspektionerne blev der dog bl.a. konstateret problemer i forhold til overvågning i opgange, hvor kameraer pegede direkte mod beboeres indgangsdøre, mangelfuld information om tv-overvågningen og opbevaring af optagelser ud over slettefristen på maksimalt 30 dage.

Tilsynet havde i efteråret 2012 endvidere fokus på fitnesscentres tv-overvågning og foretog inspektioner hos fire fitnesscentre.

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 punktet Publikationer.

Binding Corporate Rules (BCR)

Hvad er Binding Corporate Rules?

Binding Corporate Rules (BCR) – bindende virksomhedsregler – er et sæt interne regler vedrørende databeskyttelse, der vedtages for en koncern, som har virksomheder i flere lande, herunder i tredjelande. Reglerne skal opfylde bestemte kriterier, bl.a. i forhold til registreredes rettigheder, og skal godkendes af de europæiske databeskyttelsesmyndigheder, inden de kan anvendes som hjemmelsgrundlag for overførsel af personoplysninger til tredjelande.

Når en BCR skal godkendes, anvendes en særlig procedure, hvor 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.

Datatilsynets arbejde med BCR i 2012

I 2012 modtog Datatilsynet flere ansøgninger om BCR fra danske virksomheder, og tilsynet skal derfor igen være lead authority på sådanne ansøgninger.

Flere større danske virksomheder har fået øjnene op for fordelene ved BCR-modellen, da modellen indebærer en stor fleksibilitet i forhold til overførsel til tredjelande, når reglerne først er udarbejdet, godkendt og implementeret.

Datatilsynet forudser, at endnu flere danske virksomheder i de næste år vil påbegynde arbejdet med at udforme og få godkendt bindende virksomhedsregler.

2012 var endvidere året, hvor Datatilsynet var såkaldt "co-reader" på en BCR, som det britiske datatilsyn ICO var lead authority på. I forbindelse med godkendelsen af en BCR

udvælger den valgte lead authority 2 co-readers, som assisterer i forbindelse med udarbejdelsen af de bindende virksomhedsregler.

Co-readers spiller en vigtig rolle i forhold til "mutual recognition"-proceduren, hvorefter en gruppe lande har etableret den ordning, at hvis to lande – ud over lead authority – siger god for en BCR, så godkender alle de andre lande også de bindende virksomhedsregler uden bemærkninger.

Danmark deltager ikke i mutual recognition-proceduren, da vores nationale lovgivning ikke muliggør dette.

Som co-reader har man et stort ansvar for at sikre, at de bindende virksomhedsregler yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder. Ved sikringen af dette tages der udgangspunkt i de af Artikel 29-gruppen opstillede retningslinjer (læs mere om Artikel 29-gruppen under afsnittet Internationalt samarbejde).

Når co-readerne finder, at en BCR yder tilstrækkelige garantier, sendes denne ud til databeskyttelsesmyndighederne i mutual recognition-proceduren til orientering og til de øvrige landes databeskyttelsesmyndigheder til deres eventuelle bemærkninger. Når de øvrige landes databeskyttelsesmyndigheder er kommet med deres bemærkninger, og disse er blevet adresseret, melder lead authority ud, at arbejdet med den pågældende BCR nu er afsluttet.

Herefter kan de enkelte datatilsyn så meddele tilladelse til overførsel af personoplysninger til tredjelande på baggrund af den pågældende BCR, hvis der måtte være krav derom i den nationale lovgivning.

Internationalt BCR-samarbejde

Datatilsynet deltager i en undergruppe under Artikel 29-gruppen – International Transfer Subgroup – som bl.a. arbejder med BCR.

I 2012 har arbejdet vedrørende BCR i denne undergruppe primært handlet om BCR for databehandlere.

Indtil nu har BCR været forbeholdt overførsel af personoplysninger til forskellige dataansvarlige inden for samme koncern, men fra 1. januar 2013 lægges op til, at databehandlere

også skal kunne udarbejde og implementere bindende virksomhedsregler og derigennem få mulighed for at overføre personoplysninger til hele koncernen.

Datatilsynet har indtil videre ikke kendskab til danske virksomheder, der påtænker at udarbejde en BCR for databehandlere.

Internationalt samarbejde

Europol

Som en del af tilsynet med Europols behandling af personoplysninger deltager Datatilsynet i arbejdet i Den Fælles Kontrolinstans og Det Fælles Klageudvalg for Europol.

