DATATILSYNET

# Datatilsynets årsberetning 2015

Udgiver: Datatilsynet
Tryk og layout: Rosendahls A/S
Beretningen er sat med Meta
Oplag: 180
Juli 2016
ISSN nr: 1601-5657
ISBN nr: 978-87-999222-0-8

# Datatilsynets årsberetning 2015

# Indhold

# Til Folketinget

Datatilsynet har i 2015 fortsat bestræbelserne på at effektivisere arbejdsgange og sagsbehandling med henblik på at få mest muligt ud af de ressourcer, som tilsynet har til rådighed. Året har imidlertid også i vidt omfang været præget af arbejdet med større sagskomplekser og opgaver af international karakter.

Datatilsynet har behandlet flere større og mere principielle sager om behandling af personoplysninger hos såvel private virksomheder som offentlige myndigheder.

Datatilsynet udtalte således kritik af en regions indretning af den fælles elektroniske patientjournal. Tilsynet fandt, at systemet ikke levede op til persondatalovens regler, ligesom det fandtes tvivlsomt, om sundhedslovens regler om indhentning af elektroniske helbredsoplysninger var opfyldt. Datatilsynet rejste i den forbindelse over for Sundhedsministeriet (nu Sundheds- og Ældreministeriet) nogle spørgsmål om rækkevidden af reglerne i sundhedsloven.

I forbindelse med Rigspolitiets overvejelser om at indføre et system med automatisk nummerpladegenkendelse (ANPG) har Datatilsynet afgivet udtalelser, herunder i forbindelse med udstedelsen af en bekendtgørelse om politiets brug af ANPG, som er affattet i overensstemmelse med Datatilsynets tilkendegivelser.

Spørgsmål om datasikkerhed har også i høj grad været i fokus, og Datatilsynet har behandlet flere sager om større sikkerhedsbrister. Datatilsynet har også revideret sine retningslinjer om offentlige myndigheders kommunikation med borgerne via sms og e-mail, og endvidere har tilsynet bl.a. afgivet udtalelse om hackerangrebet mod CSC i 2012.

Datatilsynets virksomhed har i 2015 tillige været præget af flere større opgaver af international karakter.

Datatilsynet har bl.a. lagt mange ressourcer i arbejdet med bindende virksomhedsregler (BCR – Binding Corporate Rules), der giver mulighed for, at virksomheder inden for en koncern kan overføre personoplysninger mellem hinanden, også selv om overførslen sker til lande uden for EU/EØS. Datatilsynet har været "lead authority" på flere danske virksomheders BCR og har endvidere deltaget som "co-reader" i forhold til udenlandske virksomheders BCR.

I oktober 2015 afsagde EU-Domstolen dom i en præjudiciel forelæggelse fra den irske High Court i en sag mellem en østrigsk statsborger og det irske datatilsyn. EU-Domstolen fastslog bl.a., at den såkaldte Safe Harbor-ordning er ugyldig. Dommen vil i praksis bl.a. få betydning for virksomheder, der overfører oplysninger til en dataansvarlig eller en databehandler i USA, som har tilsluttet sig ordningen, idet en sådan overførsel ikke længere vil blive betragtet som sikker. Dommen har imidlertid også betydning for overførsel af oplysninger, der sker på andet grundlag end Safe Harbor, og Datatilsynet deltager i det omfattende fælleseuropæiske arbejde med at klarlægge dommens konsekvenser og finde mulige løsningsmodeller.

Datatilsynet har endvidere fulgt arbejdet med et nyt retsgrundlag. Efter flere års arbejde blev der i december 2015 i Bruxelles opnået enighed mellem Kommissionen, Rådet og Europa-Parlamentet om teksten til en forordning, der skal afløse databeskyttelsesdirektivet fra 1995. Forordningen blev endeligt vedtaget i april 2016 og får virkning fra den 25. maj 2018.

Forordningen vil få stor betydning for Datatilsynets fremtidige arbejde. 2016 og de kommende år vil derfor i meget vidt omfang komme til at stå i forordningens tegn, og Datatilsynet vil sætte betydelige ressourcer ind på at opnå et tilbundsgående kendskab til det nye retsgrundlag og på at forberede overgangen til dette såvel nationalt som internationalt.


# Datatilsynets virksomhed i 2015

## 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. 639 af 12. juni 2013.

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 2014 bl.a. haft følgende opgaver:

- Information og vejledning
- 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 og lign.

Det er Datatilsynets vision, at myndigheder og private kender og overholder reglerne for behandling af personoplysninger, og at borgerne kender og kan bruge deres rettigheder. Datatilsynet gør dette muligt og lettere gennem synlighed, information, dialog og kontrol.

## 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. Herudover har Datatilsynet også i 2015 publiceret særlige it-sikkerhedstekster om forskellige it-sikkerhedsemner.

Datatilsynet bidrager løbende med oplæg på forskellige konferencer og møder. I 2015 har Datatilsynet deltaget med 27 af sådanne oplæg. Eksempelvis har Datatilsynet holdt oplæg for kommunale jurister om Datatilsynets inspektioner hos kommuner. Datatilsynet har også deltaget i debatter på Folkemødet på Bornholm, ligesom tilsynets direktør har holdt oplæg om fremtidens Datatilsyn på to persondata-seminarer. Datatilsynet deltog igen i 2015 endvidere på den årlige digitaliseringsmesse i Odense. Det er Datatilsynets oplevelse, at der bliver større og større efterspørgsel efter at få tilsynet til at stille op og med sin særlige ekspertise og tilsynsrolle fortælle om persondataretlige problemstillinger. Endvidere er den fremtidige regulering på databeskyttelsesområdet og Datatilsynets rolle i den forbindelse et emne, som interesserer mange. Samtidig giver sådanne oplæg tilsynet god mulighed for at komme i dialog med både dataansvarlige og registrerede og på den måde bl.a. få indblik i, hvilke persondataretlige udfordringer de dataansvarlige i praksis møder.

På den årlige databeskyttelsesdag den 28. januar informerede Datatilsynet også nærmere om persondataretlige emner. Datatilsynet markerede dagen ved at invitere borgere og professionelle med interesse for persondataret til sessioner om følgende emner: 1. Præsentation af Datatilsynet – hvad laver tilsynet egentlig? 2. Korrekt håndtering af borgernes rettigheder hos myndighederne 3. Databeskyttelse i forskning 4. Datasikkerhed i borgerservicecentre. Datatilsynet deltog endvidere med et indlæg på en konference på Christiansborg i anledning af databeskyttelsesdagen. Indlægget havde titlen "Årets afgørelser og iagttagelser".

Herudover er telefonisk rådgivning en stor del af Datatilsynets arbejde. Tilsynet har i 2015 registreret 13.388 telefoniske henvendelser. Antallet af telefoniske henvendelser har dermed været på et lidt lavere niveau end i 2014 (ca. 14.000 opkald).

Datatilsynet giver endvidere vejledning på baggrund af skriftlige forespørgsler om persondataloven. Nedenfor ses et eksempel på en sådan sag.


## Automatisk nummerpladegenkendelse (ANPG)

Rigspolitiet rettede i januar 2015 henvendelse til Datatilsynet med et ønske om anvende ANPG til at understøtte politiets opgaver, herunder til understøttelse af kontrolopgaver og efterforskning af lovovertrædelser. Systemet består af stationære ubemandede ANPG-kameraer, der opstilles på udvalgte steder, og bemandede ANPG-kameraer monteret på flere af politiets køretøjer.

Datatilsynet udtalte efter behandling af spørgsmålet i Datarådet, at der er behov for en nærmere regulering af behandlingen af personoplysninger i forbindelse med ANPG. Tilsynet lagde herved vægt på, at omfanget af oplysninger og karakteren af visse personoplysninger tilsiger, at behandlingen sker på et tilstrækkeligt præcist grundlag, og at en sådan regulering som minimum bør ske ved bekendtgørelse.

Justitsministeriet har på baggrund af Datatilsynets tilkendegivelser sidenhen udarbejdet en bekendtgørelse om politiets anvendelse af ANPG (bekendtgørelse nr. 1776 af 16. december 2015).

**Hvad er ANPG?**

ANPG indebærer, at der via kameraer optages fotos af køretøjer, som passerer forbi kameraet, hvorefter speciel software automatisk udfinder nummerpladeoplysninger fra fotoet. Nummerpladeoplysningerne kan herefter dels (umiddelbart) søges i relevante databaser, dels (eventuelt) lagres med oplysninger om position samt data og tidspunkt vedrørende optagelsen.

## Klagesagsbehandling

I klagesagerne træffer Datatilsynet afgørelse om, hvorvidt en behandling af personoplysninger er sket i overensstemmelse med persondataloven.

Når Datatilsynet modtager en klage fra en borger, kigger tilsynet på, om den dataansvarlige allerede har modtaget en henvendelse fra borgeren med en klage over forholdet. Hvis ikke borgeren selv har rettet henvendelse til den dataansvarlige, sender tilsynet som udgangspunkt borgerens klage videre til den dataansvarlige, så denne i første omgang kan foretage en vurdering af, om behandlingen af personoplysninger er berettiget. Tilsynet underretter samtidig borgeren og den dataansvarlige om muligheden for på ny at rette henvendelse til tilsynet, hvis borgeren ikke er tilfreds med den dataansvarliges besvarelse.

I 2015 har tilsynet registreret et fald på 12,1 % i antallet af nye sager (forespørgsler og klager) vedrørende private virksomheder mv. (fra 1.265 i 2014 til 1.112 i 2015). Hvad angår lignende sager vedrørende offentlige myndigheder, er der i 2014 registreret et fald på 14,8 % i antallet af nye sager (fra 975 i 2014 til 831 i 2014).

Nedenfor ses et eksempel på en klagesag, som Datatilsynet i 2015 traf afgørelse i.

### Taxiselskabs registrering af oplysninger om vognmænds færden via GPS

Datatilsynet traf afgørelse i en sag, hvor flere vognmænd, der var tilknyttet et bestemt taxiselskab, havde klaget over, at selskabet foretog GPS-overvågning af alle hyrevogne, der var tilmeldt selskabet.

Det fremgik, at GPS-overvågningen foregik ved, at vognens position blev lagret, når bestillingskontoret sendte en tur ud til vognen. Hvis føreren af vognen ikke kørte ud på den adresse, som den var sendt ud til, eller hvis føreren meldte forgæves tur fra en anden position end den, hvor vognen var sendt til, ville dette afsløres af systemet ved næste taxameterstart. Det var endvidere oplyst, at selskabets kontraktskunder stillede krav om, at alle vogne skulle sende GPS-positioner til centralen hvert minut.

