Retsudvalget 2017-18
REU Alm.del Bilag 439
Offentligt

DATATILSYNET

Datatilsynets årsberetning 2017

Udgiver: Datatilsynet
Tryk og layout: Rosendahls a/s
Beretningen er sat med Meta
Oplag: 130
September 2018
ISSN nr: 1601-5657
ISBN nr: 978-87-999222-2-2

Datatilsynets årsberetning 2017



DATATILSYNET

Indhold





Til Folketinget

Datatilsynet har i 2017 brugt betydelige ressourcer på at forberede, at EU's databeskyttelsespakke fuldt ud finder anvendelse fra den 25. maj 2018. Det gælder både herhjemme og internationalt i den såkaldte "Artikel 29-gruppe".

Databeskyttelsespakken, der vil få stor betydning for Datatilsynets fremtidige arbejde, består af en generel forordning om beskyttelse af personoplysninger, som gælder for både den private og offentlige sektor (databeskyttelsesforordningen), og et direktiv om beskyttelse af personoplysninger, som gælder for retshåndhævelsesområdet (retshåndhævelsesdirektivet). Forordningen, der erstatter databeskyttelsesdirektivet fra 1995, får virkning fra den 25. maj 2018. Direktivet, der erstatter en rammeafgørelse fra 2008, blev gennemført i dansk ret ved lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

Tilsynet har således bl.a. bidraget væsentligt til den betænkning om databeskyttelsesforordningen, der blev offentliggjort den 24. maj 2017 som et resultat af det projektarbejde, der siden forordningens vedtagelse i april 2016 har været iværksat i regi af Justitsministeriets departement. Datatilsynet har endvidere bl.a. i forbindelse med afgivelse af høringssvar forberedt implementeringen af retshåndhævelsesdirektivet og har siden 1. maj 2017, hvor retshåndhævelsesloven trådte i kraft, behandlet relevante generelle og konkrete sager efter denne lov. Herudover har Datatilsynet i forlængelse heraf bl.a. været ansvarlig for offentliggørelse af nationale vejledninger om forordningen, ligesom tilsynet – i regi af Artikel 29-gruppen – har bidraget til udarbejdelsen af fælleseuropæiske vejledninger om reglerne.

I 2017 har Datatilsynet også brugt mange ressourcer på internt at sikre, at tilsynet som organisation er klar, når det nye retsgrundlag finder anvendelse. Det gælder ikke mindst i forhold til de mange nye opgaver, Datatilsynet får i den forbindelse. Der er som følge heraf bl.a. foretaget en vis opnormering i antallet af medarbejdere i tilsynet på en række helt centrale områder.

Som en konsekvens af de betydelige ressourcer, som Datatilsynet har brugt på at forberede, at EU's databeskyttelsespakke fuldt ud finder anvendelse fra den 25. maj 2018, jf. ovenfor, har tilsynet i 2017 gennemført færre tilsyn, end hvad der har været tilfældet i de senere år. Datatilsynet foretog således 69 tilsyn i 2015 og 51 tilsyn i 2016. Datatilsynet har

dog i 2017 gennemført 38 tilsyn, herunder 15 tilsyn med fokus på supermarkeders tv-overvågning.

Datatilsynet har i 2017 også bidraget til en ny udgave af Erhvervsstyrelsens PrivacyKompas. På PrivacyKompasset kan virksomheder tage en onlinetest, der kan hjælpe dem i gang med at implementere databeskyttelsesreglerne i deres organisation og få svar på helt basale spørgsmål i forhold til ansvarlig datahåndtering. PrivacyKompasset kan således bruges til at få en status på dels, hvordan virksomheden håndterer personoplysninger, og dels hvad virksomheden skal gøre for at efterleve lovkravene og forberede sig til de kommende databeskyttelsesregler.

Endvidere prioriterer Datatilsynet at deltage med bl.a. indlæg på konferencer mv. for at informere om persondataloven, tilsynets praksis og – ikke mindst i 2017 – om det nye retsgrundlag, men også for, at tilsynet kan opnå større viden om, hvilke udfordringer de registrerede, andre offentlige myndigheder og den private sektor oplever inden for databeskyttelsesområdet.

Datatilsynet har i 2017 fortsat bestræbelserne på at effektivisere arbejdsgange og sagsbehandling med henblik på at få mest muligt ud af de ressourcer, som tilsynet har til rådighed. Samtidig er der med start fra 1. september 2017 gennemført en omorganisering af Datatilsynet, der bl.a. har resulteret i etableringen af en ny enhed, der har fået til opgave at få et større fokus og en mere effektiv indsats på det internationale arbejde.

Året har imidlertid også i vidt omfang været præget af arbejdet med større sagskomplekser og opgaver af international karakter. Datatilsynet har således behandlet flere større og ganske principielle sager om behandling af personoplysninger hos såvel offentlige myndigheder som private virksomheder. Der er endvidere i februar 2017 gennemført en Schengen-evaluering af Danmark i forhold til databeskyttelsesreglerne, hvor tilsynet også deltog.

Datatilsynets virksomhed i 2017

Datatilsynets opgaver

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

Persondataloven:

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

I tilknytning til persondataloven har Justitsministeriet udstedt en række bekendtgørelser. Datatilsynet har endvidere udarbejdet en række vejledninger vedrørende loven.

Tilsynet med persondataloven indebærer et stort antal forskelligartede opgaver. Datatilsynet har i 2017 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 (inkl. ad hoc-tilsyn), herunder tilsyn hos kommuner, regioner og private dataansvarlige mv.
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsyns-myndigheder
- Deltagelse i arbejdsgrupper, udvalg mv.
- 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.

Det er Datatilsynets mission at rådgive om registrering, videregivelse og anden behandling af person-oplysninger samt at føre tilsyn med, at myndigheder, virksomheder og andre dataansvarlige overholder persondataloven.

Rådgivning og vejledning

Datatilsynet udøver – som forudsat i de almindelige bemærkninger til persondataloven – først og fremmest sin virksomhed gennem generelle retningslinjer og ved en serviceorienteret rådgivning og vejledning.

Dette sikres bl.a. gennem tilsynets hjemmeside, hvor tilsynet løbende offentliggør relevant praksis og vejledning i relation til persondataloven samt vejledning i relation til databeskyttelsesforordningen mv. I 2017 offentliggjorde Datatilsynet således fem nationale vejledninger om forordningen. Endvidere har tilsynet – i regi af Artikel 29-gruppen – bidraget til udarbejdelsen af indtil videre fem fælleseuropæiske vejledninger om reglerne.

Det er Datatilsynets oplevelse, at der er en stadig større efterspørgsel efter at få tilsynet til at stille op og fortælle om persondataretlige problemstillinger. Datatilsynet har i 2017 deltaget med indlæg mv. på 34 konferencer og seminarer. Den fremtidige regulering på databeskyttelsesområdet og Datatilsynets rolle er i den forbindelse et emne, som interesserer mange. Datatilsynets direktør har således holdt flere indlæg om bl.a. databeskyttelsesforordningen, herunder status for arbejdet med implementeringen af forordningen for både den private og den offentlige sektor. Endvidere har Datatilsynet også deltaget i en debat om digitalisering og datasikkerhed til gavn for borgerne, hvor der deltog 150 it-chefer fra staten og kommunerne samt private it-chefer og leverandører, ligesom tilsynet har holdt oplæg om bl.a. markedsføring og samtykke.

Den Europæiske Databeskyttelsesdag finder sted hvert år den 28. januar. Databeskyttelsesdagen er en anledning til at gøre en særlig indsats for at give borgerne viden om databeskyttelse og deres rettigheder i den forbindelse. Datatilsynet fejrede i 2017 dagen ved at afholde en række webinarer om oplysningspligt og brud på persondataloven, som alle kunne tilmelde sig til. Endvidere var tilsynet i Grønland for at holde oplæg om konsekvenser af persondatalovens ikraftsættelse for Grønland dels for grønlandske myndigheder og dels for private virksomheder i Grønland. Oplægget til de grønlandske myndigheder blev i den forbindelse livestreamet til alle de grønlandske kommuner.

Herudover er rådgivning og vejledning om persondataloven over telefonen eller på baggrund af skriftlige forespørgsler en stor del af Datatilsynets arbejde. Tilsynet har i 2017 således registreret 11.687 telefoniske henvendelser. Antallet af telefoniske henvendelser har dermed været på cirka samme niveau som i 2016 (11.751 opkald).

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, undersøger tilsynet først, 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 2017 har Datatilsynet registreret en stigning på 39,5 % i antallet af nye sager (forespørgsler og klager) vedrørende private dataansvarlige (fra 1.083 i 2016 til 1511 i 2017). Hvad angår lignende sager vedrørende offentlige myndigheder, er der i 2017 registreret en stigning på 19 % i antallet af nye sager (fra 590 i 2016 til 702 i 2017).

Nedenfor ses eksempler på klagesager, som Datatilsynet i 2017 traf afgørelse i.

Rigspolitiets behandling af no-hits i politiets system for automatisk nummerpladegenkendelse (ANPG)

På baggrund af en borgerhenvendelse behandlede Datatilsynet i 2017 en sag om Rigspolitiets behandling af såkaldte no-hits i politiets system for automatisk nummerpladegenkendelse. Tilsynet har tidligere behandlet spørgsmål om ANPG. Se f.eks. Datatilsynets årsberetning 2015, side 8.