I Den Fælles Kontrolinstans for Europol har der i 2012 været afholdt fem møder, hvor man bl.a. har drøftet resultaterne af kontrolinstansens årlige inspektion af Europol og kontrolinstansens anden inspektion målrettet Europols rolle i TFTP-aftalen mellem USA og EU. Endvidere har Den Fælles Kontrolinstans i forbindelse med evalueringen af Europol-afgørelsen[10] drøftet databeskyttelsesretlige elementer i det fremtidige retsgrundlag for Europol med Europa-Kommissionen. Endelig har Den Fælles Kontrolinstans drøftet Europa-Kommissionens ændrede forslag til Europa-Parlamentet og Rådets forordning om oprettelse af Eurodac, der indfører en adgang for Europol til oplysninger, der behandles i Eurodac-systemet. I oktober 2012 afgav Den Fælles Kontrolinstans en udtalelse om det ændrede forslag, hvor kontrolinstansen konkluderede, at Europa-Kommissionen ikke har påvist, at det er nødvendigt for Europol med adgang til oplysninger i Eurodac-systemet.

Det Fælles Klageudvalg har i 2012 afholdt ét møde. Klageudvalget har under mødet drøftet behandlingen af to klager til udvalget.

Offentliggjorte referater fra Den Fælles Kontrolinstans' møder og kontrolinstansens udtalelser kan findes via link fra Datatilsynets hjemmeside under punktet Internationalt → Europol. Her findes også generel information om Europol og Datatilsynets opgaver i relation til hertil.

Schengen

Inspektion af ambassade

Datatilsynet har i 2012 gennemført en inspektion af anvendelsen af Schengen-informationssystemet (SIS) ved den danske ambassade i Kiev i forbindelse med visumbehandlingen. Ved inspektionen gennemgik tilsynet bl.a. ambassadens procedurer for håndtering af personoplysninger fra SIS. Derudover besøgte Datatilsynet den virksomhed, som er databehandler for Udenrigsministeriet.

10 Rådets afgørelse af 6. april 2009 om oprettelse af Den Europæiske Politienhed (Europol)

Evaluering på databeskyttelsesområdet i fire Schengenlande

I første halvår 2012 havde Danmark formandskabet i Den Europæiske Union.

Datatilsynet bidrog til det danske formandskab, idet tilsynets IT-chef fungerede som Ledende Ekspert ved gennemførelsen af Schengenevalueringer på databeskyttelsesområdet i Tjekkiet, Slovakiet, Polen og Ungarn.

Schengenevaluering i et land sker på vegne af og i henhold til mandat fra Rådet for Den Europæiske Union.

Formålet med Schengenevaluering af databeskyttelsesområdet er at undersøge og vurdere implementeringen af databeskyttelse i forbindelse med Schengen-konventionen i det evaluerede land samt at rapportere observationerne til både Rådet for Den Europæiske Union og det evaluerede land. Desuden er det hensigten at give anbefalinger om mulige forbedringer på databeskyttelsesområdet i forbindelse med implementeringen af Schengen-konventionen i det evaluerede land.

Den Ledende Ekspert repræsenterer i forbindelse med evalueringen Rådet for Den Europæiske Union og har ansvaret for evalueringens gennemførelse og afrapportering.

En Schengenevaluering af databeskyttelsesområdet i et land udføres af et evalueringshold, som besøger landet. Evalueringsholdet bemandes med eksperter inden for databeskyttelse. De kommer fra andre Schengenlande end det, der evalueres. EU-Kommisionen kan vælge at deltage med en observatør.

Den Ledende Ekspert fastlægger forud og i samarbejde med det evaluerede land programmet for evalueringsholdets besøg i landet.

Forinden evalueringsbesøget har evalueringsholdet lejlighed til at gøre sig bekendt med relevant national lovgivning vedrørende databeskyttelse, Schengen og visumudstedelse i landet.

Under evalueringsbesøget i et land leder Den Ledende Ekspert evalueringsholdet og er bemyndiget til på stedet at træffe de nødvendige beslutninger til sikring af evalueringsbesøgets succesfulde gennemførelse.

I forbindelse med Schengenevalueringerne af databeskyttelsesområdet i Tjekkiet, Slovakiet, Polen og Ungarn aflagde evalueringsholdene besøg hos landets databeskyttelses-

myndighed, den nationale politimyndighed, landets SIRENE kontor, lokaliteten for det Nationale Schengen Informationssystem (NSIS) og i flere af landene også udenrigsministeriet. De besøgte myndigheder gav præsentationer, og evalueringsholdene havde lejlighed til at stille spørgsmål samt til at besigtige lokaliteter.

Schengenevaluering af databeskyttelsesområdet i et land omfatter bl.a. (i) den relevante lovgivning i landet, (ii) den nationale databeskyttelsesmyndigheds uafhængighed, ressourcer og håndhævelsesbeføjelser, (iii) den registreredes rettigheder, (iv) visumudstedelse ved landets udenrigsrepræsentationer og (v) sikkerheden omkring NSIS.

Efter et evalueringsbesøg i et Schengenland udfærdiger evalueringsholdet en evalueringsrapport, som Den Ledende Ekspert efterfølgende fremlægger for *Gruppen vedrørende Schengenevaluering* under Rådet for Den Europæiske Union.