Det fremgik endvidere, at selskabet havde orienteret om brugen af GPS på et vognmandsmøde, og at kontrolfunktionerne havde været omtalt i selskabets interne blad.


Datatilsynet lagde ved sin vurdering af sagen til grund, at GPS-overvågningen bl.a. havde til formål at effektivisere bestillingscentralens daglige arbejde, idet ledige vogne kunne lokaliseres hurtigt og nemt, at effektivisere behandlingen af kundeklager, idet rigtigheden af en kundes påstand om kørsel af omveje nemt kunne undersøges, og at sikre hurtig reaktion i alarmsituationer.

Endvidere måtte Datatilsynet lægge til grund, at GPS-overvågningen var blevet brugt til at overvåge vognmændenes færden, idet ledelsen i taxiselskabet efter det oplyste havde anvendt registreringer fra GPS-overvågningen til at konfrontere vognmænd med deres færden i forbindelse med mistanke om kørsel uden om bestillingskontoret.

Datatilsynet tilkendegav, at det umiddelbart var tilsynets opfattelse, at en sådan brug af oplysninger fra GPS-overvågning efter omstændighederne må antages at leve op til kravet om proportionalitet i persondatalovens § 5, stk. 3. Datatilsynet fandt endvidere, at taxiselskabet ved at behandle oplysninger fra GPS-overvågningen forfulgte en berettiget interesse, og at hensynet til de registrerede chauffører ikke oversteg denne interesse, jf. persondatalovens § 6, stk. 1, nr. 7.

Datatilsynet fandt imidlertid, at systemet burde indrettes på en sådan måde, at der kun foretages GPS-overvågning af vognmanden, når denne er på vagt.

Datatilsynet lagde i den forbindelse navnlig vægt på det oplyste om forholdet mellem bestillingskontor og bevillingshaver og på, at GPS-overvågningen var konstant, dvs. at vognmændene og chaufførerne også blev overvåget, når de holder pause eller befinder sig hjemme. Dette er efter Datatilsynets opfattelse ikke i overensstemmelse med kravet i persondatalovens § 5, stk. 3, hvoraf det følger, at oplysninger, som behandles, ikke må omfatte mere, end hvad der kræves til opfyldelse af formålet.

Datatilsynet fandt det beklageligt, at overvågningen ikke levede op til kravene i persondatalovens § 5, og henstillede til taxaselskabet, at systemet indrettes på en sådan måde, at GPS-overvågningen ikke er konstant, men udelukkende finder sted, når vognmanden er på vagt.

## Sager på eget initiativ

I 2015 er der sket et fald på 3,2 % i antallet af sager på Datatilsynets initiativ (fra 145 i 2013 til 155 i 2014). Det sker efter, at der i flere år har været en stigning i antallet af sådanne egen drift-sager. Ressourcemæssige overvejelser har selvsagt indflydelse på den løbende prioritering af, hvilke sager der kan tages op af egen drift.

## Høringer over lovforslag mv.

I 2015 registrerede Datatilsynet 397 nye høringssager i forbindelse med lovforslag, bekendtgørelser mv. Der er hermed sket et voldsomt fald på 23,5 % i forhold til 2014 (519 i 2014). Faldet kommer i forlængelse af en stigende tendens i antallet af sådanne sager siden persondatalovens ikrafttræden i 2000. I 2014 var antallet af høringssager således på sit hidtil højeste.

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.


# Ny anmeldelses- og tilladelsesordning for offentlige myndigheder ved behandling udelukkende i videnskabeligt eller statistisk øjemed

## Fællesanmeldelser

Datatilsynet indførte medio 2015 en ny og forenklet fremgangsmåde for anmeldelse af behandling af personoplysninger, der i staten og kommunerne udelukkende finder sted i videnskabeligt eller statistisk øjemed.

Anmeldelse til Datatilsynet sker herefter ved, at den dataansvarlige myndighed tilslutter sig en såkaldt fællesanmeldelse, der omfatter alle behandlinger af personoplysninger, som myndigheden foretager udelukkende i videnskabeligt eller statistisk øjemed. Der skal således ikke længere ske anmeldelse af de enkelte undersøgelser/projekter. De statslige myndigheder, der behandler personoplysninger i forbindelse med forskningsbiobanker, skal anmelde dette via en separat fællesanmeldelse, der specifikt vedrører biobanker.

Myndighederne skal føre oversigter over deres igangværende undersøgelser/projekter samt eventuelle databaser/registre, der er omfattet af fællesanmeldelserne. Disse oversigter skal efter anmodning udleveres til Datatilsynet, f.eks. i forbindelse med inspektioner. Myndighederne skal endvidere på Datatilsynets anmodning skriftligt oplyse nærmere om aktiviteter i forbindelse med den anmeldte behandling i øvrigt, herunder f.eks. om eventuelle sikkerhedshændelser.

Som hidtil har myndighederne selv ansvaret for at sikre, at behandlingen af oplysninger sker i overensstemmelse med persondataloven og sikkerhedsbekendtgørelsen.

## Videregivelsestilladelser

En statslig myndighed eller kommune, der tilslutter sig fællesanmeldelsen vedrørende videnskabelige og statistiske undersøgelser, anmoder samtidig automatisk om tilladelse efter persondatalovens § 10, stk. 3, til at videregive personoplysninger omfattet af anmeldelsen til brug for andre undersøgelser udelukkende i statistisk eller videnskabeligt øjemed.

Datatilsynet stiller i forbindelse med disse tilladelser en række vilkår, herunder om at modtageren inden videregivelsen skriftligt skal have bekræftet over for myndigheden, at

oplysningerne alene vil blive anvendt i statistisk eller videnskabeligt øjemed. Myndighederne skal også føre oversigter over foretagne videregivelser; disse oversigter skal efter anmodning udleveres til Datatilsynet.

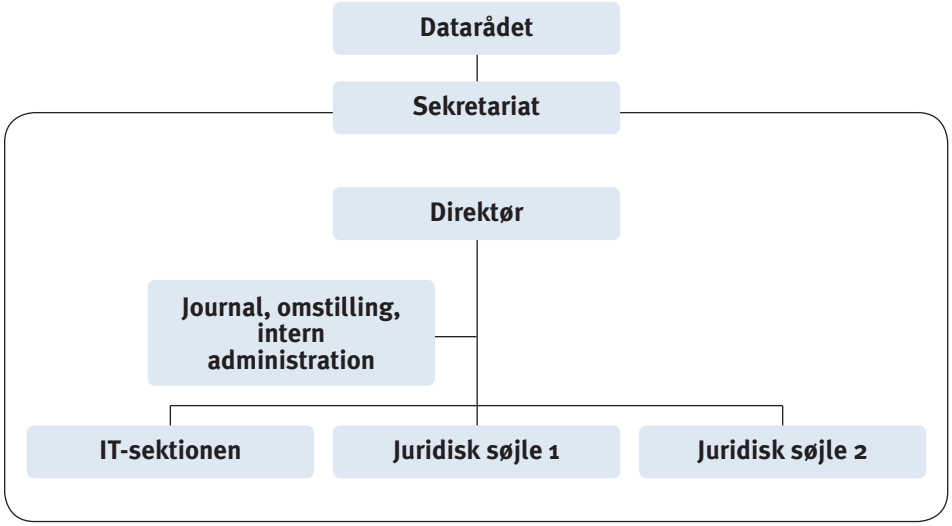
Tilladelserne omfatter ikke videregivelse af personoplysninger til dataansvarlige i udlandet eller videregivelse af biologisk materiale fra biobanker. Sådanne videregivelser kræver således fortsat individuel tilladelse fra Datatilsynet.

I forbindelse med udrulningen af den beskrevne ordning for de statslige myndigheder og kommunerne har Datatilsynet meddelt regionerne tilsvarende generelle tilladelser til at videregive oplysninger omfattet af deres eksisterende paraplyanmeldelser vedrørende sundhedsvidenskabelig forskning samt kliniske kvalitetsdatabaser, der er godkendt af Statens Serum Institut/Sundhedsdatastyrelsen.


## 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 2015)
Formand, højesteretsdommer Henrik Waaben
Næstformand, advokat Janne Glæsel
Professor, dr.jur. Peter Blume
Overlæge, vicedirektør Hans Henrik Storm
Kommunaldirektør Niels Johannesen
Chefkonsulent Henning Mortensen
Direktør Lars Pram

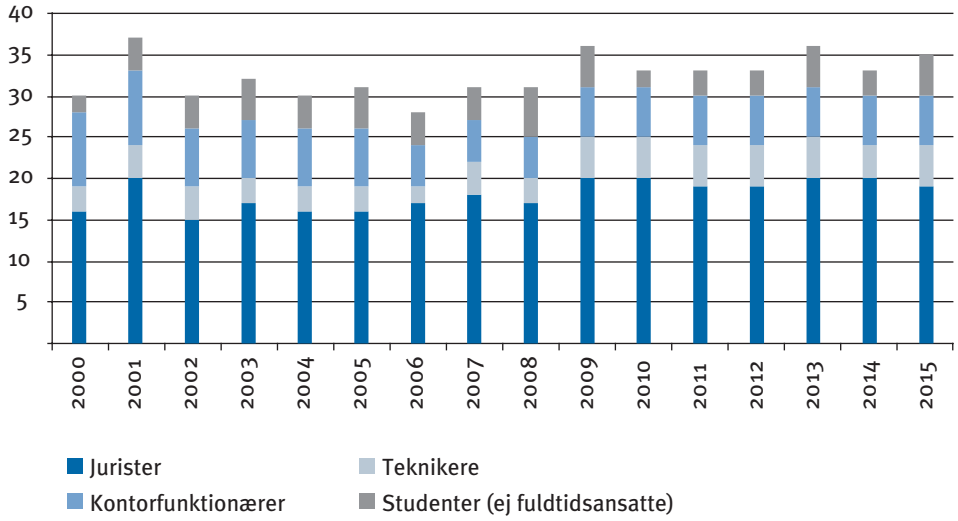
Medlemmerne beskikkes for 4 år ad gangen. De er personligt udpeget i kraft af deres sagkundskab inden for bestemte sagsområder og er ikke repræsentanter for bestemte interesseorganisationer el.lign.