Sagen drejede sig om, hvorvidt Rigspolitiets opbevaring af no-hits i ANPG-systemet var i strid med Datatilsynets anbefalinger til Rigspolitiet og reglerne i bekendtgørelse nr. 1080 af 20. september 2017 om automatisk nummerpladegenkendelse (ANPG) og retshåndhævelsesloven. Til brug for sagens behandling indhentede Datatilsynet en udtalelse fra Rigspolitiet.

Efter at sagen var blevet forelagt for Datarådet, udtalte Datatilsynet, at det var tilsynets overordnede opfattelse, at behandlingen af no-hits i ANPG som udgangspunkt må anses for at ligge inden for rammerne af bekendtgørelsens § 6, stk. 1, da Rigspolitiet – efter tilsynets opfattelse – i sin udtalelse i tilstrækkelig grad havde redegjort for, at indsamlingen

af oplysninger om no-hits er sket på grundlag af en konkret politifaglig vurdering, hvor anvendelsen af ANPG vurderes at være af væsentlig betydning for de pågældende målrettede indsatser.

Om grundlaget for behandlingen af no-hits i ANPG udtalte Datatilsynet, at det er en forudsætning, at indsamlingen sker til ét eller flere udtrykkeligt angivne og saglige formål i form af en målrettet politiindsats, som ud fra proportionalitetsbetragtninger skal være tidsmæssigt og geografisk afgrænset. Afgrænsningen kan efter tilsynets opfattelse efter omstændighederne omfatte hele Danmarks territorialområde. Endvidere er det afgørende, at anvendelsen af ANPG vurderes at være af væsentlig betydning for den målrettede politiindsats.

Efter Datatilsynets opfattelse indebærer dette – bl.a. set i lyset af kravet om proportionalitet i retshåndhævelsesloven – at ikke blot anvendelse af ANPG, men selve opbevaringen af oplysninger om no-hits ud fra en politifaglig vurdering skal have væsentlig betydning for den målrettede politiindsats. Det er således en forudsætning, at der er foretaget en konkret politifaglig vurdering, hvorefter opbevaring af no-hits anses at have væsentlig betydning for opfyldelse af formålet med indsamlingen.

Datatilsynet understregede derfor generelt vigtigheden af, at Rigspolitiet i forhold til formålet med hver enkelt indsats nøje overvejer nødvendigheden af indsamling og opbevaring af no-hits i ANPG-systemet, hvorfor Rigspolitiet bør foretage en nærmere afvejning af behovet for og nytteværdien af behandlingen af no-hits set i forhold til det meget store antal personer, hvis færden bliver registreret.

Datatilsynet havde endvidere bemærkninger til Rigspolitiets fastsættelse af nye indsatsområder og anden anvendelse af indsamlede oplysninger fra ANPG.

Hvad er ANPG?

ANPG indebærer, at der via kameraer optages fotos af køretøjer, som passerer forbi kameraet, hvorefter speciel software automatisk finder 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. Behandlingen af oplysninger i ANPG er reguleret i bekendtgørelse nr. 1080 af 20. september 2017 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG).

ANPG-systemet indeholder en hit-del og en no-hit-del. Ved hits forstås nummerplader, hvortil der er registreret et særligt forhold (eksempelvis på grund af manglende syn), mens der for no-hits ikke er registreret et sådan forhold.

I no-hit-delen kan der bl.a. behandles oplysninger om nummerplader, som ikke er omfattet af hit-delen, når oplysningerne er indsamlet som led i en målrettet politiindsats. Indsatsen skal være tidsmæssigt og geografisk afgrænset og iværksat på baggrund af en konkret politifaglig vurdering, hvor anvendelsen af ANPG vurderes at være af væsentlig betydning for indsatsen. No-hits indsamlet i forbindelse med en målrettet politiindsats skal slettes senest 30 dage efter det tidspunkt, hvor oplysningerne er indsamlet.

Registrering og kreditvurdering af en virksomhed hos Creditsafe Denmark ApS

Datatilsynet traf i 2017 afgørelse om en virksomheds klage over Creditsafe Denmark ApS' registrering af virksomheden i Creditsafe Denmark ApS' erhvervsdatabase, og at Creditsafe Denmark ApS havde kreditvurderet virksomheden uden at være i besiddelse af tilstrækkelige oplysninger til at foretage en korrekt vurdering.

Datatilsynet vurderede med hjemmel i persondatalovens § 20, stk. 1, at Creditsafe Denmark ApS kunne behandle oplysninger om virksomheden i form af bl.a. stamdata trukket fra CVR. Datatilsynet lagde i den forbindelse vægt på, at tilsynet ikke umiddelbart kunne tilsidesætte en vurdering af, om oplysningerne efter deres art er af betydning for bedømmelsen af økonomisk soliditet og kreditværdighed, og som dermed kan registreres og videregives uden samtykke fra den registrerede. Datatilsynet fandt derfor ikke anledning til at udtale kritik af Creditsafe Denmark ApS' registrering af virksomheden i erhvervsdatabasen.

Creditsafe Denmark ApS havde endvidere foretaget en kreditvurdering af virksomheden. Kreditvurderingen fremstod som en rapport indeholdende informationer om virksomhedens nuværende og tidligere navne, CVR-nummer, virksomhedens startdato, virksom-

hedsform, branchekode, adresse, herunder e-mailadresse, telefonnummer og antal medarbejdere fordelt efter årstal. Derudover var virksomheden angivet med både en lokal og international score, der blev beskrevet som en moderat risiko, ligesom kreditvurderingen fastsatte en kreditbegrænsning på 25.000 kr. for virksomheden.

Creditsafe Denmark ApS oplyste i sagen, at når en virksomhed ikke har udarbejdet et årsregnskab, vil de parametre, der indgår i beregningen af kreditscoren, være informationer om den enkelte virksomheds stiftelsestidspunkt, branchekode, ledelse, antal medarbejdere, beliggenhed, virksomhedsform, tid på adressen og om virksomheden indgår i en koncern. Informationerne samles i en ratingmodel, hvor den enkelte virksomhed angives med en lokal og international score samt en angivelse af risikoen.

Datatilsynet fandt det på den baggrund kritisabelt, at Creditsafe Denmarks ApS' kreditvurdering af virksomheden ikke levede op til persondatalovens § 20. Datatilsynet lagde i sin afgørelse vægt på, at der i scoren ikke indgår økonomiske oplysninger, hvorfor der efter tilsynets opfattelse ikke blev givet et retvisende billede af virksomhedens kreditværdighed og betalingsevne i et fremtidigt skyldforhold.

Manglende indsigt i tv-optagelser i Dansk Supermarked

Datatilsynet har i 2017 behandlet en sag, hvor en mor (herefter klager) på vegne af sin søn klagede over, at hun havde fået afslag på indsigt i tv-overvågningsoptagelser optaget den 22. april 2015 i en butik tilhørende Dansk Supermarked Group (herefter Dansk Supermarked).

Baggrunden for klagers ønske om at få indsigt var, at hendes søn sammen med to andre personer havde været involveret i en sag om butikstyveri i den pågældende butik, og at politiet var blevet tilkaldt og havde optaget rapport. Sønnen var dog ikke blevet sigtet for butikstyveriet. Klager oplyste endvidere i sagen, at hun til Dansk Supermarked havde beskrevet, hvilket tøj hendes søn havde på den pågældende dag.

Dansk Supermarked anførte, at man ikke kunne give indsigt til klager uden et samtykke fra sønnen, ligesom der var brug for en regulær skriftlig fuldmagt udstedt af sønnen til moren, og at fuldmagten skulle vitterlighedspåtegnes.

Endvidere anførte Dansk Supermarked, at man fra sin leverandør af tv-overvågning havde fået oplyst, at det ikke var teknisk muligt at sløre de øvrige personer på tv-overvågningen. Optagelsen ville i stedet skulle hugges op i mindre stykker (5-8 billeder pr. sekund), sløres og herefter sættes sammen igen.

Dansk Supermarked anførte herudover, at det ville være forbundet med uforholdsmæssigt store omkostninger, hvis der skulle meddeles indsigt i tv-overvågningen (levende billeder), men at det kunne lade sig gøre at meddele indsigt i billeder fra tv-overvågningen, som Dansk Supermarked fortsat var i besiddelse af.

Datatilsynet udtalte bl.a., at der ikke kan stilles krav om, at den person, som fremsætter begæring om indsigt, præcist kan angive de behandlinger, som vedkommende ønsker indsigt i. På den anden side er det berettiget, at den dataansvarlige anmoder personen, der ønsker indsigt i forbindelse med tv-overvågning, om at komme med oplysninger, som kan hjælpe den dataansvarlige med at finde frem til eventulle oplysninger om personen. Sådanne oplysninger kan f.eks. være tid, sted og eventuelt et billede af den pågældende.

Datatilsynet udtalte også, at hvis en repræsentant for en registreret person retter henvendelse til en dataansvarlig, påhviler det denne at sikre sig, at repræsentanten er berettiget til at handle på vegne af den registrerede. Det er den dataansvarlige, som afgør, hvorledes repræsentanten skal godtgøre, at vedkommende er berettiget til at optræde som repræsentant for den, om hvem oplysninger behandles. Datatilsynet bemærkede i den forbindelse, at den dataansvarlige også har et ansvar for at sikre, at der ikke udleveres oplysninger til uvedkommende. Sker dette, vil den dataansvarlige evt. kunne gøres ansvarlig for at overtræde persondatalovens regler om databeskyttelse.

Datatilsynet henviste til afsnit 3.1.4 i tilsynets rettighedsvejledning fra 2000, hvori indsigt i oplysninger om børn og unge under 18 år er omtalt. Datatilsynet bemærkede hertil, at hovedreglen er, at en forældremyndighedsindehaver kan få indsigt i oplysninger om vedkommendes barn uden at skulle fremvise fuldmagt.