Evalueringen af Ungarn foregik under usædvanlige omstændigheder. Op til evalueringsbesøget i Ungarn havde EU-Kommissionen sendt en *åbningsskrivelse* til Ungarn med påstand om traktatbrud vedrørende databeskyttelsesmyndighedens uafhængighed. EU-kommissionen fremskyndte processen og sendte Ungarn en såkaldt *begrundet udtalelse* i sagen. Få dage før evalueringsbesøget ændrede det ungarske parlament databeskyttelseslovgivningen. Siden evalueringsbesøget har EU-Kommissionen imidlertid stævnet Ungarn ved Den Europæiske Unions Domstol for traktatbrud.

JSA Schengen

I Den Fælles Tilsynsmyndighed for Schengen (JSA Schengen), hvor Datatilsynet er repræsenteret, er der i 2012 blevet afholdt fire møder. Her har man bl.a. drøftet den forestående overgang til det nye informationssystem (SIS II) og det retlige grundlag for Schengen-informationssystemet samt en række undersøgelser af medlemsstaternes anvendelse af SIS, herunder en opfølgning på en tidligere gennemført undersøgelse vedrørende Schengen-konventionens artikel 99 (vedrørende diskret overvågning/målrettet kontrol), en undersøgelse vedrørende artikel 95 (vedrørende eftersøgte personer) og en mindre undersøgelse af, hvordan medlemsstaternes myndigheder med adgang til SIS gøres bekendt med reglerne for håndtering af SIS.

På Datatilsynets hjemmeside under punktet Internationalt → Schengen findes generel information om Schengen-samarbejdet, Schengen-informationssystemet (SIS) og Datatilsynets opgaver i relation til SIS.

Told-informationssystemet (CIS)

På toldområdet deltager Datatilsynet i Den Fælles Tilsynsmyndighed for Told-informationssystemet (JSA Customs) og Koordinationsgruppen for tilsynet med Told-informationssystemet (CISSCG).

I Den Fælles Tilsynsmyndighed for Told-informationssystemet er der i 2012 blevet afholdt fire møder, hvor man bl.a. har drøftet omfanget af medlemsstaternes anvendelse af CIS. Man har endvidere arbejdet på en mindre vejledning vedrørende forholdet til Rådets rammeafgørelse 2008/977/RIA[11] og i samarbejde med Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) udarbejdet en fælles udtalelse vedrørende en håndbog til et nyt europæisk sagsbehandlingssystem på skatteområdet (FIDE).

I Koordinationsgruppen for tilsynet med Told-informationssystemet er der i 2012 blevet afholdt to møder, hvor man ud over den fælles udtalelse om FIDE-håndbogen bl.a. har drøftet tilsynet med Det Europæiske Kontor for Bekæmpelse af Svigs (OLAF) behandling af oplysninger fra CIS. Gruppen er endvidere blevet orienteret om og har drøftet udviklingen af ny regulering på toldområdet med Europa-Kommissionen. Endelig har gruppen foretaget en undersøgelse af, hvilke myndigheder og dele af myndigheder der har adgang til CIS.

Eurodac

Som led i tilsynet med Eurodac deltager Datatilsynet i Koordinationsgruppen for tilsynet med Eurodac (ESCG). I 2012 er der afholdt to møder, hvor man bl.a. har drøftet Europa-Kommissionens forslag til ændring af Eurodac-forordningen og foretaget en undersøgelse af eventuelle problemer med ulæselige fingeraftryk i medlemsstaterne.

Ved det ene møde i første halvår af 2012 har man endvidere drøftet emner i relation til Visum-informationssystemet (VIS), herunder udviklingen og status for den praktiske implementering af systemet.

På Datatilsynets hjemmeside under punktet Internationalt → Eurodac findes generel information om Eurodac og Datatilsynets opgaver i relation hertil.

11 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, s. 38.

Visum-informationssystemet (VIS)

I sidste halvår af 2012 blev det første møde i Koordinationsgruppen for tilsynet med Visum-informationssystemet (VISSCG) afholdt. Datatilsynet er repræsenteret i denne gruppe. På mødet blev rammerne for fremtidige møder drøftet, ligesom udviklingen og status for implementeringen af Visum-informationssystemet (VIS) blev drøftet.

Artikel 29-gruppen

I relation til Artikel 29-gruppens arbejde i 2012 skiller tre ting sig ud: 1) Gruppens arbejde med udkast til forordning om databeskyttelse, 2) en udtalelse om cloud computing og 3) den såkaldte Google-sag.

1. Arbejdet vedrørende forordningsudkastet sker primært i 'Future of Privacy'-undergruppen. Der er i 2012 blevet godkendt to arbejdsdokumenter vedrørende det nye forordningsudkast.