## Sekretariatet

Sekretariatet beskæftiger omkring 35 medarbejdere (jurister, it-teknikere, kontorfunktionærer og studenter) og varetager Datatilsynets daglige drift under ledelse af en direktør. I 2015 fik Datatilsynet ny direktør, idet Janni Christoffersen blev afløst af Cristina Angela Gulisano.

Datatilsynets bevillingsmæssige forhold mv. fremgår af Datatilsynets årsrapport for 2015. Årsrapporten er offentliggjort på tilsynets hjemmeside.

Personalesammensætning




**Datatilsynets medarbejdere** (pr. 31. december 2015)
Direktør, cand.jur. Cristina Angela Gulisano
Kontorchef, cand.jur. Lena Andersen
Kommitteret, cand.jur. Birgit Kleis
It-chef, civilingeniør, HD, Sten Hansen
Chefkonsulent, cand.jur. Maiken Christensen
Chefkonsulent, cand.jur. Lene Engedal Kragelund
Specialkonsulent, cand.jur. Jesper Husmer Vang
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
It-sikkerhedskonsulent, cand.scient.dat. Farshid Shaikhrezai
Kontorfuldmægtig Helle Jensen
Kontorfuldmægtig Pernille Jensen
Kontorfuldmægtig Anne-Marie Müller
Kontorfuldmægtig Suzanne Stenkvist
Kontorfuldmægtig Mette-Maj Aner Leilund
Assistent Camilla Knutsdotter Hallingby
It-medarbejder Flemming Nielsen
It-medarbejder Thomas Klarskov Jensen
Fuldmægtig, cand.jur. Signe Vestergård Abildskov
Fuldmægtig, cand.jur. Bjarke Asger Bro
Fuldmægtig, cand.jur. Signe Astrid Bruun
Fuldmægtig, cand.jur. Søren Klæbel Clemmensen
Fuldmægtig, cand.jur. Kasper Frederiksen
Fuldmægtig, cand.jur. Sissel Michelle Kristensen
Fuldmægtig, cand.jur. Helle Ginnerup-Nielsen
Fuldmægtig, cand.jur. Christian Vinter Hagstrøm
Fuldmægtig, cand.jur. Mette Hansen (orlov)
Fuldmægtig, cand.jur. Hanne Louise Høimark (orlov)
Fuldmægtig, cand.jur. Victoria Maria Ljunggren
Fuldmægtig, cand.jur. Sofie Katrine Mannering
Fuldmægtig, cand.jur. Cathrine Serup Raasdal
Fuldmægtig, cand.jur. Anders Robodo Petersen
Fuldmægtig, cand.jur. Morten Tønning
Stud.jur. Markus Gammelgaard Klokhøj
Stud.jur. Mille Selbach Rasmussen
Stud.jur. Sofie Amalie Friis Sharif
Stud.jur. Jonas Thøger Skjødt
Stud.jur. Kamille Frølund Thomsen

## Statistiske oplysninger

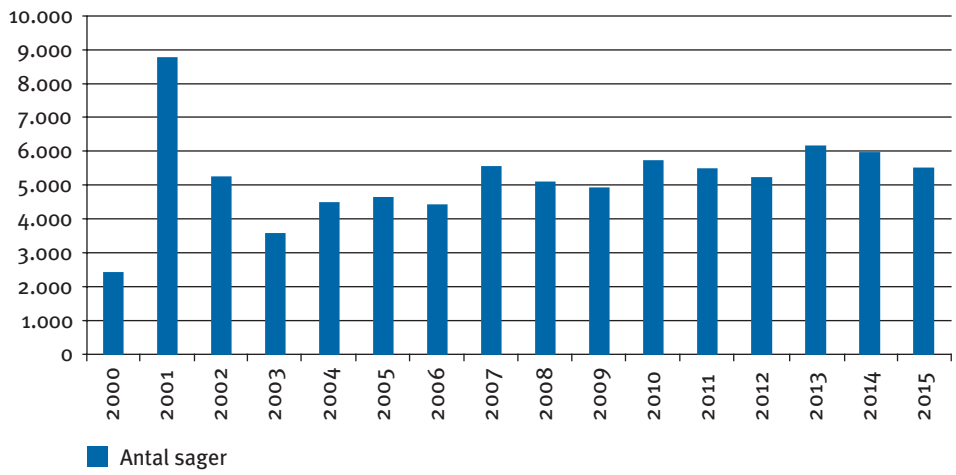
Her er oplysninger om antallet af nye sager i Datatilsynets journalsystem i 2015. Tallene omfatter sager, som er oprettet i løbet af 2015. En del af Datatilsynets sagsbehandling er imidlertid en fortsættelse af eksisterende sager. Dette er for eksempel tilfældet, når en anmeldelse ændres, eller en tilladelse forlænges. Disse sager er af praktiske årsager ikke medtaget i statistikken.

Datatilsynet registrerede 5.461 nye sager i 2015.

**Nyoprettede sager 1. januar 2015 til 31. december 2015:**

| | |
|---|---|
| Datatilsynets egen administration mv. | 300 |
| Lovforberedende arbejde | 397 |
| Forespørgsler og klager vedrørende private | 1.112 |
| Forespørgsler og klager vedrørende offentlige myndigheder | 831 |
| Anmeldelser for den private sektor | 1585 |
| Anmeldelser for den offentlige sektor | 756 |
| Sager på Datatilsynets eget initiativ (egen drift-sager) | 150 |
| Sikkerhedsspørgsmål | 17 |
| Internationale sager | 190 |
| Datatilsynets kompetence efter anden lovgivning | 123 |
| I alt | 5.461 |

Der har været et fald på 7,5 % i det samlede antal nyoprettede sager i 2015 set i forhold til 2014. I 2015 blev der oprettet 5.461 nye sager mod 5.904 i 2014. Faldet er fordelt på forskellige sagsgrupper, herunder sager om lovforberedede arbejde, klager og forespørgsler samt anmeldelsessager.


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

## Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 1.112 nye sager om forespørgsler og klager vedrørende private dataansvarlige.

Sagerne havde følgende fordeling på forskellige virksomhedstyper:

| | |
|---|---|
| Almindelige virksomheder | 81 |
| Den finansielle sektor | 73 |
| Fagforeninger, a-kasser, pensionskasser mv. | 9 |
| Telesektoren | 30 |
| Foreninger og organisationer | 125 |
| Sundhedssektoren (medicinalfirmaer, klinikker, læger mv.) | 40 |
| Kreditoplysningsbureauer | 107 |
| Advarselsregistre | 4 |
| Stillingsbesættende virksomheder | 5 |
| Ansøgninger om tilladelser | 81 |
| Internet, sociale netværk, cloud mv. | 237 |
| Tv-overvågning | 56 |
| Private forskere | 17 |
| Diverse | 244 |
| Sager af generel karakter | 3 |

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2015[1], var:

| | |
|---|---|
| Klager | 5 % |
| Forespørgsler | 78 % |
| Ikke kategoriserede | 19 % |

1 I lighed med Datatilsynets Årsberetning 2014 er disse tal for 2015 ikke opgjort på grundlag af sager, som er oprettet i 2015, men på grundlag af sager, som Datatilsynet har færdigbehandlet i 2015. Heriblandt er sager oprettet i 2015 og 2014 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 831 nye sager om forespørgsler og klager vedrørende offentlige myndigheder.

Sagerne var fordelt således:

| | |
|---|---|
| Statslige myndigheder | 212 |
| Regioner | 60 |
| Kommuner | 277 |
| Ansøgning om tilladelser | 243 |
| Diverse | 39 |

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2015[2], var:

| | |
|---|---|
| Klager | 5 % |
| Forespørgsler | 55 % |
| Ikke kategoriserede | 40 % |

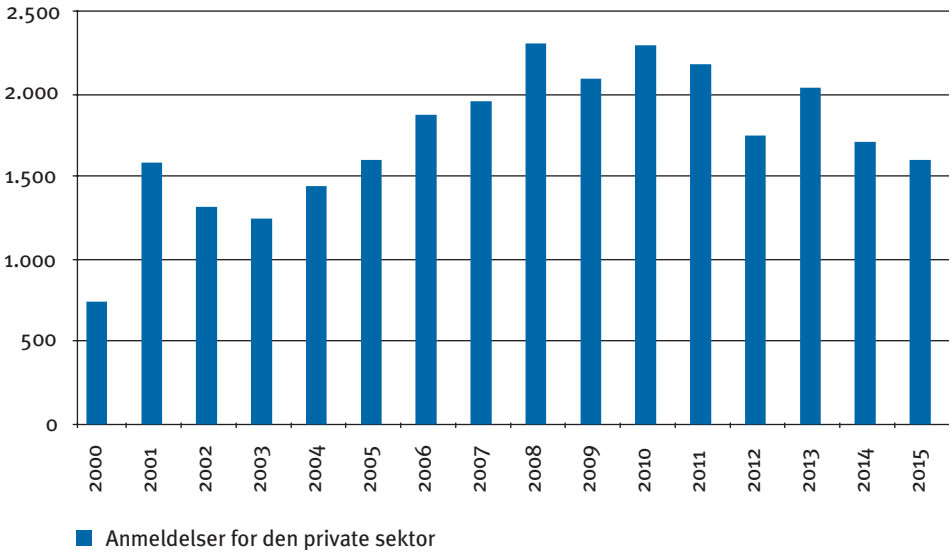
2 Se note 1

## Anmeldelser

### Anmeldelser for den private sektor

Datatilsynet registrerede i alt 1.585 nye sager om anmeldelser for den private sektor. Fordelingen af sagerne var:

| | |
|---|---|
| Forskning og statistik | 858 |
| Privates behandling af oplysninger om rent private forhold | 672 |
| Advarselsregistre | 7 |
| Spærrelister | 4 |
| Kreditoplysningsbureauer | 5 |
| Stillingsbesættende virksomheder | 19 |
| Edb-servicebureauer | 16 |
| Diverse sager af generel karakter | 4 |

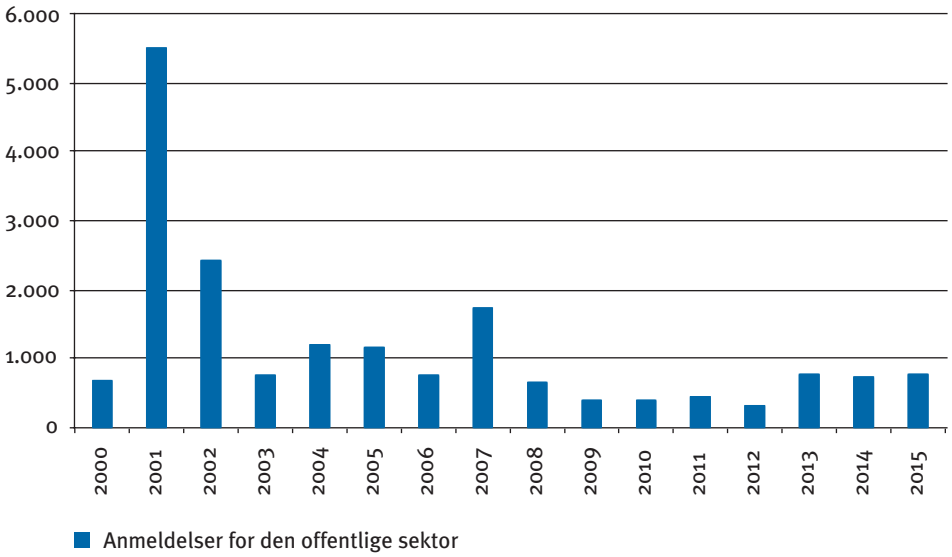



Faldet i antallet af anmeldelser for den private sektor fra 2014 til 2015 skyldes først og fremmest et fald i anmeldelser af forskning og statistik. Her er der sket et fald på 14,1 % fra 999 sager i 2014 til 858 i 2015. Dette fald skyldes sandsynligvis, at meget forskning – som tidligere er blevet betragtet som privat forskning – nu betragtes som offentlig forskning og derfor falder under f.eks. regionernes paraplyanmeldelser af sundhedsvidenskabelig forskning.