Efter Datatilsynets umiddelbare vurdering var der ikke i denne sag tale om forhold, som kun den unge kunne få indsigt i. Datatilsynet bemærkede hertil, at klager allerede var bekendt med detaljer omkring hændelsesforløbet og bistod sønnen med at få fjernet registreringer, som efter hendes mening var urigtige. Efter Datatilsynets opfattelse var en fuldmagt derfor ikke påkrævet.

Herefter præciserede Datatilsynet, at retten til indsigt efter persondataloven kun omfatter oplysninger om personen selv. Dette indebar, at det reelt kun ville være de brudstykker af overvågningsoptagelsen, hvor klagers søn fremgik, der skulle udleveres. Det kunne således være nødvendigt at opsplitte optagelsen til mindre billedsekvenser, som derefter kunne udleveres.

Klager havde således heller ikke krav på at få udleveret optagelser med de andre drenge – tværtimod: Hvis både klagers søn og andre personer indgik i en billedsekvens, skulle der ske sløring/overdækning af de andre tilstedeværende, medmindre de havde givet samtykke til udleveringen.

Hvis personerne var placeret på en sådan måde på nogle af billederne, at sløringen/overdækningen af en anden person i praksis også ville overdække billedet af klagers søn, var det reelt ikke muligt at give indsigt i de billedsekvenser, hvor dette måtte være tilfældet.

Hvis det reelt ikke var muligt at genkende klagers søn – eller at skelne ham fra de andre drenge – selv ved brug af et foto af klagers søn fra dengang og informationer om hans påklædning på dagen, var det heller ikke muligt at give indsigt.

Bortset fra de ovenfor beskrevne tilfælde, hvor det reelt ville være umuligt at give indsigt, var det Datatilsynets opfattelse, at der skulle gives klager som repræsentant for hendes søn indsigt i de optagelser, hvor han indgik.

Dansk Supermarkeds oplysning om store omkostninger forbundet hermed kunne ikke føre til et andet resultat.

Datatilsynet understregede, at det er den dataansvarlige virksomheds ansvar at besvare indsigtsanmodninger og at imødekomme disse i videst muligt omfang. Hvis den dataansvarlige virksomhed finder, at der er behov for yderligere oplysninger eller fuldmagter for at kunne besvare anmodningen, må virksomheden gå i dialog med den registrerede, dennes repræsentant og/eller eventuelt de andre registrerede for at få oplysningerne fremskaffet. Det bør ikke være nødvendigt med Datatilsynets mellemkomst.

Datatilsynet fandt det herefter kritisabelt, at Dansk Supermarked endnu ikke havde givet indsigt til klager og hendes søn i det omfang, det var muligt.

Sager på eget initiativ

I 2017 er der sket et fald på 33,6 % i antallet af sager på Datatilsynets eget initiativ (fra 110 i 2016 til 73 sager i 2017). Ressourcemæssige overvejelser har selvsagt indflydelse på den løbende prioritering af, hvilke sager der kan tages op af egen drift i Datatilsynet.

Behandling af oplysninger om bl.a. ophavsretlige krænkelser

På baggrund af flere borgerhenvendelser indledte Datatilsynet en undersøgelse af et specialiseret advokatfirma, der blandt andet beskæftiger sig med håndhævelse af immaterielle rettigheder.

Advokatfirmaet foretog registrering af IP-adresser, der havde deltaget i et peer-to-peer-baseret fildelingsnetværk, hvorfra der angiveligt var foretaget ulovlig download og distribution af eksempelvis film og tv-serier, med henblik på efterfølgende civilretlig påtale af ophavsretlige krænkelser.

Datatilsynet fandt, at når en IP-adresse, der er knyttet til en fysisk person, kædes sammen med ulovlig download og/eller distribution af ophavsretligt beskyttede værker, kan der være tale om en følsom oplysning om vedkommendes strafbare forhold omfattet af persondatalovens § 8.

Datatilsynet vurderede, at behandlingen kunne ske i medfør af persondatalovens § 7, stk. 2, nr. 4, jf. § 8, stk. 6, § 8, stk. 4, og § 6, stk. 1, nr. 7. Datatilsynet fandt således ikke grundlag for at kunne tilsidesætte advokatfirmaets vurdering af, at behandlingen af personoplysninger om personer, der formodes at have krænket advokatfirmaets klienters ophavsrettigheder, er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares i forbindelse med politianmeldelse eller civilretlig forfølgning.

Datatilsynet lagde vægt på, at ophavsretskrænkelser som hovedregel er undergivet privat påtale, og at det derfor i praksis ofte ville være umuligt for rettighedsindehavere at håndhæve deres rettigheder, hvis oplysningerne ikke kunne behandles.

Datatilsynet lagde også vægt på, at de indsamlede IP-adresser, der er kædet sammen med rettighedskrænkelserne, ikke er umiddelbart personhenførbare før det tidspunkt, hvor oplysninger om navn og adresse på abonnenten modtages fra internetudbyderen på baggrund af en retskendelse. Datatilsynet lagde i den forbindelse til grund, at der ved rettens vurdering af, hvorvidt en internetudbyder skal pålægges at udlevere disse identifikationsoplysninger, foretages en afvejning mellem bl.a. hensynet til beskyttelsen af personoplysninger og kommunikationshemmeligheden over for hensynet til effektiv

håndhævelse af immaterielle rettigheder med inddragelse af eksempelvis proportionalitetsprincippet.

Brug af fingeraftryk (biometri) ved bloddonation

Efter henvendelser fra en række borgere om registrering af fingeraftryk hos Blodbanken på Rigshospitalet startede Datatilsynet en sag af egen drift over for Region Hovedstaden.

I sin udtalelse til sagen oplyste Region Hovedstaden bl.a., at regionen anvender fingeraftryksidentifikation for at sikre identiteten på bloddonoren. På denne måde sikres det, at bloddonoren ikke forveksles med en anden person, hvorved risikoen for potentielt livsfarlige forbytninger mindskes. Oplysningerne blev lagret i form af billeder (bitmap-filer) sammen med donors personnummer, og ved et match af et fingeraftryk godkendtes donor, og tappeproceduren kunne fortsætte. De omhandlede billeder skulle efter regionens opfattelse opbevares i mindst 30 år, idet regionen henviste til bekendtgørelse nr. 1230 af 8. december 2005 om kvalitets- og sikkerhedskrav til blodbankvirksomhed.

Datatilsynet fandt, at Region Hovedstaden inden for rammerne af persondataloven kunne gøre brug af en biometrisk løsning med henblik på at kunne foretage en entydig identifikation af bloddonorer. Datatilsynet lagde bl.a. vægt på, at personforveksling ved bloddonation kan have meget alvorlige og potentielt fatale konsekvenser for modtagere af blod.

Datatilsynet fandt imidlertid, at den valgte løsning var betydeligt mere indgribende over for den registrerede, end hvad der kræves til formålet. Tilsynet lagde vægt på, at Region Hovedstaden registrerede billeder af donorernes fingeraftryk og ikke kun matematiske værdier udregnet på baggrund heraf (templates).

Datatilsynet bemærkede i den forbindelse, at den matematiske værdi, der registreres i en templateløsning, afhænger af den anvendte algoritme. Den matematiske værdi hos én dataansvarlig vil altså ikke nødvendigvis være den samme, som registreres på baggrund af det samme fingeraftryk hos en anden dataansvarlig. Mulighederne for at kunne samkøre to databaser og eventuelt anvende oplysningerne til uretmæssige eller uforenelige formål er derved begrænsede. Billeder af fingeraftryk udgør derimod de biometriske "rådata", som vil kunne samkøres med fingeraftryksbaserede oplysninger i andre databaser samt reproduceres og anvendes i andre uvedkommende sammenhænge.

Datatilsynet fandt endvidere ikke holdepunkter for at antage, at bestemmelserne i den nævnte bekendtgørelse forpligter regionen til at opbevare de biometriske oplysninger om donorer i mindst 30 år. Bekendtgørelsens krav om sporbarhed forudsætter efter tilsynets

forståelse ikke behandling af biometriske oplysninger om de pågældende donorer. Tilsynet fandt det derfor ikke godtgjort, at en generel slettefrist på 30 år levede op til persondatalovens princip om tidsbegrænsning.

Endelig bemærkede Datatilsynet, at tilsynets vurdering af regionens behandling af oplysninger om bloddonorers fingeraftryk – som blev foretaget i henhold til persondataloven – fortsat vil være aktuel efter databeskyttelsesforordningen.

Region Hovedstaden oplyste efterfølgende, at regionens procedure ville blive ændret, således at der i stedet for det nuværende billede af donorers fingeraftryk fremadrettet gemmes en hash-streng (matematiske værdier, template), som er den metode, der anvendes af de øvrige regioners blodbanker.

Advarselsregistre

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

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

Oplysninger om virksomheder mv. i advarselsregistre:

Persondataloven gælder som udgangspunkt kun for oplysninger om personer, men når der er tale om advarselsregistre, gælder loven også for oplysninger om virksomheder, foreninger mv.

Tilladelse og vilkår:

Datatilsynet fastsætter vilkår i forbindelse med en tilladelse til at føre et advarselsregister. Det er vilkår om, hvornår der må ske registrering i advarselsregistret. Herudover fastsætter Datatilsynet en række standardmæssige vilkår om oplysningspligt, indsigtsret, sletning og sikkerhed.