2. Cloud Computing har fyldt ganske meget i billedet de sidste par år, og i 2012 kom en længe ventet udtalelse fra Artikel 29-gruppen vedrørende cloud computing. Heri beskrives nogle af problemstillingerne ved brugen af cloud computing samtidig med, at Artikel 29-gruppen kommer med en række anbefalinger på området.

3. Den vigtigste enkeltsag i 2012 i Artikel 29-sammenhæng har været en sag om Google's nye privatlivsindstillinger. Artikel 29-gruppen anmodede det franske datatilsyn (CNIL) om at agere som ledende datatilsyn i sagen, og arbejdsgruppen har dermed også indledt en proces, som kan blive hverdagen, hvis databeskyttelsesområdet overgår til regulering ved en forordning.

På Datatilsynets hjemmeside under punktet Internationalt → Artikel 29-gruppen findes generel information om Artikel 29-gruppen. Her findes også link til Artikel 29-gruppens dokumenter.

WPPJ

I marts 2012 blev det sidste møde i arbejdsgruppen Working Party on Police and Justice (WPPJ) afholdt. Her blev gruppens arbejde – fra 2011 – afrundet og afsluttet.

WPPJ blev nedsat af de europæiske datatilsyn til at undersøge udviklingen inden for det strafferetlige område med særlig fokus på databeskyttelsesretlige problemstillinger. Fremover vil arbejdet med disse områder og problemstillinger foregå i regi af Artikel 29-gruppen.

Eurojust

I Den Fælles Kontrolinstans for Eurojust (JSB Eurojust), hvor Datatilsynet er repræsenteret, er der i 2012 afholdt ét møde. Her drøftede medlemmerne bl.a. to appelsager og implementeringen af artikel 13 i Eurojust-afgørelsen[12].

JSB overvåger kollektivt Eurojust's aktiviteter, der involverer behandling af persondata, og sikrer, at disse udføres i henhold til Eurojust-afgørelsen.

Europarådet

I 2012 har ændringer af Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger været behandlet i arbejdsgruppen om databeskyttelse. Datatilsynet har ikke deltaget i møderne i 2012.

Berlin-gruppen

International Working Group on Data Protection in Telecommunication, også kaldet Berlin-gruppen, har i 2012 afholdt to møder. I april mødtes gruppen i Sopot efter invitation fra det polske datatilsyn (Giodo), og i september mødtes gruppen i Berlin.

Berlin-gruppen besluttede allerede i april 2011 på sit møde i Montreal at udarbejde en udtalelse om cloud computing. Datatilsynet har været primus motor på arbejdet med udtalelsen, som blev vedtaget på mødet i Sopot. Udtalelsen er nu også kendt som *Sopot Memorandum*. Udtalelsen belyser risici for databeskyttelse i forbindelse med cloud computing og giver anbefalinger til interessenter inden for området.

12 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

I forbindelse med Berlin-gruppens møder i 2012 er der bl.a. blevet drøftet spørgsmål om privacy og databeskyttelsesaspekter i forbindelse med IPv6, geolokalisering, sociale netværk, håndtering af grænseoverskridende sikkerhedsbrister og web tracking.

Nordisk samarbejde

I 2012 afholdt de nordiske datatilsynsmyndigheder i Norge, Sverige, Finland, Åland, Island, Færøerne og Danmark for første gang et stort fælles møde for både chefer, sagsbehandlere, it-teknikere og informationsmedarbejdere. Mødet foregik i Oslo.

På mødet blev den fremtidige regulering af persondatabeskyttelse diskuteret, idet EU-Kommissionen netop havde offentliggjort sit udspil til nye regler om beskyttelse af personoplysninger i EU. Desuden blev der afholdt separate sessioner for henholdsvis cheferne, sagsbehandlerne, it-teknikerne og informationsmedarbejderne.

It-sikkerhed

Cloud computing

Cloud computing må stadig betragtes som en forholdsvis ny måde at anvende it-ressourcer på, og behandling af personoplysninger i cloud-løsninger giver fortsat anledning til en række databeskyttelsesretlige udfordringer. Cloud computing var således også i 2012 højt på Datatilsynets dagsorden.

Hvad er cloud computing?

Cloud computing kan defineres 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[14]. 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 afgav i 2012 to udtalelser vedrørende Microsofts cloud-løsning Office 365 og en udtalelse vedrørende en sikkerhedsbrist, der opstod som følge af KL's overførsel af kommunernes køreprøvesystem til en cloud-løsning.

KL's overførsel af køreprøvesystem til en cloud-løsning

Datatilsynet blev i 2011 på baggrund af en henvendelse fra Dansk Kørerlærer-Union opmærksom på, at der havde været en sikkerhedsbrist i kommunernes køreprøvesystem.