## Anmeldelser for den offentlige forvaltning

Datatilsynet registrerede i alt 756 nye sager om anmeldelser for den offentlige sektor. Fordelingen af sagerne var:

| | |
|---|---|
| Fællesanmeldelser | 0 |
| Kommuner | 151 |
| Regioner | 11 |
| Statslige myndigheder | 241 |
| Tilslutninger, kommuner | 209 |
| Tilslutninger, regioner | 0 |
| Tilslutninger, statslige myndigheder | 143 |
| Diverse/sager af generel karakter | 1 |




Antallet af offentlige anmeldelser er i 2015 på niveau med 2013 og 2014, hvor antallet var henholdsvis 755 og 717. Der er sket en voldsom stigning i antallet af statslige myndigheders tilslutninger til fællesanmeldelser. Dette skyldes, at Datatilsynet i 2015 har indført statslige fællesanmeldelser på forskningsområdet, som omfatter alle behandlinger af personoplysninger, som myndigheden udelukkende foretager i videnskabeligt eller statistisk øjemed. Der skal således ikke længere ske anmeldelse af hver enkelt videnskabelig undersøgelse/projekt.

## Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 150 nye sager oprettet på tilsynets eget initiativ. Fordelingen af sagerne var:

| | |
|---|---|
| Inspektion og kontrol vedrørende private | 21 |
| Inspektion og kontrol vedrørende offentlige myndigheder | 26 |
| Sager rejst på grundlag af presseomtale og lign. | 75 |
| Diverse/sager af generel karakter | 2 |
| Online-undersøgelser | 26 |

## Internationale sager

Datatilsynet registrerede i alt 190 nye internationale sager. Fordelingen af sagerne var:

| | |
|---|---|
| Forespørgsler fra udlandet | 86 |
| Nordisk tilsynssamarbejde | 3 |
| Europarådet | 2 |
| EU | 86 |
| Datakommissærsamarbejdet | 5 |
| OECD | 1 |
| Diverse/sager af generel karakter | 7 |


# Kreditoplysning

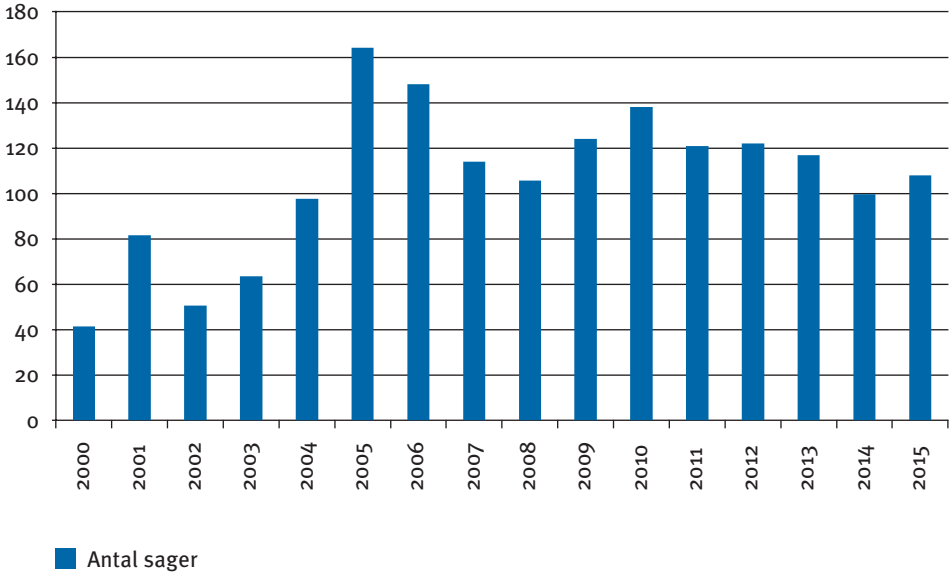
## Klager over registrering

Registrering hos kreditoplysningsbureauer er et område, hvor Datatilsynet modtager en del klager og henvendelser fra såvel private personer som virksomheder.

De fleste sager vedrørende kreditoplysning er henvendelser om indberetninger fra private virksomheder (kreditorer). Offentlige myndigheder kan også indberette til kreditoplysningsbureauer efter særlige regler i persondatalovens kapitel 5, men tilsynet modtager kun meget få henvendelser om dette.

Antallet af henvendelser på kreditoplysningsområdet svinger noget fra år til år. I 2015 har Datatilsynet modtaget 107 henvendelser om kreditoplysning, hvilket næsten er på det samme lave niveau som i 2014.

Klager og forespørgsler vedrørende kreditoplysning



## Ny praksis på kreditoplysningsområdet

Reglerne for kreditoplysningsbureauer er stort set en videreførelse af de regler, der var gældende før persondatalovens ikrafttræden, og Datatilsynet har derfor på dette område en omfattende praksis. Nye problemstillinger dukker dog fortsat op. I 2015 har Datatilsynet derfor også i to tilfælde måttet tage sin tidligere praksis op til revision, og indført en ny praksis, jf. nedenfor.

## Finansielle nøgletal

Datatilsynet har tidligere i forbindelse med flere sager konkluderet, at videregivelse af standardmæssige finansielle nøgletal ikke skal anses for en aktivitet, der kræver iagttagelse af kapitel 6 i persondataloven.

Datatilsynet har herved bl.a. lagt vægt på, at nøgletallene er beregnet efter almindelige anerkendte formler, og at formidlingen af oplysningerne i dag sker ganske anderledes, end da tilsynet (Registertilsynet) i midten af 1990'erne afgjorde lignende sager.

Det vil derfor fremover være tilsynets generelle praksis i forhold til virksomheder, der videregiver standardmæssige finansielle nøgletal (beregnet efter almindelige anerkendte formler), at denne aktivitet ikke anses for omfattet af kapitel 6 i persondataloven om kreditoplysningsbureauer.

Det er endvidere Datatilsynets opfattelse, at en grafisk præsentation samt en eventuel inddeling i overordnede kategorier (f.eks. "meget god", "god", "tilfredsstillende", etc.) ikke bringer videregivelsen af finansielle nøgletal ind under lovens kapitel 6.

Det er i den forbindelse en afgørende forudsætning, at der ved præsentationen anvendes en standardmæssig inddeling af nøgletallene, og at hjemmesiden indeholder en tydelig forklaring på, hvordan tallene inddeles, ligesom en eventuel farveindeksering eller lignende tydeligt skal være forklaret på hjemmesiden.


## Vilkår om kryptering

Datatilsynet har modtaget henvendelser fra kreditoplysningsbureauer om, hvorvidt det er muligt at fremsende registreringsmeddelelser via e-mail.

Der er bl.a. henvist til, at hovedparten af danske virksomheder i dag kan kontaktes via e-mail. Dette er en konsekvens af, at virksomhederne siden november 2013 har været forpligtet til at modtage digital post fra offentlige myndigheder.

Datatilsynet vil – efter at sagen har været behandlet i Datarådet – fremadrettet kunne acceptere, at kreditoplysningsbureauer fremsender oplysninger via internettet uden kryptering, når disse alene vedrører registrering og videregivelse af oplysninger fra offentligt tilgængelige kilder.

Dette forudsætter imidlertid en tilføjelse til det gældende vilkår 10[3] i Datatilsynets tilladelser til kreditoplysningsbureauerne.

Datatilsynet kontaktede derfor samtlige kreditoplysningsbureauer i Danmark med oplysning om, at hvis kreditoplysningsbureauet ønsker det, vil Datatilsynet ændre bureauets tilladelse og indsætte et vilkår 10, stk. 2, med følgende formulering:

> 10. stk. 2.
> "Der gælder dog ikke krav om kryptering, hvis der udelukkende fremsendes oplysninger fra offentligt tilgængelige kilder."

Det er en forudsætning, at bureauet ved eventuel fremsendelse af registreringsmeddelelser via e-mail sikrer sig, at den anvendte e-mailadresse er korrekt f.eks. ved, at der anvendes e-mailadresser fra CVR.

Det er endvidere en forudsætning, at registreringsmeddelelserne fra kreditoplysningsbureauet ikke antager karakter af reklame/spam-mails i konflikt med markedsføringslovens regler[4].

3 De vilkår, som Datatilsynets standardmæssigt meddeler kreditoplysningsbureauerne, omfatter bl.a. følgende vilkår: 10. Fremsendelse af oplysninger over det åbne internet må alene ske i forsvarlig krypteret form

4 Lovbekendtgørelse nr. 58 af 20. januar 2012 med senere ændringer

# It-sikkerhed

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

§ 41, stk. 3, er nærmere udmøntet i den såkaldte sikkerhedsbekendtgørelse – bekendtgørelse nr. 528 af 15. juli 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (med senere ændringer). Datatilsynet har endvidere udarbejdet en vejledning til sikkerhedsbekendtgørelsen – vejledning nr. 37 af 2. april 2001.