Nets' advarselsregister over kunder, som tidligere har misligholdt en kundeaftale

Nets søgte om tilladelse til at oprette et advarselsregister over virksomheder, der tidligere har misligholdt en kundeaftale med et selskab i Nets-koncernen.

Formålet med registret er at advare selskaber i Nets-koncernen mod kundeforhold med virksomheder, som tidligere har misligholdt en kundeaftale, og advare mod kundeforhold med personer, der har været ejere af en virksomhed, som tidligere har misligholdt en aftale med et selskab i Nets-koncernen.

Optagelse i registret afslører således, at den pågældende virksomhed har misligholdt en aftale med et selskab i Nets-koncernen, eller at den pågældende person har været ejer af en virksomhed, der har misligholdt en aftale med et selskab i Nets-koncernen.

Efter persondatalovens § 50, stk. 1, nr. 2, skal Datatilsynets tilladelse indhentes forinden iværksættelse af en behandling, som er omfattet af anmeldelsespligten i lovens § 48, når behandlingen af oplysningerne sker med henblik på at advare mod forretningsforbindelser med eller ansættelsesforhold til en registreret. Det er Datatilsynets opfattelse, at registret kun kunne tillades oprettet, hvis det tjener et anerkendelsesværdigt og sagligt formål.

Henset til, at registreret har til formål at forebygge økonomisk kriminalitet og at begrænse økonomisk tab for Nets-koncernen, fandt Datatilsynet efter forelæggelse for Datarådet, at registret tjener et anerkendelsesværdigt formål under forudsætning af, at der kunne opstilles objektive kriterier for, under hvilke omstændigheder registrering og videregivelse kan finde sted.

Datatilsynet meddelte på denne baggrund Nets tilladelse til at føre et advarselsregister med oplysninger om virksomheder og/eller personer, som kun kan indgå en kundeaftale efter en særlig vurdering. Tilladelsen blev meddelt på en række nærmere angivne vilkår, herunder en række vilkår for optagelse i advarselsregistret med henblik på at sikre, at optagelse i registret ikke beror på subjektive vurderinger.

Af disse vilkår fremgår bl.a., at registret efter sit indhold skal fremstå som en fortegnelse over virksomheder og/eller personer, som kun kan indgå en kundeaftale efter en særlig vurdering. Registret må ikke gennem sin overskrift eller øvrige indhold angive, at de registrerede virksomheder og/eller personer er afskåret fra at indgå en kundeaftale eller kun kan indgå en kundeaftale på særlige vilkår. Det fremgår endvidere, at der ikke må ske behandling af oplysninger om et forhold vedrørende virksomheden og/eller personen,

hvis forholdet er bestridt. Oplysningerne om en registreret må højst være registreret i to år.

I advarselsregistret må der kun ske registrering og videregivelse af oplysninger om virksomheder og/eller personer, hvis oplysningerne vedrører skyldforhold til samme kreditor på mere end 1.000 kr., og kreditor enten har erhvervet den registreredes skriftlige erkendelse af en forfalden gæld eller har foretaget retslige skridt mod den pågældende. Der kan endvidere behandles oplysninger, der hidrører fra Statstidende. Oplysninger om endeligt godkendt gældssanering må dog ikke videregives.

Endvidere kunne der ske optagelse i advarselsregistret på særlige vilkår godkendt af Datatilsynet.

I det omfang optagelse i registret sker på baggrund af misligholdelse af en indgået aftale, vil registrering og videregivelse af oplysningerne – forudsat registrering sker på baggrund af de særlige vilkår godkendt af Datatilsynet – alene udgøre behandling af almindelige, ikke-følsomme oplysninger omfattet af persondatalovens § 6.

Registret vil herudover indeholde en række identifikationsoplysninger om de registrerede virksomheder og/eller personer.

Datatilsynet lagde derfor til grund, at registret vil indeholde almindelige, ikke-følsomme oplysninger omfattet af persondatalovens § 6.

Datatilsynet fandt, at Nets og de øvrige selskaber i Nets-koncernen har en berettiget interesse i, at det i forbindelse med indgåelse af en ny kundeaftale kan tages i betragtning, om potentielle kunder tidligere har misligholdt en kundeaftale med et andet selskab i Nets-koncernen, og hvis de fastsatte vilkår for optagelse i registret bliver overholdt, at der kan ske registrering og videregivelse af oplysningerne, jf. persondatalovens § 6, stk. 1, nr. 7.

Datatilsynet fandt endvidere, at Nets inden for rammerne af persondatalovens § 11, stk. 2, nr. 2, og § 5, stk. 2, vil kunne behandle oplysninger om personnummer med henblik på entydig identifikation, hvis der foreligger et udtrykkeligt samtykke til behandlingen.

Høringer over lovforslag mv.

I 2017 registrerede Datatilsynet 584 nye høringssager i forbindelse med lovforslag, bekendtgørelser mv. Der er hermed sket en stigning på 24,5 % i forhold til 2016, hvor der var 469 høringssager.

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. Datatilsynet 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.

Lovhøring om ændring af taxiloven

Trafik-, Bygnings- og Boligministeriet anmodede om Datatilsynets eventuelle bemærkninger til et forslag til taxilov.

Datatilsynet udtalte sig bl.a. om, at der ved registrering og opbevaring af oplysninger om kørte taxiture, herunder bl.a. GPS-koordinater mv., efter Datatilsynets opfattelse vil være tale om behandling af personoplysninger. Datatilsynet anbefalede derfor, at Trafik-, Bygnings- og Boligministeriet foretog en nærmere vurdering af formålet eller formålene med den foreslåede forpligtelse til at registrere de pågældende oplysninger og om de(t) ønskede formål kunne opnås ved behandling af færre oplysninger.

Herudover anbefalede Datatilsynet at udvalgte bestemmelser i lovforslaget blev præciseret i forhold til persondatalovens og tv-overvågningslovens regler.

Lov om ændring af lov om Forsvarets Efterretningstjeneste (FE) og toldloven (FE's adgang til oplysninger om flypassagerer og ændring af FE's forpligtelse til sletning af oplysninger)

Forsvarsministeriet anmodede om Datatilsynets bemærkninger til lov om ændring af lov om Forsvarets Efterretningstjeneste (FE) og toldloven (FE's adgang til oplysninger om flypassagerer og ændring af FE's forpligtelse til sletning af oplysninger).

Udkastet til lovforslag vedrørte bl.a. etablering af særskilt lovhjemmel til, at FE kan få adgang til visse af de oplysninger om passagerer og besætning, som luftfartsselskaberne efter forslaget til ændring af toldloven skal overføre til skattemyndighederne. Med forslaget blev der således lagt op til, at skattemyndighederne skal videregive oplysninger om passagerer og besætning, der ikke er danske statsborgere, til FE, hvis tjenesten vurderer,

at oplysningerne kan have betydning for varetagelsen af tjenestens efterretningsmæssige virksomhed rettet mod forhold i udlandet. Dertil blev der foreslået hjemmel til, at forsvarsministeren efter forhandling med skatteministeren kan fastsætte regler om, hvordan oplysningerne skal stilles til rådighed, herunder ved oprettelse af en terminaladgang for FE til SKATs it-løsning.

Forslaget om terminaladgang rejste efter Datatilsynets opfattelse en række persondataretlige spørgsmål. Det stod eksempelvis ikke tilsynet klart, hvordan det i forbindelse med videregivelse kan sikres, at der, forinden oplysninger indhentes, foretages en konkret vurdering af nødvendigheden heraf. Tilsynet bemærkede, at det i sidste ende beror på en politisk vurdering, om en sådan terminaladgang skal etableres.

I forhold til udvidelsen af skattemyndighedernes eksisterende hjemmel til at modtage (og videregive til PET) oplysninger om passagerer og besætning på luftfartøjer, som luftfartsselskaberne er i besiddelse af, uanset om skattemyndighederne måtte have en selvstændig interesse i at få oplysningerne til brug for toldkontrol, bemærkede Datatilsynet bl.a., at det efter tilsynets opfattelse fulgte af persondatalovens § 5, at en dataansvarlig kun må indsamle oplysninger, som den dataansvarlige aktuelt har et behov for, og at indsamlingen af oplysninger skal sigte mod at løse opgaver, som falder inden for den dataansvarliges kompetenceområde/myndighedsudøvelse.

Det var derfor tilsynets opfattelse, at skattemyndighederne kun bør behandle, herunder indsamle og registrere, oplysninger, som myndigheden selv har behov for af hensyn til varetagelsen af egne formål, hvorfor det efter Datatilsynets opfattelse ville være mest hensigtsmæssigt at vælge en konstruktion, hvor oplysningerne enten videregives direkte til FE fra flyselskaberne, eller at etablere en ordning, hvor SKAT er databehandler for FE.

Lov om ændring af udlændingeloven (Øget brug af biometri m.v.)

Udlændinge- og Integrationsministeriet anmodede om Datatilsynets eventuelle bemærkninger til udkast til lov om ændring af udlændingeloven (Øget brug af biometri m.v.).

Efter forslaget skulle alle fingeraftryk af udlændinge optaget til forskellige formål, eksempelvis i forbindelse ansøgning om opholdstilladelse efter udlændingeloven, samles i én database, hvor fingeraftrykkene skulle opbevares i 30 år efter optagelsen heraf. Tilsvarende bestemmelser blev foreslået indsat i udlændingeloven i forhold til optagelse og opbevaring af personfotografi.

Indledningsvis bemærkede Datatilsynet, at der i forskellige internationale regelsæt er mulighed for at registrere fingeraftryk, og at den tidsmæssige udstrækning derfor afhang af formålet med registreringen.