13 Se It-sikkerhedskomiteens publikation "Sikkerhed i cloud computing" fra december 2010

Datatilsynet indledte på baggrund heraf en nærmere undersøgelse af sagen af egen drift. Det fremgik af oplysningerne i sagen, at køreprøvesystemet indeholdt oplysninger om elevers navn, adresse, personnummer og bestået og ikke-bestået prøver samt oplysninger om kørelæreres navn, telefonnummer, e-mailadresse og personnummer. Det fremgik endvidere af sagen, at der i forbindelse med omlægning af driften af systemet til cloud-løsningen Microsoft Azure skete en fejl i opsætningen, der betød, at kørelærere, som loggede på systemet i enkelte perioder, overtog andre samtidige brugeres rettigheder, herunder adgang til oplysninger om andre kørelærere og disses elever. I hvert fald tre kørelærere havde som følge heraf haft adgang til andre kørelæreres data.

Datatilsynet udtalte i sit brev af 3. april 2012 kritik af KL's håndtering af personoplysninger i køreprøvesystemet og fremhævede i den forbindelse navnlig følgende forhold:

- KL handlede som dataansvarlig uden at være berettiget dertil.
- Persondatalovens krav om, at oplysninger skal beskyttes med de fornødne sikkerhedsforanstaltninger, blev ikke iagttaget.
- KL overførte køreprøvesystemet til en cloud-løsning uden at leve op til persondatalovens krav om en skriftlig databehandleraftale.
- KL's begrundelse om, at data ikke har været behandlet uden for EU, var ikke tilstrækkelig, da der kan være sket overførsel til Microsoft Corporation i USA.

Datatilsynet fandt endvidere, at der var behov for, at KL indhentede en revisionserklæring fra en uafhængig tredjepart med henblik på at få bekræftet, at oplysningerne fra kommunernes system var blevet slettet uigenkaldeligt i den anvendte cloud-løsning. Tilsynet lagde herved vægt på, at der var tale om, at personoplysninger – bl.a. omfattende private og fortrolige oplysninger – var overført uden om de dataansvarlige kommuner og uden databehandleraftale.

Behandling af personoplysninger i cloud-løsningen Office 365

Datatilsynet modtog i starten af 2012 en henvendelse fra IT-Universitet i København vedrørende brug af Microsofts cloud-løsning Office 365 som e-mail- og kalenderløsning. I forbindelse med Datatilsynets behandling af IT-Universitetets henvendelse blev der på Microsofts initiativ indledt en dialog mellem Datatilsynet og Microsoft.

På baggrund af denne dialog afgav Datatilsynet – efter behandling af sagen på et møde i Datarådet – den 6. juni 2012 en udtalelse til Microsoft, hvor tilsynet dels fremkom med bemærkninger om Microsofts ansvar som henholdsvis databehandler og dataansvarlig,

dels omtalte en række spørgsmål, som danske dataansvarlige vil skulle tage i betragtning ved brug af Office 365.

Blandt de spørgsmål, som danske dataansvarlige skal tage i betragtning ved brug af Office 365, omtalte Datatilsynet persondatalovens krav til tredjelandsoverførsel og datasikkerhed. Tilsynet omtalte herunder særligt følgende:

- kravet om aftale og kontrol med databehandlere,
- kravet om risikovurdering og
- kravet om logning.

IT-Universitetets brug af cloud-løsningen Office 365

Som nævnt ovenfor modtog Datatilsynet i starten af 2012 en henvendelse fra IT-Universitetet i København vedrørende brug af Microsofts cloud-løsning Office 365 som e-mail- og kalenderløsning. Henvendelsen skete i form af anmeldelse af ændringer til IT-Universitetets tidligere fremsendte anmeldelser vedrørende personale- og studieadministration.

Efter at have indhentet en række oplysninger fra IT-Universitetet og været i dialog med Microsoft afgav Datatilsynet – efter behandling af sagen på et møde i Datarådet – den 10. juli 2012 en udtalelse til IT-Universitetet vedrørende den påtænkte brug af Office 365.

Datatilsynet gjorde i sin udtalelse opmærksom på følgende forhold:

- Overførsel af personoplysninger til et tredjeland på baggrund af Kommissionens standardkontraktbestemmelser kræver tilladelse fra Datatilsynet. Forinden de anmeldte ændringer blev sat i kraft, var det således påkrævet, at IT-Universitetet anmodede om en sådan tilladelse, og at IT-Universitetet i den forbindelse fremsendte kopi af den/de indgåede standardkontrakt(er) eller anvendte den forenklede procedure for tredjelandsoverførsel baseret på standardkontraktbestemmelserne.
- Datatilsynet havde ved brev af 6. juni 2012 afgivet en udtalelse til Microsoft vedrørende behandling af personoplysninger i Office 365. Tilsynet henviste til denne udtalelse for nærmere information om, hvilke krav IT-Universitetet bl.a. skal leve op til ved brug af Office 365.
- Datatilsynet godkender ikke databehandleraftaler og skal ikke have sådanne forelagt. Det var således IT-Universitetets ansvar at sikre sig, at der blev indgået en databehandleraftale med Microsoft, som lever op til persondatalovens krav.