De anvisninger, som fremgår af sikkerhedsbekendtgørelsen og sikkerhedsvejledningen, gælder kun for dataansvarlige i den offentlige forvaltning. Datatilsynet har imidlertid i mange konkrete sager vedrørende private dataansvarlige taget udgangspunkt i disse anvisninger.

Et sikkerhedsmæssigt forhold, som har fyldt meget hos Datatilsynet igennem de seneste år, er hackerangrebet mod CSC. I 2015 afgav Datatilsynet udtalelser til myndighederne Rigspolitiet, SKAT, Økonomi- og Indenrigsministeriet (nu Social- og Indenrigsministeriet) og Moderniseringsstyrelsen, som anvendte CSC som databehandler. Sagerne er omtalt nedenfor.

## Hackerangrebet mod CSC

I 2012 blev informationssystemer, som en række danske myndigheder – herunder Rigspolitiet, SKAT, Økonomi- og Indenrigsministeriet (nu Social- og Indenrigsministeriet) og Moderniseringsstyrelsen – fik driftafviklet hos CSC, udsat for et hackerangreb. Informationssystemerne blev driftet på én og samme mainframe hos CSC i Valby.

I forbindelse med politiets efterforskning af sagen viste det sig, at angrebet bl.a. havde omfattet en database (RACF-databasen) indeholdende oplysninger om ca. 85.000 bruger- og administrator-id'er samt oplysninger om de hertil knyttede passwords og autorisationer til at anvende programmer, services og data på hele mainframen. RACF-sikkerhedssy-

stemet kontrollerede brugere og administratorer af systemerne fra de fire ovenfor nævnte myndigheder. En kopi af RACF-databasen blev fundet på hackerens computer.

Det blev endvidere konstateret, at uvedkommende havde haft adgang til Rigspolitiets informationssystemer på den hackede mainframe, herunder oplysninger fra Schengen-informationssystemet.

Efter at være blevet gjort bekendt med hackerangrebet i maj 2013 indledte Datatilsynet en undersøgelse af sagen ved bl.a. at indhente oplysninger fra de berørte myndigheder.

Datatilsynets udtalelser til de fire myndigheder er offentliggjort på tilsynets hjemmeside.

I relation til Rigspolitiet fokuserede Datatilsynet i første række på forholdene omkring Schengen-informationssystemet.

Datatilsynet fandt samlet set, at Rigspolitiet ikke havde truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kunne komme til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Datatilsynet fandt derfor, at Rigspolitiet ikke havde opfyldt persondatalovens § 41, stk. 3.

Datatilsynet fandt endvidere, at Rigspolitiet ikke havde levet op til Schengen-konventionens artikel 118 (1) b), c) og d).

Den manglende efterlevelse af persondatalovens § 41, stk. 3, og Schengen-konventionens artikel 118 (1) b), c) og d) var efter Datatilsynets opfattelse **overordentlig kritisabel**.

Datatilsynet tilkendegav, at tilsynet måtte lægge til grund, at hackeren havde haft ubegrænsede rettigheder på mainframen og mulighed for at tilgå alle data på mainframens delte disksystem.

Det var på den baggrund Datatilsynets umiddelbare vurdering, at tilsynets konklusioner vedrørende Rigspolitiets manglende efterlevelse af persondatalovens § 41, stk. 3, for så vidt angår Schengen-informationssystemet, tilsvarende måtte gøre sig gældende for Rigspolitiets andre informationssystemer, som blev driftet på mainframen, heriblandt Kriminalregisteret, Pasregisteret, Kørekortregisteret og Index-registeret.

Datatilsynet fandt endvidere, at Rigspolitiet ikke i tilstrækkeligt omfang havde underrettet den berørte personkreds om uvedkommendes adgang til persondata.

Rigspolitiet har efterfølgende i et brev til Datatilsynet redegjort for bl.a. de tekniske og processuelle tiltag, som Rigspolitiet havde gennemført siden hackerangrebet, og for overvejelser om fremadrettede tiltag.

For så vidt angår SKAT, Økonomi- og Indenrigsministeriet (nu Social- og Indenrigsministeriet) og Moderniseringsstyrelsen måtte Datatilsynet lægge til grund, at hackeren potentielt havde haft adgang til at ændre i, tilføje eller slette data, som befandt sig i systemer, som på vegne af myndighederne blev håndteret hos CSC.

Efter Datatilsynets opfattelse var der tale om, at personoplysninger, som myndighederne var dataansvarlig for, var kommet til uvedkommendes kendskab, da RACF-databasen var blevet kopieret og downloadet.

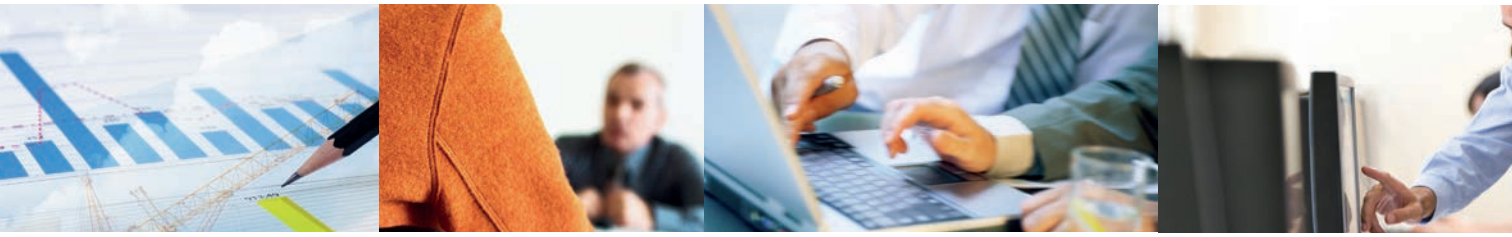
Det forhold, at mainframemiljøet hos CSC var delt mellem flere myndigheder, medvirkede efter Datatilsynets opfattelse til, at en angriber via en webserver, som én myndighed var dataansvarlig for, kunne tilgå både data, som den pågældende myndighed var dataansvarlig for, og data, som andre myndigheder var dataansvarlige for.

Det forhold, at RACF-databasen var delt mellem flere myndigheder, forøgede desuden angriberens mulighed for at skaffe sig adgang til systemer tilhørende én myndighed via uberettiget adgang til andre myndigheders systemer.

Efter Datatilsynets opfattelse havde de enkelte myndigheder derfor ikke haft tilstrækkelig kontrol med sikkerheden omkring de personoplysninger, som på myndighedens vegne blev håndteret hos CSC. Datatilsynet fandt herefter, at myndighederne ikke havde levet op til kravet i persondatalovens § 41, stk. 3, om de fornødne sikkerhedsforanstaltninger.

Datatilsynet fandt det meget alvorligt, at en udenforstående potentielt havde haft mulighed for at tilgå, kopiere, slette og ændre i oplysningerne i systemerne hos CSC, og at personoplysninger i RACF-databasen var blevet kopieret og downloadet.

Datatilsynet fandt derfor den manglende efterlevelse af persondatalovens sikkerhedskrav hos SKAT, Økonomi- og Indenrigsministeriet (nu Social – og Indenrigsministeriet) og Moderniseringsstyrelsen **kritisabel**.



## Medarbejderes adgang til personoplysninger

Datatilsynet har igennem årene flere gange udtalt sig om medarbejderes adgange i it-systemer til borgeres personoplysninger. Bl.a. har Datatilsynet i 2015 udtalt sig om spørgsmålet i nedenstående to sager.

### Adgang til patientoplysninger i fælles elektronisk patientjournal

Datatilsynet gennemførte i 2011 en inspektion på Regionshospitalet Randers. Inspektionen tog udgangspunkt i regionens fælles elektroniske patientjournal – MidtEPJ.

Efterfølgende korresponderede Datatilsynet med Region Midtjylland om brugeradgangen i MidtEPJ til elektroniske patientoplysninger og om opfølgningen på inspektionen.

Efter behandling af sagen i Dataarådet afgav Datatilsynet i 2015 en udtalelse til regionen om MidtEPJ. I sin udtalelse til Region Midtjylland udtalte Datatilsynet kritik af, at regionen i sit elektroniske patientjournalsystem havde valgt, at alle autoriserede personalegrupper, inden for de "roller" de var blevet tildelt, havde adgang til oplysninger om alle patienter på tværs af regionens forskellige behandlingsenheder. En sådan indretning af EPJ-systemet var efter Datatilsynets opfattelse kritisabel og ikke i overensstemmelse med persondatalovens regler om saglighed, proportionalitet og behandlingssikkerhed, jf. § 5 og § 41, ligesom kravene i sikkerhedsbekendtgørelsens § 11, stk. 2, ikke kunne anses for opfyldt. Efter de oplysninger, som Datatilsynet havde kunnet få fra regionen, var det således tilsynets vurdering, at i hvert fald nogle autoriserede personalegrupper havde adgang til oplysninger, som de måtte antages ikke at have behov for i deres opgaveløsning.

Datatilsynet udtalte endvidere kritik af, at regionen ikke havde kunnet redegøre for baggrunden for, at der i systemet var oprettet en række brugerroller for ikke-sundhedspersoner – eksempelvis kapelbetjent, piccoline og musikterapeut – som havde systemteknisk adgang til funktioner som f.eks. "epikriselæser" og "e-journal".

Regionen blev også anmodet om at bekræfte, at der nu etableredes halvårlige kontroller af udstedte autorisationer – et forhold Datatilsynet tidligere havde påtalt – og at regionen havde foretaget sletning af brugere, der ikke længere var ansat i regionen.

Datatilsynet vurderede det samtidig som tvivlsomt, om EPJ-systemet levede op til reglerne i sundhedslovens § 42 a, stk. 2, og stk. 11, og orienterede derfor Ministeriet for Sundhed og Forebyggelse (nu Sundheds- og Ældreministeriet) om sagen.

Tilsynet anmodede i den forbindelse også ministeriet om en udtalelse om, hvorvidt den ordning, regionen havde, var i overensstemmelse med sundhedslovens § 42 a, stk. 1.

Regionen fremkom efterfølgende på Datatilsynets anmodning med tilbagemeldinger på tilsynets kritik.

Ministeriet oplyste over for Datatilsynet, at det på baggrund af oplysningerne i Datatilsynets breve til ministeriet og til Region Midtjylland var ministeriets umiddelbare vurdering, at sikkerhedsmodellen i MidtEPJ ikke var i overensstemmelse med sundhedslovens § 42 a. Det fremgik endvidere af ministeriets brev, at ministeriet havde anmodet Danske Regioner om at redegøre for sikkerhedsmodellerne i alle fem regioners EPJ-løsninger, herunder også MidtEPJ. Ministeriet ville på baggrund af redegørelsen afgive et endeligt svar i sagen.