Datatilsynet bemærkede herefter under henvisning til persondatalovens grundlæggende principper om formålsbestemthed og proportionalitet, at behandling af personoplysninger ikke må gå videre – hverken i omfang eller varighed – end hvad der kræves til opfyldelse af de formål, som den dataansvarlige er berettiget til at benytte.

Datatilsynet bemærkede i forlængelse heraf, at biometriske data (f.eks. fingeraftryk), der behandles med det formål entydigt at identificere en fysisk person, fra den 25. maj 2018, hvor databeskyttelsesforordningen finder anvendelse, vil være omfattet af de særlige kategorier af oplysninger (følsomme oplysninger) i forordningens artikel 9.

Henset til fingeraftrykkets særlige karakter bemærkede Datatilsynet, at behandling af fingeraftryk i en central database i 30 år efter tilsynets opfattelse er en særdeles indgribende behandling af personoplysninger for den registrerede, som derfor alene kan ske, hvis der er foretaget en nøje vurdering af behandlingens nødvendighed i forhold til de formål, der var angivet i udkastet til lovforslag.

Det fremgik ikke af udkastet til lovforslag, at der var foretaget en sådan nøje vurdering, hvorfor behandlingen efter Datatilsynets umiddelbare opfattelse gik langt ud over, hvad der er nødvendigt for at opnå det ønskede formål, som efter det oplyste var, at politiet og udlændingemyndighederne skal kende identiteten på de udlændinge, der indrejser og opholder sig i Danmark.

Datatilsynet fandt det således betænkeligt, at der skulle ske opbevaring af fingeraftryk i 30 år på personer, der ikke er mistænkt for at have begået strafbare handlinger, ligesom der ikke ses at være påvist en sammenhæng mellem udlændinge og identitetstyveri og/eller socialt bedrageri, hvorfor behovet for at anvende udlændinges – og ikke danske statsborgeres – fingeraftryk i denne sammenhæng ikke stod tilsynet klart.

Datatilsynet havde endvidere bemærkninger til lovforslaget i forhold til spørgsmål om dataansvar og samkøring af personoplysninger.

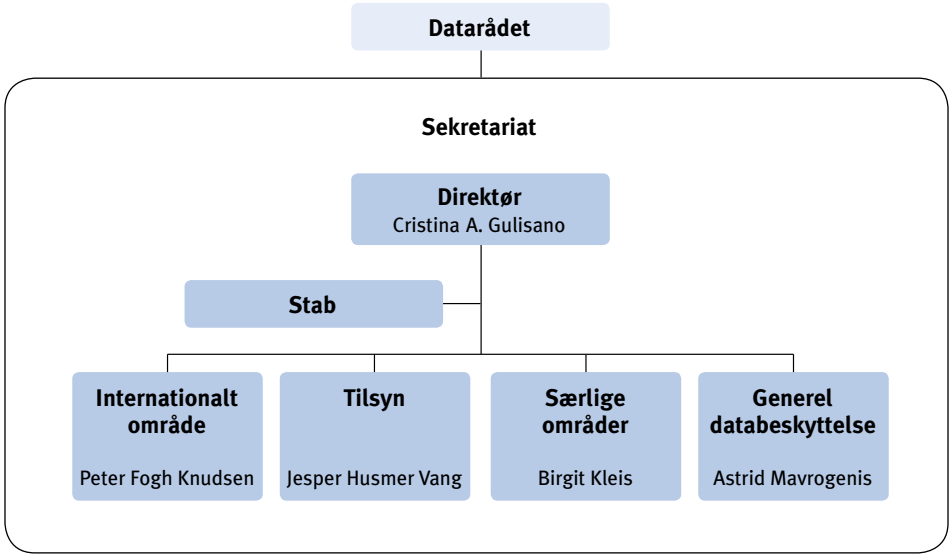
I det lovforslag, som blev fremsat af udlændinge- og integrationsministeren den 5. april 2017 (lovforslag L 188), var tidsrammerne ændret således, at fingeraftryk, der er optaget i forbindelse med ansøgning om asyl eller forlængelse af opholdstilladelse, opbevares til brug for identifikation og identitetskontrol i 20 år efter optagelsen af fingeraftrykket eller i 10 år efter optagelsen af fingeraftrykket, hvis udlændingen meddeles opholdstilladelse.

Endelig blev det i bemærkningerne til lovforslaget tilføjet, at fingeraftryk slettes, hvis udlændingen meddeles dansk indfødsret.

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 seks andre medlemmer, der alle 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.

Datarådets medlemmer (pr. 31. december 2017)

Formand, højesteretsdommer Henrik Waaben
Næstformand, advokat Janne Glæsel
Professor, dr.jur. Peter Blume
Overlæge, vicedirektør Hans Henrik Storm
Kommunaldirektør Niels Johannesen
IT-sikkerhedschef Henning Mortensen
Direktør Lars Pram

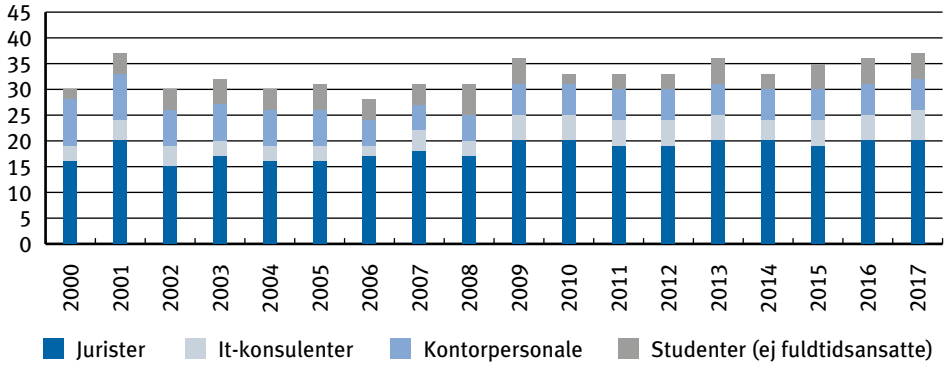
Medlemmerne beskikkes for fire år ad gangen. De er personligt udpeget i kraft af deres sagkundskab inden for bestemte sagsområder og er ikke repræsentanter for bestemte interesseorganisationer el.lign.

Sekretariatet

Sekretariatet beskæftiger omkring 38 medarbejdere (jurister, IT-konsulenter, kontorpersonale og studenter) og varetager Datatilsynets daglige drift under ledelse af en direktør, cand. jur. Cristina Angela Gulisano.

Datatilsynets bevillingsmæssige forhold mv. fremgår af Datatilsynets årsrapport for 2017. Årsrapporten er offentliggjort på tilsynets hjemmeside.

Personalesammensætning






Datatilsynets medarbejdere (pr. 31. december 2017)

Direktør, cand.jur. Cristina Angela Gulisano
Kommitteret, cand.jur. Birgit Kleis
Kontorchef, cand.jur. Astrid Mavrogenis
Kontorchef, cand.jur. Jesper Husmer Vang
Kontorchef, cand.jur. Peter Fogh Knudsen
It-chef, civilingeniør, HD, Sten Hansen
Chefkonsulent, cand.jur. Kia Hee Gade
Chefkonsulent, cand.jur. Lene Engedal Kragelund
Chefkonsulent, cand.jur. Mia Staal Klintrup
Chefkonsulent, cand.jur. Susanne Richter
Specialkonsulent, cand.jur. Katrine Valbjørn Trebbien
AC-stabsmedarbejder, cand.soc. Anne Bech
It-sikkerhedskonsulent, cand. jur. Allan Frank
It-sikkerhedskonsulent, cand.scient.dat. Farshid Shaikhrezai
It-sikkerhedskonsulent, Ph.d., Martin Mehl Lauridsen Schadegg
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
It-medarbejder Flemming Nielsen
It-medarbejder Thomas Klarskov Jensen
Kontorfuldmægtig Anne-Marie Müller
Kontorfuldmægtig Helle Jensen
Kontorfuldmægtig Mette-Maj Aner Leilund
Kontorfuldmægtig Pernille Jensen
Kontorfuldmægtig Suzanne Stenkvist
Assistent Camilla Knutsdotter Hallingby
Fuldmægtig, cand.jur. Ahang Faraje
Fuldmægtig, cand.jur. Amanda Lærke Vad
Fuldmægtig, cand.jur. Bjarke Asger Bro
Fuldmægtig, cand.jur. Camilla Andersen
Fuldmægtig, cand.jur. Cathrine Engsig Sørensen
Fuldmægtig, cand.jur. Cathrine Serup Raasdal
Fuldmægtig, cand.jur. Christine Børglum Sørensen
Fuldmægtig, cand.jur. Hanne Louise Høimark (Orlov)
Fuldmægtig, cand.jur. Karen Valgreen Knudsen
Fuldmægtig, cand.jur. Kenni Elm Olsen
Fuldmægtig, cand.jur. Lise Fredskov
Fuldmægtig, cand.jur. Makar Juhl Holst
Fuldmægtig, cand.jur. Mette Hansen
Fuldmægtig, cand.jur. Michala Nehammer
Fuldmægtig, cand. jur. Mikkel Brandenborg Stenalt
Fuldmægtig, cand.jur. Rasmus Møller Jakobsen
Fuldmægtig, cand.jur. Signe Vestergård Abildskov
Fuldmægtig, cand.jur. Sissel Michelle Kristensen (Orlov)
Fuldmægtig, cand.jur. Viktor Herskind Ingemann
Studentermedhjælper, stud.jur. Hakan Fehmi Secilmis
Studentermedhjælper, stud.jur. Jens Norgil Damgaard
Studentermedhjælper, stud.jur. Klara Kamilla Billeskov