- Datatilsynet havde ikke på baggrund af den fremsendte it-risikoanalyse mulighed for at vurdere, om IT-Universitetets risikovurdering var foretaget på grundlag af indsigt i reelle forhold hos Microsoft, eller om den foretagne risikovurdering i øvrigt var tilstrækkelig.
- Datatilsynet gik ud fra, at IT-Universitetet ville foretage en risikovurdering i forhold til samtlige aspekter af den påtænkte anvendelse af cloud-løsningen baseret på indsigt i reelle forhold hos Microsoft, inden behandlingen af personoplysninger i Office 365 blev iværksat.
- IT-Universitetet burde navnlig være opmærksom på sit ansvar for, at uvedkommende ikke kan få adgang til personoplysninger, som behandles i cloud-løsningen, herunder ved at sikre sig, at der anvendes betryggende og effektive sletteprocedurer.
- Tilsynet anbefalede, at IT-Universitetet undersøgte mulighederne for – og så vidt muligt sørgede for – at personoplysninger lagres i krypteret form hos Microsoft.
- Sikkerhedsforanstaltningerne ved transmission og login samt spørgsmålet om logning burde efter tilsynets vurdering også indgå i IT-Universitetets risikovurdering og videre overvejelse om anvendelse af Office 365.

Under forudsætning af, at IT-Universitetets behandling af personoplysninger ved brug af Office 365 skete under iagttagelse af reglerne i persondataloven og sikkerhedsbekendtgørelsen, gav de fremsendte ændringer ikke Datatilsynet anledning til yderligere bemærkninger.

Læs mere

Datatilsynets udtalelser til KL, Microsoft og IT-Universitetet i København er tilgængelige på tilsynets hjemmeside under punktet Afgørelser.

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

Arbejdsgruppe

Den tidligere regering 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. Datatilsynet har været repræsenteret i denne arbejdsgruppe.

Arbejdsgruppen afgav den 4. juli 2012 et notat om love og regler, der unødigt vanskeliggør anvendelsen af cloud computing, hvori enkelte ændringer af sikkerhedsbekendtgørelsen blev foreslået. Datatilsynet har bl.a. på baggrund heraf i slutningen af 2012 indledt overvejelser om revision af sikkerhedsbekendtgørelsen.

NemID for private

Hvad er NemID for private?

NemID dækker over mange forskellige typer log-in til både den offentlige og private sektor. Som borger har man mulighed for at anskaffe en version af NemID, der giver adgang til f.eks. offentlig selvbetjening eller online spillesider. Denne version af NemID gør brug af en offentlig og en privat certifikatnøgle, hvor den private nøgle oprindeligt kun kunne opbevares hos CA (Certification Authority), som på daværende tidspunkt var DanID.

Det er Datatilsynets opfattelse, at et generelt hensyn til brugernes privacy taler for, at brugerne skal have et valg med hensyn til, hvor deres private nøgle opbevares. Datatilsynet opfordrede derfor allerede i 2009 til, at der hurtigst muligt blev skabt mulighed for egen opbevaring af den private nøgle. Datatilsynet anbefalede endvidere, at det overvejedes, om ikke muligheden for egen opbevaring af den private nøgle burde være gratis, eller at prisen i det mindste blev så lav som muligt og alene kom til at afspejle omkostningerne. Senest i forbindelse med lovforslag om obligatorisk digital selvbetjening[14] i 2012 har Datatilsynet henvist til problemstillingen omkring opbevaring af borgernes private nøgle.

I slutningen af 2012 blev der etableret mulighed for, at borgere mod betaling kan få en NemID, hvor den private nøgle etableres på hardware, som er i borgerens besiddelse. I

14 Forslag til lov om ændring af lov om Det Centrale Personregister, lov om dag-, fritids- og klubtilbud mv. til børn og unge, lov om folkeskolen og sundhedsloven

den forbindelse har tilsynet evalueret registreringsprocedurerne, som benyttes ved bestilling af såkaldt "NemID på hardware".

Datatilsynet har også i andre sammenhænge udtalt sig om NemID i 2012:

Brug af medarbejderes private NemID

På baggrund af henvendelser fra Kommunernes Landsforening (KL) samt en række kommuner har Datatilsynet vurderet brugen af medarbejderes private NemID i kommunernes log-in procedurer.

Datatilsynet afgav den 30. marts 2012 – efter at sagen havde været behandlet på et møde i Datarådet – en udtalelse til KL, som sammenfattede tilsynets konklusioner, og som indeholdt seks konkrete eksempler på brug af medarbejdernes private NemID i kommunernes log-in procedurer.

Datatilsynet udtalte bl.a., at medarbejderes private NemID kan anvendes ved log-in som alternativ til en adgang med brugernavn og adgangskode under følgende forudsætninger:

- der må alene være tale om adgang til oplysninger, som hverken er af følsom eller fortrolig karakter, og
- brug af den private NemID skal være et frivilligt tilbud for medarbejderne.