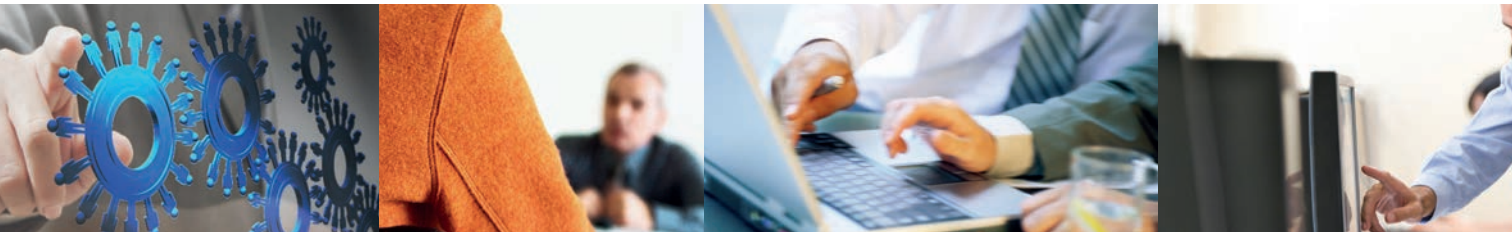
Sagen var endnu ikke afsluttet ved udløbet af 2015.

## Terminaladgang til følsomme personoplysninger i fagforeningssager

Efter lokal medieomtale og efter henvendelser fra en række borgere blev Datatilsynet i 2011 opmærksom på, at 3F Fælles Fagligt Forbund muligvis behandlede personoplysninger i strid med persondataloven.

3F afgav i sagen en række udtalelser, hvoraf det fremgik, at a-kassens medarbejdere hos 3F havde haft en fuld terminaladgang til fagforeningens sager. Terminaladgangen omfattede bl.a. arbejdsskadesager, hvilket indebar, at a-kassens medarbejdere havde adgang til bl.a. følsomme oplysninger fra fagforeningssager. Imens sagen var under behandling hos Datatilsynet, blev terminaladgangen for a-kassens medarbejdere hos 3F bragt til ophør ved en systemændring hos 3F.

Datatilsynet fandt, at den generelle adgang for a-kassens medarbejdere til at se dokumenter i fagforeningssager var meget vidtgående og vanskelig at forene med grundprincipperne i persondatalovens § 5 og de generelle krav om datasikkerhed i lovens § 41, stk.



3. Tilsynet lagde vægt på, at a-kassens medarbejdere havde haft adgang til følsomme oplysninger i arbejdsskadesager uden, at 3F kunne give en fyldestgørende begrundelse herfor og uden hjemmel for adgangen.

Datatilsynet konkluderede på den baggrund, at følsomme oplysninger havde været håndteret i en løsning, der ikke levede op til persondataloven, hvilket tilsynet fandt **kritisabelt**.

## Offentlige myndigheders kommunikation med borgerne via sms og e-mail

Datatilsynet behandlede i 2010 spørgsmålet om offentlige myndigheders brug af sms og e-mail til kommunikation med borgerne. Dengang fastsatte tilsynet retningslinjer, der indebar en vis fravigelse af de sikkerhedskrav, som følger af tilsynets generelle sikkerhedsvejledning. Retningslinjerne skulle gælde for 5 år.

I 2015 tog Datatilsynet sagen op igen med henblik på at vurdere, om retningslinjerne skulle videreføres. Datatilsynet indhentede i den forbindelse udtalelser fra Digitaliseringsstyrelsen, KL og Danske Regioner. Sagen blev drøftet i Datarådet. Tilsynet besluttede herefter at videreføre muligheden for at sende aftalepåmindelser og andre servicebeskeder, som kan indeholde fortrolige og/eller følsomme personoplysninger, via sms og e-mail. Samtidig opdaterede tilsynet sine retningslinjer. Med retningslinjerne forsøger Datatilsynet fortsat at finde en fornuftig balance mellem på den ene side behovet for at anvende sms til god service og effektiv borgerkontakt og på den anden side behovet for at beskytte personoplysninger mod misbrug, tab og uvedkommendes adgang. Den væsentligste ændring i de nye retningslinjer er, at Datatilsynet anbefaler, at offentlige myndigheder benytter sig af NemSMS-løsningen.

De nye retningslinjer skal som udgangspunkt gælde frem til, at databeskyttelsesforordningen finder anvendelse.

Retningslinjerne kan findes på Datatilsynets hjemmeside.

## It-sikkerhedstekster

Datatilsynet finder det fortsat relevant at publicere særlige it-sikkerhedstekster. Teksterne behandler problemstillinger, som tilsynet får kendskab til fra sit daglige virke gennem inspektioner, henvendelser og sikkerhedsbrister. Den stadig hurtigere udvikling inden for it og de mange sager om sikkerhedsbrister, som tilsynet behandler, har vist et behov for konkrete og aktuelle anbefalinger angående it-sikkerhedsemner. Visse offentlige myndigheder og private virksomheder har også valgt at henvise til teksterne fra deres egen hjemmeside, og fra flere sider er der ytret ønske om, at Datatilsynet fortsætter med at publicere sådanne tekster. I 2015 er der publiceret fem nye it-sikkerhedstekster.


# Nyt retsgrundlag på vej

I januar 2012 offentliggjorde EU- Kommissionen sit udspil til nye regler om beskyttelse af personoplysninger i EU – også kaldet databeskyttelsespakken. Pakken består af en generel forordning om beskyttelse af personoplysninger, som skal gælde horisontalt i både den private og offentlige sektor (databeskyttelsesforordningen), samt et direktiv om beskyttelse af personoplysninger, som skal gælde for retshåndhævelsesområdet (databeskyttelses-direktivet). Forordningen skal erstatte databeskyttelsesdirektivet fra 1995, mens direktivet skal erstatte en rammeafgørelse fra 2008.

Datatilsynet har siden 2012 og også i 2015 bidraget til forhandlingerne med databeskyttelsespakken i form af høringssvar på udkast til bestemmelserne i forordningen. I december 2015 blev der opnået enighed om pakken i de såkaldte trilogforhandlinger – mellem EU-Kommissionen, EU-Parlamentet og Ministerrådet. Pakken er formelt vedtaget den 14. april 2016 og får virkning fra den 25. maj 2018.

Forordningen vil få stor betydning for Datatilsynets fremtidige arbejde. 2016 og de kommende år vil derfor i meget vidt omfang komme til at stå i forordningens tegn, og Datatilsynet vil sætte betydelige ressourcer ind på at opnå et tilbundsgående kendskab til det nye retsgrundlag og på at forberede overgangen til dette såvel nationalt som internationalt.

## Forordningens elementer

Forordningen bygger helt grundlæggende på samme systematik som databeskyttelsesdirektivet fra 1995 og persondataloven.

Forordningens kapitel 1 handler om, hvilke behandlinger af personoplysninger forordningen omfatter. Behandling af personoplysninger på internettet om EU-borgere vil i højere grad end i dag være omfattet af forordningens regler. Dette gælder også, selv om den ansvarlige for behandlingen ('den dataansvarlige') eller en anden, der behandler oplysningerne på vegne af den ansvarlige ('databehandleren'), ikke er etableret inden for EU's grænser.

Ligesom i dag er der ifølge forordningens kapitel 2 visse grundlæggende principper, som altid skal iagttages, når personoplysninger behandles, samtidig med, at behandling kun

må finde sted under visse betingelser. Der vil også fremadrettet blive sondret mellem almindelige personoplysninger og følsomme personoplysninger. Helt overordnet svarer forordningens behandlingsregler i vidt omfang til reglerne i det gældende direktiv. Efter forordningen vil man således fortsat kunne behandle relevante personoplysninger til saglige formål bl.a. på baggrund af et udtrykkeligt samtykke fra den person, oplysningerne vedrører ('den registrerede'), eller når det er nødvendigt at behandle oplysningerne med henblik på myndighedsudøvelse.

Forordningens kapitel 3 viderefører og præciserer en række allerede gældende rettigheder for de registrerede personer. Der vil således også fremover bl.a. være en pligt for den dataansvarlige til at oplyse den registrerede om, at der behandles oplysninger om den pågældende, samt en ret for den registrerede til at få indsigt i oplysninger om sig selv, til at få slettet eller berigtiget urigtige oplysninger og til at gøre indsigelse mod, at oplysninger behandles.

Kapitel 4 indeholder bl.a. bestemmelser om den dataansvarliges og databehandlerens generelle forpligtelser og regler om, at der skal være passende sikkerhedsforanstaltninger bl.a. mod, at uvedkommende får adgang til personoplysninger. Kapitel 4, der indholdsmæssigt i vidt omfang er en videreførelse og præcisering af gældende regler, bygger som noget nyt udtrykkeligt på en såkaldt risikobaseret tilgang. Det betyder, at graden af risikoen for den registreredes grundlæggende rettigheder, herunder retten til privatliv, er bestemmende for, hvilke sikkerhedsforanstaltninger en given behandling kræver. Som en konsekvens af denne tilgang vil der i visse tilfælde være krav om, at der forud for en behandling af personoplysninger skal udarbejdes en konsekvensanalyse, som skal kortlægge risiciene for de registrerede. Viser en konsekvensanalyse, at der vil være en høj risiko for den registrerede, skal tilsynsmyndigheden høres, inden behandlingen iværksættes.

Herudover findes der i kapitel 4 regler om, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger designet til at understøtte databeskyttelse ("data protection by design and by default").

Yderligere er der nye krav i kapitel 4 om, at dataansvarlige offentlige myndigheder og visse private virksomheder skal udpege en såkaldt databeskyttelsesrådgiver, som bl.a. skal rådgive den dataansvarlige og databehandleren om behandlingen af personoplysninger. Endelig er der i kapitel 4 et krav om, at dataansvarlige anmelder brud på datasikkerheden til tilsynsmyndigheden, ligesom de registrerede i visse tilfælde skal underrettes herom.


Forordningens kapitel 5 indeholder regler om, hvornår personoplysninger kan overføres til tredjelande. Disse regler bygger i vid udstrækning på reglerne i det gældende direktiv.