Statistiske oplysninger

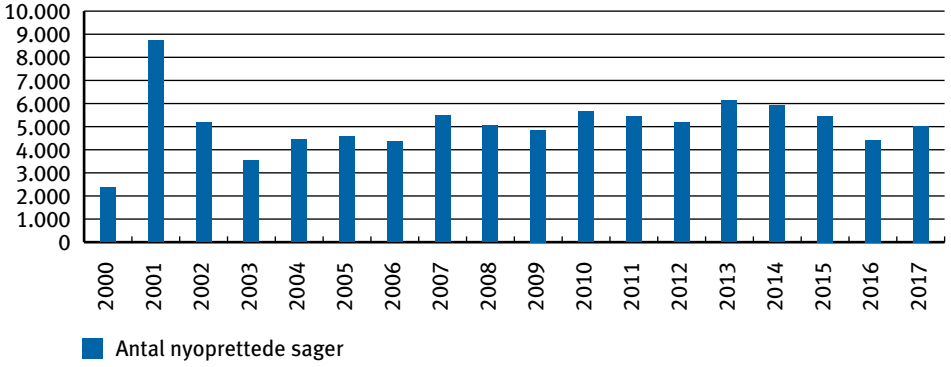
Her er oplysninger om antallet af nye sager i Datatilsynets journalsystem i 2017. Tallene omfatter sager, som er oprettet i løbet af 2017. En del af Datatilsynets sagsbehandling er imidlertid en fortsættelse af eksisterende sager. Dette er for eksempel tilfældet, når en anmeldelse ændres, eller en tilladelse forlænges. Disse sager er af praktiske årsager ikke medtaget i statistikken.

Datatilsynet registrerede 5.026 nye sager i 2017.

Nyoprettede sager 1. januar 2017 til 31. december 2017:

Datatilsynets egen administration mv.	391
Lovforberedende arbejde	584
Forespørgsler og klager vedrørende private	1.511
Forespørgsler og klager vedrørende offentlige myndigheder	702
Anmeldelser for den private sektor	1.271
Anmeldelser for den offentlige sektor	168
Sager på Datatilsynets eget initiativ (egendriftssager)	73
Sikkerhedsspørgsmål	2
Internationale sager	255
Datatilsynets kompetence efter anden lovgivning	69

Der har været en stigning på 14 % i det samlede antal nyoprettede sager i 2017 set i forhold til 2016. I 2017 blev der oprettet 5.026 nye sager mod 4.427 i 2016. Stigningen er fordelt på forskellige sagsgrupper, herunder sager om forespørgsler og klager særligt fra private, internationale sager samt lovforberedende arbejde.



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

Forespørgsler og klager vedrørende private

Datatilsynet registrerede i alt 1.511 nye sager om forespørgsler og klager vedrørende private dataansvarlige. Sagerne havde følgende fordeling på forskellige virksomhedstyper:

Almindelige virksomheder	83
Den finansielle sektor	83
Fagforeninger, a-kasser, pensionskasser mv.	5
Telesektoren	46
Foreninger og organisationer	189
Sundhedssektoren (medicinalfirmaer, klinikker, læger mv.)	37
Kreditoplysningsbureauer	95
Advarselsregistre	10
Stillingsbesættende virksomheder	3
Ansøgninger om tilladelser	68
Internet, sociale netværk, cloud mv.	326
Tv-overvågning	70
Private forskere	28
Diverse	486

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2017[1], var:

Klager	12 %
Forespørgsler	70 %
Ikke kategoriserede	18 %

Forespørgsler og klager vedrørende offentlige myndigheder

Datatilsynet registrerede i alt 702 nye sager om forespørgsler og klager vedrørende offentlige myndigheder. Sagerne var fordelt således:

Statslige myndigheder	248
Regioner	50
Primærkommuner	290
Ansøgning om tilladelser	73
Diverse	41

Fordelingen mellem klager og forespørgsler i sager, som Datatilsynet færdigbehandlede i 2017[2], var:

Klager	20 %
Forespørgsler	57 %
Ikke kategoriserede	23 %

1 I lighed med Datatilsynets årsberetning for 2016 er disse tal for 2017 ikke opgjort på grundlag af sager, som er oprettet i 2017, men på grundlag af sager, som Datatilsynet har færdigbehandlet i 2017. Heriblandt er sager oprettet i 2016 og 2015 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.
2 Se note 1

Anmeldelser

Anmeldelser for den private sektor

Datatilsynet registrerede i alt 1.274 nye sager om anmeldelser for den private sektor. Fordelingen af sagerne var:

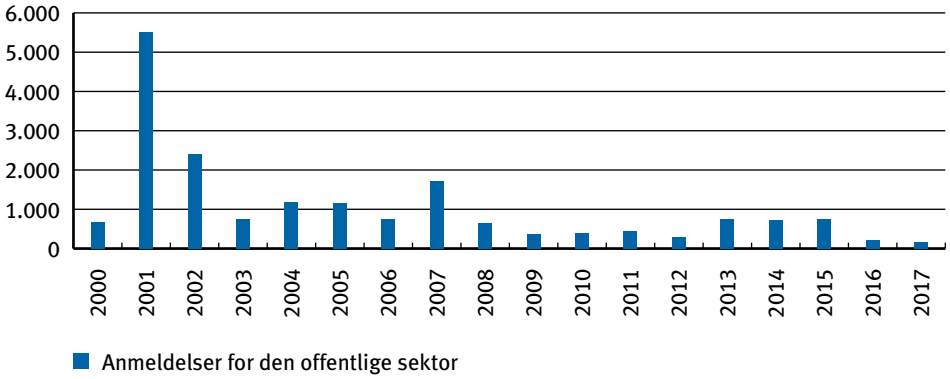
Forskning og statistik	341
Privates behandling af oplysninger om rent private forhold	890
Advarselsregistre	1
Spærrelister	0
Kreditoplysningsbureauer	7
Stillingsbesættende virksomheder	23
Edb-servicebureauer	8
Diverse sager af generel karakter	1

Faldet i antallet af anmeldelser for den private sektor fra 2016 til 2017 skyldes først og fremmest et stort fald i privates behandling af oplysninger om rent private forhold. Her er der sket et fald på 6 % fra 947 sager i 2016 til 890 i 2017. Dette fald skyldes sandsynligvis, at der fra 2015 til 2016 skete en stigning på 41 % i anmeldelser af privates behandling af oplysninger om rent private forhold.

Anmeldelser for den offentlige sektor

Datatilsynet registrerede i alt 168 nye sager om anmeldelser for den offentlige sektor. Fordelingen af sagerne var:

Fællesanmeldelser	0
Kommuner	51
Regioner	8
Statslige myndigheder	57
Tilslutninger, kommuner	42
Tilslutninger, regioner	0
Tilslutninger, statslige myndigheder	10
Diverse/sager af generel karakter	0



Antallet af offentlige anmeldelser er faldet med 17,6 % fra 204 sager i 2016 til 168 i 2017. Dette skyldes bl.a., at Datatilsynet tilbage i 2015 indførte statslige fællesanmeldelser på forskningsområdet, der omfatter alle behandlinger af oplysninger, som myndigheden udelukkende foretager i videnskabeligt eller statistisk øjemed. Der skal således ikke længere ske anmeldelse af hver enkelt videnskabelig undersøgelse og projekt. Det er derfor forventeligt, at niveauet er lavere i både 2016 og 2017.

Sager på Datatilsynets eget initiativ

Datatilsynet registrerede i alt 73 nye sager oprettet på tilsynets eget initiativ. Fordelingen af sagerne var:

Tilsyn og kontrol vedrørende private	17
Tilsyn og kontrol vedrørende offentlige myndigheder	22
Sager rejst på grundlag af presseomtale og lign.	34
Online-undersøgelser	0
Diverse/sager af generel karakter	0

Internationale sager

Datatilsynet registrerede i alt 255 nye internationale sager. Fordelingen af sagerne var:

Forespørgsler fra udlandet	115
Nordisk tilsynssamarbejde	1
Europarådet	1
EU	112
Datakommissærsamarbejdet	5
OECD	0
Diverse/sager af generel karakter	21

It-sikkerhed

Uberettiget adgang til personnumre på studerende hos Det Sundhedsvidenskabelige Fakultet på Københavns Universitet

Datatilsynet behandlede i 2017 en sag, hvor Det Sundhedsvidenskabelige Fakultet på Københavns Universitet ved en fejl havde videregivet oplysninger om navne og personnumre på 277 studerende. Datatilsynet blev bekendt med sagen på baggrund af en orientering fra en studerende fra Det Sundhedsvidenskabelige Fakultet.

Den uberettigede videregivelse var – efter det til Datatilsynet oplyste – sket ved, at en studiesekretær fra fakultetet ved en fejl havde lagt en holdliste indeholdende de studerendes navne og personnumre på systemet "Absalon". Det pågældende system var internt og kunne tilgås af de 277 studerende samt omkring 20 undervisere og administratorer ved at anvende et brugernavn og et password.

Holdlisten blev lagt på det interne system den 9. januar 2017, og blev fjernet samme dag, da man opdagede fejlen. Fakultetet havde imidlertid ikke været opmærksom på, at der systemmæssigt var genereret en kopi af den slettede liste, som automatisk var lagt i en arkivundermappe i systemet. Denne liste blev fjernet fra systemet den 13. januar 2017 efter en henvendelse fra en studerende.