Desuden udtalte Datatilsynet, at den private NemID kan anvendes som ekstra faktor, f.eks. når en sådan er påkrævet ved log-in til registre med følsomme personoplysninger via internet under følgende forudsætninger:

- den dataansvarlige myndighed skal sikre, at behandlingen af personoplysninger via den omhandlede adgang i det hele lever op til sikkerhedsbekendtgørelsen
- brug af den private NemID til log-in skal være et frivilligt tilbud.

Udtalelsen i dens helhed med de indeholdte eksempler er tilgængelig på Datatilsynets hjemmeside under punktet Afgørelser.

Datatilsynets inspektioner

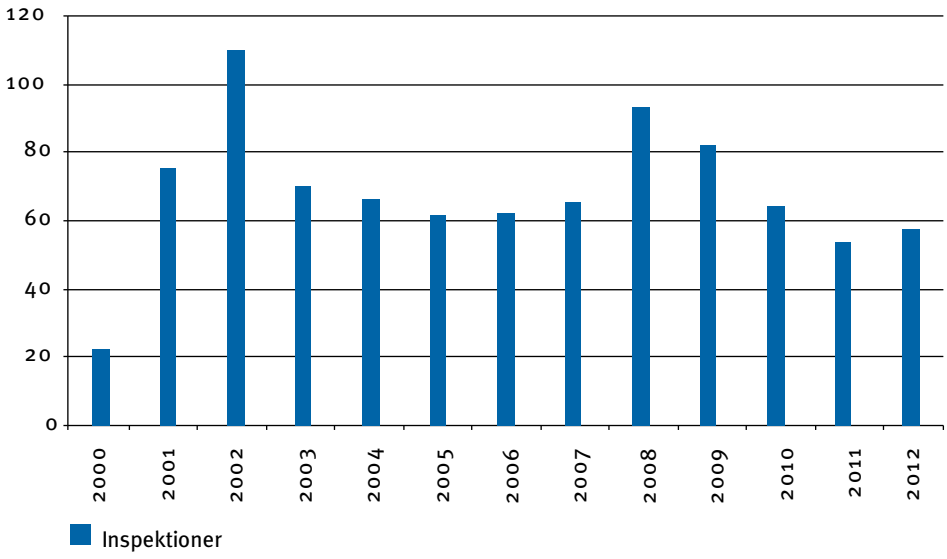
Inspektioner i 2012

Datatilsynet foretog i 2012 58 inspektioner. Disse inspektioner var fordelt på offentlige myndigheder, private virksomheder, private forskere mv.

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.



Særlige fokusområder

Datatilsynet gennemførte i 2012 8 inspektioner efter en ny model, hvor temaet for inspektionerne var indretning af ESDH-systemer. Fokus var først og fremmest på medarbejdernes adgange til personoplysninger i ESDH-systemerne.

Inspektionerne blev afholdt hos 8 jyske kommuner. 2 hold medarbejdere gennemførte hver 4 inspektioner fordelt på 2 dage. Tilsynet havde på forhånd udarbejdet et standardskema med spørgsmål. Kommunens svar fra inspektionen blev under besøget indsat i skemaet og gennemgået med kommunen. Efterfølgende har tilsynet til kommunerne fremsendt bemærkninger til de enkelte inspektioner. Datatilsynet vil i 2013 offentliggøre en informationstekst, som afspejler tilsynets erfaringer fra inspektionerne.

Datatilsynet har i 2012 for første gang foretaget inspektioner vedrørende tv-overvågning hos boligorganisationer. Læs mere om disse inspektioner under afsnittet Tv-overvågning. Tilsynet har desuden gennemført 4 inspektioner vedrørende tv-overvågning hos fitnesscentre.

Desuden har Datatilsynet i 2012 gennemført Schengenevalueringer på databeskyttelsesområdet i 4 Schengenlande samt gennemført en inspektion af anvendelsen af Schengeninformationssystemet (SIS) ved den danske ambassade i Kiev. Læs mere herom i afsnittet Internationalt samarbejde.

Online-undersøgelser

En inspektion indebærer normalt, at 2-3 af Datatilsynets medarbejdere møder op hos den dataansvarlige, får beskrevet den dataansvarliges behandling af personoplysninger og foretager stikprøvekontroller, besigtigelse af lokaliteter mv.

I 2012 har Datatilsynet imidlertid gennemført et pilotprojekt med online-undersøgelser, hvor inspektionerne ikke afholdes hos den dataansvarlige, men i stedet gennemføres skriftligt ved hjælp af elektroniske spørgeskemaer. Det kan dog være nødvendigt også at indhente supplerende oplysninger telefonisk.