Forordningens kapitel 6 og 7 indeholder regler om oprettelse af tilsynsmyndigheder og tilsynsmyndighedernes indbyrdes samarbejde. Forordningen indeholder en væsentlig udbygning af tilsynsmyndighedernes europæiske samarbejde. Der oprettes bl.a. et Europæisk Databeskyttelsesråd, som sammensættes af repræsentanter fra medlemsstaternes tilsynsmyndigheder, og som i visse sager kan træffe afgørelser, som er bindende for de nationale tilsynsmyndigheder.

Kapitel 8 indeholder regler om retsmidler, ansvar og sanktioner. Som noget nyt indeholder forordningen bestemmelser om, at tilsynsmyndighederne kan udstede administrative bøder på op til 20.000.000 euro eller 4 pct. af årlig global omsætning, hvis forordningens bestemmelser overtrædes. En ordning med *administrative* bøder giver anledning til grundlovsmæssige betænkeligheder for Danmark. Der er på den baggrund i forordningen tilføjet en bestemmelse, som giver mulighed for at implementere bestemmelserne om administrative bøder i det nationale *strafferetlige system*.

Forordningens kapitel 9 indeholder bestemmelser om specifikke databehandlingssituationer. Det gælder bl.a. behandling af personnumre og behandling af personoplysninger i forbindelse med videnskabelig forskning og statistikudarbejdelse.

Forordningen giver endvidere medlemsstaterne et råderum for at fastsætte nationale særregler om behandling af personoplysninger. Det er nødvendigt at analysere og vurdere råderummet til brug for overvejelser om, i hvilket omfang der kan fastsættes danske særregler.

# 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 2015 været afholdt fire møder, hvor man bl.a. har drøftet Europols mulighed for etablering af en "European Most Wanted List". Endvidere har Den Fælles Kontrolinstans fulgt udviklingen i arbejdet med Europa-Kommissionens forslag til et nyt retsgrundlag for Europol, og kontrolinstansen har i den forbindelse drøftet sin rolle i perioden frem til det nye retsgrundlags ikrafttræden. Den Fælles Kontrolinstans har endvidere udarbejdet en rapport om behandling af ofres personoplysninger i forbindelse med menneskehandel. Rapporten er tilgængelig hos Den Fælles Kontrolinstans via link fra Datatilsynets hjemmeside under punktet Internationalt → Europol. Endelig har kontrolinstansen drøftet Europols muligheder for udveksling af oplysninger med private samt resultaterne af kontrolinstansens årlige inspektion af Europol.

Det Fælles Klageudvalg har i 2015 afholdt to møder, hvor udvalget har drøftet behandlingen af én klage til udvalget.

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


## Schengen-informationssystemet

Datatilsynet deltager i Koordinationsgruppen for tilsynet med anden generation af Schengen-informationssystemet (SIS II SCG).

I 2015 har der været afholdt to møder i koordinationsgruppen, hvor man bl.a. har udarbejdet en opdateret guide til registrerede om ret til indsigt, som findes via link fra Datatilsynets hjemmeside under punktet Internationalt → Schengen-samarbejdet. Endvidere har gruppen drøftet, hvornår oplysninger om stjålne køretøjer skal slettes fra SIS II. Repræsentanter fra Europa-Kommissionen og eu-LISA[5] har endvidere deltaget på møderne med henblik på at drøfte aktuelle databeskyttelsesretlige spørgsmål og holde gruppen underrettet om den aktuelle situation for SIS II. Endelig har Datatilsynet orienteret gruppen om tilsynets afsluttende udtalelse vedrørende hackerangrebet mod CSC.

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

## Told-informationssystemet

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

I Den Fælles Tilsynsmyndighed for Told-informationssystemet har der i 2015 været afholdt to møder, hvor man bl.a. har udarbejdet spørgerskemaer til medlemsstaterne til brug for undersøgelse af anvendelsen af Told-informationssystemet.

I Koordinationsgruppen for tilsynet med Told-informationssystemet har der i 2015 været afholdt to møder, hvor man bl.a. har udarbejdet en vejledning om registreredes rettigheder. Repræsentanter fra Europa-Kommissionen og OLAF[6] har endvidere deltaget på møderne med henblik på at drøfte aktuelle databeskyttelsesretlige spørgsmål. Endelig har gruppen drøftet spørgeskema og evt. udarbejdelse af en fælles plan for inspektioner af AFIS-systemet[7].

5 Den Europæiske Unions agentur for store it-systemer
6 European Anti Fraud Office
7 Anti-fraud Information System

## Eurodac

Som led i tilsynet med Eurodac deltager Datatilsynet i Koordinationsgruppen for tilsynet med Eurodac (Eurodac SCG).

I 2015 har der været afholdt to møder, hvor man bl.a. har drøftet en undersøgelse af Eurodacs anvendelse af den nye Eurodac-forordning[8]. Endvidere har gruppen via spørgeskema indsamlet information om de enkelte medlemsstaters anvendelse af den nye Eurodac-forordning. Repræsentanter fra Europa-Kommissionen og eu-LISA[9] har endvidere deltaget på møderne med henblik på at drøfte aktuelle databeskyttelsesretlige spørgsmål og holde gruppen underrettet om den aktuelle situation for Eurodac-systemet.

## Visum-informationssystemet

Som led i tilsynet med behandling af personoplysninger i Visum-informationssystemet (VIS) deltager Datatilsynet i Koordinationsgruppen for tilsynet med Visum-informationssystemet (VIS SCG).

I 2015 har der været afholdt to møder, hvor gruppen bl.a. haft besøg af repræsentanter fra Europa-Kommissionen og eu-LISA[10], som har holdt gruppen underrettet om udrulningen af og situationen omkring Visum-informationssystemet. Gruppen har endvidere fortsat undersøgelsen fra 2014 om databehandleres adgange til Visum-informationssystemet. Endelig har gruppen påbegyndt et arbejde omkring udarbejdelse af en rapport om den registreredes ret til indsigt i Visum-informationssystemet.

8 Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 af 26. juni 2013 om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet i en af medlemsstaterne af en tredjelandsstatsborger eller en statsløs og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse og ændring af forordning (EU) nr. 1077/2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store it-systemer inden for området med frihed, sikkerhed og retfærdighed

9 Se note 1

10 Se note 1


## Artikel 29-gruppen

Artikel 29-gruppen er nedsat i henhold til artikel 29 i det generelle databeskyttelsesdirektiv[11]. Gruppen er uafhængig og rådgiver Europa-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 2015 afholdt 6 møder i Bruxelles.

EU-Domstolen afgjorde den 6. oktober 2015, at den såkaldte Safe Harbor-ordning er ugyldig, hvilket betyder at overførsel af personoplysninger til USA på baggrund af ordningen er i strid med EU-retten. Dommen har givet anledning til mange spørgsmål vedrørende overførsel af personoplysninger til USA. Derfor er spørgsmålet også prioriteret højt i Artikel 29-gruppen. Dommen har bl.a. betydet, at Artikel 29-gruppen har igangsat et analysearbejde med henblik på at vurdere, hvilke konsekvenser dommen kan have for andre overførselsgrundlag i forhold til USA. Herudover har Artikel 29-gruppen fastslået, at hvis der ikke er fundet en passende løsning med de amerikanske myndigheder ved udgangen af januar måned 2016 - afhængigt af udfaldet af de fortsatte analyser af de øvrige overførselsgrundlag - vil de europæiske datatilsyn være parate til at træffe alle nødvendige og passende foranstaltninger, hvilket også vil kunne omfatte fælles koordinerede håndhævelsesaktioner.

I 2015 har Artikel 29-gruppen desuden vedtaget en række henstillinger, udtalelser mv. Således har gruppen bl.a. afgivet udtalelser om problemstillinger vedrørende brug af droner og om forslaget til direktiv om beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, opdage eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger.

Alle Artikel 29-grupens dokumenter er tilgængelige på Europa-Kommissionens hjemmeside. Der er link til disse dokumenter på Datatilsynets hjemmeside under punktet Internationalt → Artikel 29-gruppen.

11 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

## Indre Markeds Informationssystem

Datatilsynet deltager i Koordinationsgruppen for tilsynet med det Indre Markeds Informationssystem (IMI SCG).

Der har ikke været afholdt møder i gruppen i 2015.

## Eurojust

Eurojust er et EU-organ, som blev oprettet i 2002 for at forbedre 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[12], og som kollektivt overvåger Eurojusts 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 2015 været afholdt ét møde i den fælles kontrolinstans.

## Europarådet

Arbejdsgruppen for databeskyttelse (T-PD) har fortsat sit arbejde i 2015. Gruppen har bl.a. arbejdet med behandling af helbredsoplysninger. Det er Justitsministeriet, der møder i T-PD.

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


## Berlin-gruppen

International Working Group on Data Protection in Telecommunications, også kaldet Berlin-gruppen, har i 2015 afholdt to møder. I april mødtes gruppen i Seoul efter invitation fra det sydkoreanske datatilsyn, og i oktober mødtes gruppen i Berlin.

Berlin-gruppen fokuserer på nye informationsteknologier og tendenser med henblik på at afdække implikationer for databeskyttelse og privatliv samt at give anbefalinger til interessenter. Gruppens arbejde afspejles i rækken af publicerede udtalelser, såkaldte Working Papers, som er tilgængelige på Berlin-gruppens hjemmeside.

Efter mødet i april offentliggjorde Berlin-gruppen to nye udtalelser, den ene om transparent rapportering til offentligheden vedrørende staters tilgang til persondata, som er i virksomheders besiddelse, og den anden om privatlivs- og datasikkerhedsrisici ved anvendelse af såkaldte Wearable Computing Devices, som f.eks. håndholdte terminaler, smart clothing (tøj), smart glasses (briller), smart watches (ure), kropskameraer, biosensor-plastre, aktivitetsmonitorer og søvnsensorer.

I december 2015 offentliggjorde Berlin-gruppen yderligere to udtalelser om henholdsvis sporing af mobile enheders lokalitet (sted) og intelligent videoovervågning med ansigtsgenkendelse, sporing og overvågning af f.eks. kunder i butiksmiljøer og passagerer i lufthavne.

I årets løb har Berlin-gruppen endvidere arbejdet med emnerne: VoIP (samtale via internettet), Do Not Track standarden for internettet, sociale netværk og Smart TV, som alle indeholder problemstillinger med hensyn til databeskyttelse og beskyttelse af privatliv.

## Den internationale konference

Hvert år afholdes der en international konference for databeskyttelseskommissærer med deltagere fra hele verden.

Konferencen indeholder en åben del, som også andre end datatilsynsmyndighederne kan deltage i.