Det Sundhedsvidenskabelige Fakultet på Københavns Universitet oplyste over for Datatilsynet, at de på baggrund af hændelsen internt ville skærpe fokus på, at holdlisterne ikke fremover indeholdte personnumre, samt at der generelt var et skærpet fokus på procedurerne efter hændelsen. Fakultetet oplyste endvidere, at de efter en konkret vurdering havde valgt ikke at underrette de berørte studerende om hændelsen.

Efter en gennemgang af sagen udtalte Datatilsynet kritik over for Det Sundhedsvidenskabelige Fakultet på Københavns Universitet, idet personoplysninger (personnumre), som fakultet var dataansvarlig for, havde været tilgængelige for uvedkommende i systemet "Absalon". Behandlingen af personoplysningerne havde – efter Datatilsynets opfattelse – ikke levet op til kravet om fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3.

Med hensyn til den manglende underretning af de berørte personer udtalte Datatilsynet endvidere, at en dataansvarlig myndighed eller virksomhed er forpligtet til at vurdere, om

der i forbindelse med et sikkerhedsbrud skal foretages underretning af de registrerede. Dette fulgte – efter Datatilsynets praksis – af grundreglen om god databehandlingsskik i persondatalovens § 5, stk. 1. Datatilsynet oplyste hertil, at den dataansvarlige bl.a. skal tage oplysningernes karakter samt de mulige konsekvenser for de berørte borgere i betragtning i forbindelse med en konkret vurdering.

Datatilsynet udtalte på denne baggrund, at Det Sundhedsvidenskabelige Fakultet på Københavns Universitet – efter tilsynets opfattelse – burde have underrettet de berørte personer. Datatilsynet lagde i den sammenhæng vægt på, at der findes eksempler på, at kompromittering af personnumre er blevet benyttet til f.eks. identitetstyveri, hvorfor de berørte personer kunne have et behov for at varetage deres interesser, herunder følge med i, at der ikke blev foretaget hævninger på deres private bankkonti eller lignende. Datatilsynet henstillede herefter til, at fakultetet snarest muligt underrettede de berørte personer.

Offentliggørelse af kontaktoplysninger hos jobansøgere hos Novo Nordisk

Datatilsynet blev i 2017 – på baggrund af en borgerhenvendelse – opmærksom på, at oplysninger om personer, der abonnerede på meddelelser om stillinger, som blev slået op af Novo Nordisk (”Jobagent-siden”), var tilgængelige for uvedkommende via internettet. Datatilsynet henvendte sig herefter straks til Novo Nordisk for at få stoppet sikkerhedsbruddet.

Sikkerhedsbruddet omfattede oplysninger om ca. 95.000 personer fra forskellige lande, og offentliggørelsen omfattede bl.a. oplysninger om fulde navn, e-mailadresse, telefonnummer, jobkategorier, der havde interesse for brugeren, lande, hvor brugeren var interesseret i at arbejde, antal års arbejdserfaring og tidsstempel for registrering af oplysningerne (dato for tilmelding til ”jobagenten”).

Novo Nordisk oplyste over for Datatilsynet bl.a., at personoplysningerne ved en fejl var gjort tilgængelige via en testside, som virksomhedens eksterne IT-leverandør oprettede i produktionsmiljøet på novonordisk.com, og at der var tale om en menneskelig fejl, som var foretaget i strid med godkendte testprocedurer.

Herudover oplyste Novo Nordisk, at der ikke optrådte nogen hyperlinks til hjemmesiden på andre dele af Novo Nordisks hjemmeside, at testsiden derfor i praksis alene kunne tilgås via søgemaskiner og af avancerede internet crawlers, at Novo Nordisk efter at være blevet bekendt med hændelsen instruerede IT-leverandøren om at deaktivere og slette

testsiden, at Novo Nordisk straks tog tiltag til at fjerne enhver gemt udgave af testsiden fra Google Search-søgemaskinen, at det blev bekræftet, at alle gemte udgaver af testsiden var slettet den 1. februar 2017, og at Novo Nordisk har verificeret, at testsiden ikke optræder på eller er gemt af de 13 største globale søgemaskiner.

Novo Nordisk oplyste endvidere, at der var igangsat en procedure med henblik på at underrette de berørte personer om hændelsen.

Efter en gennemgang af sagen udtalte Datatilsynet kritik over for Novo Nordisk, idet en stor mængde af personoplysninger, som Novo Nordisk var dataansvarlig for, havde været tilgængelige for uvedkommende via internettet. Behandlingen af personoplysningerne havde – efter Datatilsynets opfattelse – ikke levet op til kravet om fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3.

Sikkerhedsbrist hos Frederikshavn Kommune

Datatilsynet blev i 2017 – via en borgerhenvendelse – opmærksom på, at Frederikshavn Kommune ved en fejl havde sendt følsomme personoplysninger, herunder helbredsoplysninger, om flere borgere til en anden uvedkommende borger. Oplysningerne var herudover sendt via en ukrypteret e-mail.

Frederikshavn Kommune oplyste over for Datatilsynet, at sikkerhedsbruddet skyldtes en menneskelig fejl, og at medarbejderen ved en fejl ikke havde anvendt sikker post ved fremsendelsen.

Frederikshavn Kommune oplyste endvidere, at kommunen efterfølgende har planlagt, at alle afdelinger får undervisning i brug af sikker mail, at der vil blive udarbejdet en guide til brug af sikker mail, og at kommunens jurist og informationssikkerhedsmedarbejder sammen vil afvikle kurser i tavshedspligt og informationssikkerhed for hele organisationen.

Efter en gennemgang af sagen udtalte Datatilsynet kritik over for Frederikshavn Kommune, idet kommunens behandling af personoplysningerne – efter Datatilsynets opfattelse – ikke havde levet op til kravet om fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3, og i sikkerhedsbekendtgørelsen.

Datatilsynet noterede sig herudover, at Frederikshavn Kommune havde underrettet de berørte borgere om sikkerhedsbruddet via Digital Post.

Sikkerhedsbrist ved Styrelsen for Patientsikkerhed

Datatilsynet behandlede i 2017 en sag, hvor Styrelsen for Patientsikkerhed til en klager – med e-mail - havde sendt 900 siders dokumenter indeholdende sundhedsoplysninger om klager. Mailen indeholdt links til dokumenterne, som kunne hentes uden at indtaste en kode.

I forbindelse med behandlingen af sagen kom det frem, at Styrelsen for Patientsikkerhed havde benyttet en løsning benævnt Blue-whale. Denne løsning blev efter det oplyste benyttet ved fremsendelse af materiale, der fylder mere, end hvad der kan sendes via sikker Digital Post. Løsningen indebærer, at styrelsen sender links til dokumenterne via mail. I en række tilfælde indeholder mailen alene et link til en login-side, hvor modtageren skal indtaste en PIN-kode for at få adgang til materialet. Pinkoden bliver sendt til modtagerens mobilnummer. I den sendte e-mail er alt indhold fjernet, og emnet er ændret til "Sikker besked". For at kunne åbne og læse mailens korrekte emne, tekstindholdet og links til dokumenterne på Blue-whaleserveren skal modtageren både benytte linket i mailen og den fremsendte pinkode.

I klagers tilfælde havde styrelsen imidlertid ved en manuel fejl først sendt klager en e-mail med links til dokumenterne, som derefter kunne hentes uden at indtaste en kode. Efterfølgende sendte styrelsen klager en mail med link til en pinkode-beskyttet login-side og sendte desuden en PIN-kode til klagers mobilnummer.

Umiddelbart efter modtagelsen af den første e-mail fra Styrelsen for Patientsikkerhed rettede klager henvendelse til styrelsen omkring den utilstrækkelige sikkerhed.

Det blev under behandlingen af klagesagen oplyst, at den medarbejder, der stod for fremsendelsen, troede, at den første e-mail ikke var blevet sendt. Medarbejderen havde efter det oplyste tilbagekaldt mailen.

Efter en gennemgang af sagen fandt Datatilsynet det kritisabelt, at Styrelsen for Patientsikkerhed havde lagt 900 siders dokumenter med bl.a. helbredsoplysninger på internettet. Styrelsens behandling af personoplysninger havde ikke efter Datatilsynets opfattelse levet op til kravet om fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3.

Herudover udtalte Datatilsynet, at det er tilsynets opfattelse, at Styrelsen for Patientsikkerhed burde have opdaget sikkerhedsbristen i forbindelse med den første e-mail, som en medarbejder forsøgte at tilbagekalde, og at styrelsen burde have taget skridt til at begrænse skadevirkningerne – herunder ved at fjerne dokumenterne fra internettet. Herudover burde styrelsen have reageret på fejlen ved modtagelsen af klagers henvendelser.




Datatilsynet indskærpede også, at det er styrelsens ansvar, at medarbejderne er instrueret i, hvordan personoplysninger beskyttes, og at der skal tages effektive skridt til at begrænse skaden, hvis der sker fejl.

Utilstrækkelig sikkerhed i løsningen EASY-P

Datatilsynet behandlede i 2017 en sag, hvor en klager havde klaget til Datatilsynet over sikkerheden i løsningen EASY-P, som er et administrationssystem til praktikdelen af erhvervsskolerne.

Det fremgik af sagen, at:

- det havde været muligt at tilgå oplysninger om CPR-numre på en side i EASY-P benævnt "Værktøjssiden", hvis man havde adgang fra klagers uddannelsesinstitutions åbne trådløse netværk, som bl.a. kunne tilgås uden for skolen på kommunale stier,
- det havde været muligt at tilgå størstedelen af funktionaliteten i EASY-P ved at fjerne "secure" fra adressestien på en side for brugergodkendelse, hvorefter der var adgang til systemet,
- der bl.a. indgik et menupunkt benævnt "CPR-Søgning", som tillod indtastning af et givent CPR-nummer, hvorefter man som svar fik personens navn, samt
- at CPR-søgningen ikke var begrænset til elever på erhvervsskoler.