De i 2012 afholdte online-undersøgelser har rettet sig mod private forsknings- og statistikprojekter.

I online-undersøgelserne udsender Datatilsynet elektronisk et spørgeskema til den dataansvarlige forsker. Dette sker via et særligt spørgeskemasystem. Den dataansvarlige bes-

varer spørgeskemaet elektronisk. Spørgsmålene relaterer sig til de vilkår, som Datatilsynet har stillet i sin tilladelse til den dataansvarliges projekt.

Hvis besvarelsen indikerer, at der sker behandling af personoplysninger, som ikke lever op til Datatilsynets vilkår eller persondataloven i øvrigt, følger Datatilsynet op på, at den dataansvarlige bringer forholdene i orden.

I 2012 har Datatilsynet gennemført 13 online-undersøgelser. Ud af disse gav 10 efter endt sagsbehandling ikke Datatilsynet anledning til at konstatere, at var sket behandling af personoplysninger i strid med tilsynets vilkår. I 1 sag skulle der ske ændring af den dataansvarliges anmeldelse. I 2 projekter skete der ikke den fornødne kryptering af elektroniske identifikationsoplysninger eller erstatning af identifikationsoplysninger med kodenummer. Desuden kunne Datatilsynet i 1 af disse projekter konstatere, at der var sket videregivelse af oplysninger uden den fornødne tilladelse fra tilsynet.

Online-undersøgelserne indebærer, at der ikke sker en fysisk besigtigelse fra tilsynets side, sådan som tilsynet ellers typisk gør ved inspektioner på stedet hos de dataansvarlige. Der er tale om en mere summarisk inspektionsform, som ikke giver tilsynet mulighed for at stille uddybende spørgsmål/kontrolspørgsmål.

På den anden side er online-undersøgelserne efter Datatilsynets opfattelse et godt supplement til de traditionelle inspektioner hos de dataansvarlige. Dels kan online-undersøgelserne afdække nogle åbenbare mangler hos de dataansvarlige, dels skaber undersøgelserne bevidsthed hos de dataansvarlige om tilsynets vilkår. Samtidig er der tale om en inspektionsform, som kræver færre ressourcer end en inspektion, hvor flere af tilsynets medarbejdere møder op hos den dataansvarlige. Hertil kommer, at online-undersøgelserne giver mulighed for at lave tematiserede kontroller, hvor resultaterne fra flere undersøgelser kan sammenlignes og udviklingstendenser uddrages. Datatilsynet vil derfor også i 2013 benytte denne inspektionsform.

Oversigt over udførte inspektioner i 2012

Staten:
Ambassaden i Kiev (visum/SIS)
Københavns Vestegns Politi
Schengen-evaluering (Tjekkiet/Slovakiet)
Schengen-evaluering (Ungarn/Polen)
Hjemmeværnskommandoen

Kommuner:
Glostrup Kommune
Roskilde Kommune
Frederiksberg Kommune (utilsigtede hændelser i sundhedsvæsenet)

Temainspektioner – indretning af ESDH-systemer:
Mariagerfjord Kommune
Vesthimmerlands Kommune
Skive Kommune
Favrskov Kommune
Syddjurs Kommune
Norddjurs Kommune
Morsø Kommune
Randers Kommune

Regioner:
Region Sjælland (utilsigtede hændelser i sundhedsvæsenet)
Region Syddanmark (telemedicin)

Tv-overvågning:
Temainspektioner – tv-overvågning i private boligorganisationer:
Tranemosegård, Brøndby Strand
AB Askerød, Greve
Boligselskabet Baldersbo
AB Hørsholm Kokkedal
SAB Samvirkende Boligselskaber



Temainspektioner – tv-overvågning i fitnesscentre:
Fitnessworld (Brøndby)
Fitnessworld (Gothersgade)
Fitness dk (Adelgade)
Fitness dk (ABC)

Privat forskning og statistik:
Bianca Albers
Karsten Albæk
Carrinna Hansen
Kasper Hornbæk
Lisbeth Hybholt
Frank Ebsen
Dansk Psykologisk Forlag A/S
Lone Rønnov-Jessen
Eva Welander

Alternative behandlere:
Helle Haugaard
Michelle Kossmann

Whistleblower:
Carlsberg A/S
Tryg Forsikring A/S
Danske Bank A/S

Øvrige private:
Danmarks Apotekerforening
McDonald's Danmark ApS (personaleadministration)
Arto ApS (skriftlig undersøgelse)
watAgame ApS (skriftlig undersøgelse)

Online-undersøgelser (privat forskning og statistik):
Lene Mellemkjær
Johnni Hansen
Tove Klausen
Erika G. Spaich
Jesper Carl
Henrik Nielsen



Christian Godballe
Johnny Østergaard Keller
Thomas Benfield
Steinbjørn Hansen
Ole Raaschou-Nielsen
Lone Graff Stensballe
Peter Henrik Andersen

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