Herudover har konferencen et møde kun for datatilsynsmyndighederne, hvor databeskyttelseskommissærerne bl.a. vedtager resolutioner vedrørende aktuelle problemstillinger inden for databeskyttelse og beskyttelse af privatlivet.

I 2015 vedtog den internationale konference en række resolutioner, som kan findes på Datatilsynets hjemmeside under punktet Internationalt → Konferencer.

Datatilsynet var repræsenteret på årets konference, som blev afholdt i Amsterdam.

## Nordisk samarbejde

I 2015 afholdt de nordiske datatilsynsmyndigheder i Norge, Sverige, Finland, Åland, Island, Færøerne og Danmark for fjerde gang et stort fælles møde for både chefer, sagsbehandlere og it-teknikere. Mødet foregik i Helsinki.

Mødet blev indledt med fælles sessioner om det forgangne år i tilsynene og om problematikken omkring Googles behandling af personoplysninger i forbindelse med søgemaskinen.

Derudover blev der afholdt separate sessioner for henholdsvis cheferne, sagsbehandlerne og it-teknikerne. På chefmødet talte man bl.a. om forberedelserne til den kommende EU-regulering på databeskyttelsesområdet. Sagsbehandlerne talte bl.a. om fælles nordiske inspektioner og det geografiske anvendelsesområde for de nationale databeskyttelseslovgivninger. På teknikermødet blev det nyeste udkast til forordningen gennemgået med henblik på at vurdere udfordringer og mulige fremtidige opgaver for it-teknikere i de nordiske datatilsyn. Resultatet af dette blev præsenteret og diskuteret på det afsluttende fællesmøde.


# Datatilsynets inspektioner

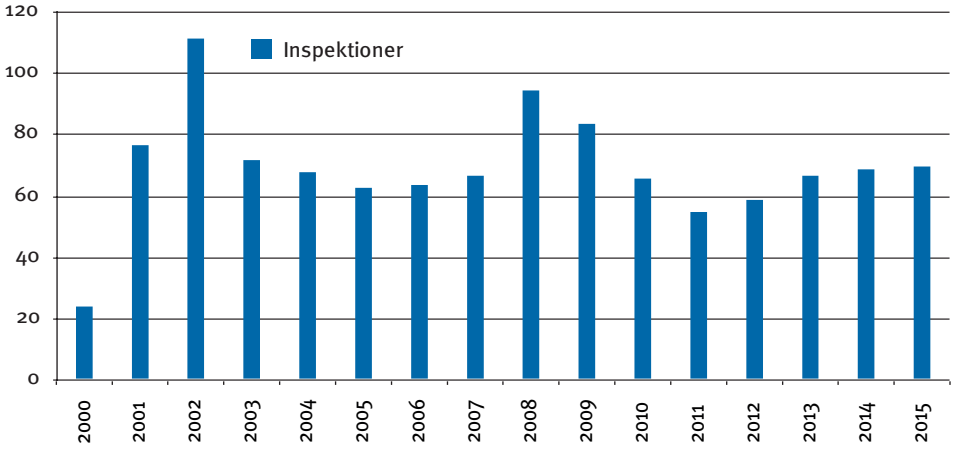
## Inspektioner i 2015

I 2015 foretog Datatilsynet 69 inspektioner, herunder 37 skriftlige kontroller. Disse inspektioner var fordelt på offentlige myndigheder, private virksomheder, private forskere mv. Nogle af inspektionerne blev afholdt over flere dage. 10 inspektioner blev gennemført som et raid inden for samme geografiske område (Nordjylland).

27 af Datatilsynets inspektioner blev gennemført i form af online-undersøgelser af private forskeres behandling af personoplysninger. I online-undersøgelserne udsender Datatilsynet elektronisk et spørgeskema via et særligt spørgeskemasystem. Spørgsmålene relaterer sig til de vilkår, som Datatilsynet har stillet i sin tilladelse til den dataansvarliges forskningsprojekt.

Herudover blev 10 inspektioner på området for behandling af personoplysninger i forbindelse med spærrelister gennemført i form af skriftlige kontroller.

Antallet af inspektioner er steget år for år siden 2011, hvor tilsynet udførte 54 inspektioner.




Det primære formål med Datatilsynets inspektioner er at foretage konkret kontrol hos de inspicerede virksomheder og myndigheder og om nødvendigt at sikre en bedre overholdelse af loven hos virksomheden eller myndigheden.


**Datatilsynets inspektionskompetence**

Datatilsynet har inspektionsadgang hos den offentlige forvaltning, dvs. hos de statslige, kommunale og regionale myndigheder.

I den private sektor gælder inspektionsadgangen 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.

Datatilsynets inspektionskompetence fremgår af persondatalovens § 62, stk. 2-4.

## Inspektioner hos politikredse

Datatilsynet foretog i 2015 inspektioner hos Bornholms Politi og Københavns Politi. Fokus for disse inspektioner var særligt politikredsenes iagttagelse af sikkerhedsbekendtgørelsens regler, herunder logning, autorisationer og adgangskontrol.

Inspektionerne var de sidste i en række af inspektioner i samtlige politikredse, som er foretaget over en årrække. Udover de individuelle tilbagemeldinger til kredsene vil Datatilsynet foretage en evaluering af samtlige inspektioner, bl.a. for at identificere problemstillinger, der med fordel kan løses centralt.

## Inspektion af Politiets Efterforskningsstøtte Database (PED)

Datatilsynet foretog i foråret 2015 en inspektion hos Rigspolitiet af PED. Inspektionen tog udgangspunkt i PED-bekendtgørelsen[11] og omfattede bl.a. Rigspolitiets konkrete implementering heraf. Inspektionen omfattede endvidere spørgsmål vedrørende organisering, procedurer og kontrol i forbindelse med behandlinger af personoplysninger i PED.

11 Bekendtgørelse nr. 921 af 2. juli 2010 om behandling af personoplysninger i Politiets Efterforskningsstøtte Database (PED)


## Afslutning af forskningsinspektioner i regionerne

Som led i Datatilsynets inspektionsvirksomhed inspicerede tilsynet i løbet af 2014 alle fem regioner. Inspektionerne tog udgangspunkt i tilfældigt udvalgte forskningsprojekter omfattet af regionernes paraplyanmeldelse af sundhedsvidenskabelig forskning og havde bl.a. fokus på regionernes rolle som dataansvarlig for behandlingen af personoplysninger i forbindelse med forskning i regionen.

Datatilsynet afgav i 2015 sine bemærkninger til inspektionerne og udtalte i den forbindelse varierende grader af kritik til fire regioner.

Datatilsynet konstaterede, at to regioner ikke levede op til persondatalovens krav om databehandleraftaler, og at én region ikke foretog fornøden logning efter sikkerhedsbekendtgørelsens § 19 og ikke var opmærksom på persondatalovens regler om overførsel af oplysninger til tredjelande. Endvidere levede én regions sletterutiner ikke op til persondatalovens krav, og én region levede ikke op til sikkerhedsbekendtgørelsens krav om kontrol af afviste adgangsforsøg. Endelig levede én region ikke op til sikkerhedsbekendtgørelsens krav om halvårlig kontrol af autorisationer og opfølgning på afviste adgangsforsøg.

Herudover fik fire af regionerne bemærkninger vedrørende manglende opdatering af anmeldelsen, f.eks. om anvendelse af databehandlere og overførsel af oplysninger til tredjelande.

Endvidere havde Datatilsynet under inspektionerne bemærkninger til regionernes interne godkendelser af sundhedsvidenskabelige forskningsprojekter.

## It-sikkerhedsinspektioner

I andet halvår af 2015 blev der afholdt to it-sikkerhedsinspektioner, som havde til formål at undersøge efterlevelsen af logningskrav i forbindelse med statistikproduktion og analyser hos en offentlig myndighed på sundhedsområdet (Statens Serum Institut) samt en kommune (Frederiksberg). Inspektionerne var ikke afsluttet ved udgangen af 2015.


## Oversigt over udførte inspektioner i 2015

**Staten:**
Bornholms Politi
Justitsministeriets departement
Københavns Politi
Rigspolitiet (Politiets Efterforskningsstøtte Database – PED)
Statens Administration
Statens Institut for Folkesundhed (forskning)
Statens Serum Institut (Dødsårsagsregistret)
Statens Serum Institut (it-sikkerhed)
Styrelsen for Arbejdsmarked og Rekruttering
Syddansk Universitet, Det Danske Tvillingeregister (forskning)
Økonomi- og Indenrigsministeriets departement

**Kommuner:**
Aalborg Kommune
Bornholms Regionskommune
Brønderslev Kommune
Fakse Kommune
Frederiksberg Kommune (it-sikkerhed)
Frederikshavn Kommune
Hjørring Kommune
Jammerbugt Kommune
Lejre Kommune
Stevns Kommune
Vordingborg Kommune

**Tv-overvågning:**
Grundejerforeningen Nørklit
Hasseris Boligselskab, Grønnegården
Lejerbo Aalborg, Skalleruppparken
Nordjyllands Politi
Region Nordjylland, Aalborg Universitetshospital
Tech College Aalborg


**Kreditoplysning:**
Experian A/S

**Spærrelister (skriftlig kontrol):**
Flemløse Sparekasse
Forbrugsforeningen af 1886
Klim Sparekasse
Kuwait Petroleum (Danmark) A/S
Lyngby Storcenter Konto a.m.b.a.
Nykredit Bank A/S
Rejsekort A/S
Rødovre Centrum Konto A.m.b.A
TDC A/S
Uno-X

**Privat forskning og statistik:**
Morten Hylander Møller
Anne Fogh Hansen

**Øvrige private:**
Scandinavian Airlines System Denmark – Norway – Sweden


**Online-undersøgelser (privat forskning og statistik):**
Niels Holmark Andersen
Henning Rud Andersen
Vibeke Backer
Kim Brixen
Peer Christiansen
Emilie Palmgren Colov
Bent Deleuran
Asger Dirksen
Finn Edler von Eyben
Søren Fanø
Ulla Feldt-Rasmussen
Lotte Holm
Jørgen Skov Jensen
Anni Nørgaard Jeppesen
Lene Hagelskjær Kristensen
Thomas Kromann Lund
Tina Nørgaard Munch
Daniel Vega Møller
Niels Vidiendal Olsen
Lars Pedersen
Anne Peutzfeldt
Hanne Rasmussen
Ole Rasmussen
Lene Seibæk
Anne Tybjærg-Hansen
Barbara Unger
René H. Worck

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

ISSN nr: 1601-5657
ISBN nr: 978-87-999222-0-8