Datatilsynet udtalte, at Styrelsen for It og Lærings behandling af personoplysninger i EASY-P ikke havde levet op til kravet om fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3, og at tilsynet fandt dette kritisabelt.

Styrelsen for It og Lærings bemærkninger om, at der ikke var adgang fra det åbne internet, og at klager – efter styrelsens opfattelse – havde foretaget en uautoriseret handling, ændrede efter Datatilsynets opfattelse ikke på, at sikkerheden i løsningen var utilstrækkelig.

Datatilsynet udtalte også, at det var tilsynets umiddelbare vurdering, at der måtte tages initiativer til at indrette løsningen på en sådan måde, at der ikke var adgang til at foretage CPR-opslag på personer, der ikke går på erhvervsskolerne.

Logning i forbindelse med statistikproduktion

Datatilsynet afgjorde i 2017 to egendriftssager vedrørende henholdsvis Ankestyrelsens og KORA's overholdelse af logningskravet i sikkerhedsbekendtgørelsen i forhold til personoplysninger, som styrelsen og instituttet udelukkende behandlede i statistisk eller videnskabeligt øjemed.

I begge sager udtalte Datatilsynet, at logningskravet i sikkerhedsbekendtgørelsens § 19 ikke var overholdt i forbindelse med statistikproduktionen, og at tilsynet fandt dette kritisabelt.

Af sagen vedrørende KORA's overholdelse af logningskravet fremgik det, at KORA, som beskrevet i sikkerhedsbekendtgørelsens § 19, stk. 4, sidste punktum, foretog maskinel logning af bruger og tidspunkt for behandlingen, men at KORA ikke krypterede personhenførbare data, som kunne forekomme blandt observations- og interviewdata og i fraseparerede ID-filer, eller erstattede identifikationsoplysningerne med et kodenummer eller lignende.

Nyt retsgrundlag

Betænkning nr. 1565/2017 om Databeskyttelsesforordningen - og de retlige rammer for dansk lovgivning

Justitsministeriet har den 24. maj 2017 udgivet Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – de retlige rammer for dansk lovgivning (betænkningen).

Betænkningen indeholder to dele. Betænkningens første del indeholder en nærmere analyse af den gældende retstilstand og forordningens bestemmelser, herunder forordningens rammer for nationale særregler.

Første del af betænkningen er opdelt i kapitler, som svarer til kapitlerne i databeskyttelsesforordningen. Kapitlerne er endvidere opdelt i afsnit, der hovedsageligt er opdelt efter artiklerne i forordningen. Hvert afsnit indeholder – efter en indledning – en redegørelse for gældende ret i databeskyttelsesdirektivet og persondataloven med inddragelse af relevante kilder såsom praksis fra EU-Domstolen og Datatilsynet, diverse udtalelser fra Artikel 29-gruppen samt Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger.

Herefter er der i hvert afsnit oftest under overskriften "databeskyttelsesforordningen" en nærmere analyse af de pågældende bestemmelser i forordningen. Endvidere indeholder hvert afsnit et overvejelsesafsnit. Disse afsnit indeholder oftest en summarisk konklusion på, om bestemmelserne i forordningen svarer til, hvad der følger af gældende ret, eller om der er tale om en nyskabelse. Eksempelvis redegøres der i afsnittene vedrørende den registreredes rettigheder for, hvornår den registreredes rettigheder adskiller sig fra den gældende retstilstand efter persondataloven og databeskyttelsesdirektivet, samt hvornår der er tale om "nye" rettigheder. I overvejelsesafsnittene overvejes det også summarisk om en eventuel særlig dansk retstilstand vil kunne opretholdes.

Betænkningens anden del indeholder en analyse af konsekvenserne for gældende dansk særlovgivning i forhold til forordningen inden for samtlige ministeriers område. Anden del af betænkningen indeholder en samlet overordnet vurdering af gældende ret på de enkelte ministeriers ressortområde i forhold til forordningen, inklusiv et bilag med angivelse af de relevante love om behandling af personoplysninger og deres ophæng i databeskyttelsesforordningen.

De enkelte ministerier har således gennemgået lovgivningen på ministeriets ressortområde med henblik på at identificere bestemmelser, der regulerer behandling af personop-

lysninger eller i øvrigt har relation til forhold, som databeskyttelsesforordningen regulerer, herunder f.eks. den registreredes rettigheder. Ministerierne har i samarbejde med Justitsministeriet i den forbindelse vurderet, om de pågældende bestemmelser kan opretholdes, når databeskyttelsesforordningen anvendes fra den 25. maj 2018. Ministerierne har i samarbejde med Justitsministeriet vurderet, at de fleste af de identificerede bestemmelser om behandling af personoplysninger mv. kan opretholdes, når databeskyttelsesforordningen finder anvendelse.

Betænkningens konklusioner

Det fremgår af betænkningen, at analysearbejdet har vist, at forordningen i vidt omfang svarer til den gældende retstilstand efter persondataloven og databeskyttelsesdirektivet med tilhørende praksis fra bl.a. EU-Domstolen og Datatilsynet. Bl.a. svarer forordningens centrale bestemmelser om anvendelsesområde, definitioner, principper for behandling af personoplysninger, behandlingsregler, de registreredes rettigheder og behandlingssikkerhed i stort omfang til gældende ret efter persondataloven og databeskyttelses-direktivet.

Derudover indeholder forordningen bestemmelser, som er en nyskabelse i forhold til den gældende retstilstand. Dette er eksempelvis bestemmelserne om databeskyttelsesrådgivere, konsekvensanalyse og fortegnelser over behandlingsaktiviteter samt en udtrykkelig bestemmelse om "data protection by design".

På den baggrund vil der – ifølge betænkningen – med forordningen ikke være tale om omfattende ændringer for myndigheder og private organisationer, der i forvejen lever op til persondataloven.

Det fremgår dog i den forbindelse endvidere af betænkningen, at der sikkert vil være offentlige myndigheder og private organisationer mv., som ikke på nuværende tidspunkt opfylder alle krav i persondataloven og derfor ikke er "compliant" med gældende ret. For disse offentlige myndigheder og private er det oplagt, at der med databeskyttelsesforordningen er skabt "awareness" eller "bevidsthed" omkring betydningen af beskyttelse af personoplysninger. Betænkningen angiver selv, at dette nok er en konsekvens af, at EU-lovgiver nu har vedtaget en generel forordning om databeskyttelse, som bl.a. indeholder mulighed for at pålægge større bøder for overtrædelse af forordningens bestemmelser.

Betænkningens retlige status

Betænkningens analyser er baseret på eksisterende retskilder. Betænkningen vil således ikke stå alene som fortolkningsbidrag fremover. Hvor retstilstanden ikke kan anses for entydig, indeholder betænkningen i vidt omfang forslag til mulige løsninger.

Det må forventes, at fortolkningen af forordningen på flere punkter i de kommende år vil blive udviklet gennem praksis fra bl.a. det med forordningen nyoprettede Europæiske Databeskyttelsesråd, EU-Domstolen, de danske domstole og Datatilsynet.

Den nuværende retstilstand er f.eks. baseret på meget få domme, og det må forventes, at der fremover vil komme flere domme fra bl.a. EU-Domstolen.

I det omfang, der kommer bindende afgørelser fra EU-Domstolen, nationale domstole, Databeskyttelsesrådet og den uafhængige tilsynsmyndighed mv., skal betænkningens analyser naturligvis læses i lyset af den nye praksis.

Forslag til databeskyttelseslov mv. (L 68 og L 69)

I juli 2017 sendte Justitsministeriet et udkast til forslag til databeskyttelseslov (lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) i høring.

Efter behandling af sagen i Datarådet afgav Datatilsynet den 22. august 2017 en udtalelse over lovforslaget.

Datatilsynet fremkom med en række bemærkninger af mere redaktionel og præciserende karakter og havde endvidere mere indgående bemærkninger og forslag til ændringer af flere bestemmelser i lovforslaget og bemærkningerne hertil.

Tilsynet foreslog således en ændret affattelse af lovforslagets § 10 om behandling af personoplysninger i forbindelse med statistiske eller videnskabelige undersøgelser. Datatilsynets forslag er – efter yderligere dialog mellem tilsynet og Justitsministeriets departement – afspejlet i § 10, stk. 3 og stk. 4, i det lovforslag, der senere blev fremsat for Folketinget.

I høringssvaret tilsluttede Datatilsynet sig endvidere indsættelsen af bestemmelsen i databeskyttelseslovens § 11, stk. 2, nr. 4, hvorefter private – i modsætning til efter den tidligere lovgivning – har mulighed for at behandle oplysninger om personnummer, når betingelserne i lovens § 7 om behandling af følsomme oplysninger er opfyldt.

Ved fremsendelsen af lovforslaget i høring var der endnu ikke taget stilling til spørgsmålet om sanktioner i forhold til offentlige myndigheder. Datatilsynet bemærkede i høringssvaret, at der gennem tiden har været mange eksempler på, at offentlige myndigheder har begået gentagne overtrædelser af databeskyttelseslovgivningen, hvilket efter tilsynets opfattelse kunne tale for også at fastsætte bestemmelser om straf for offentlige myndigheder.

For så vidt angår de foreslåede tilladelsesordninger henviste Datatilsynet til præambelbetragtning nr. 89 til databeskyttelsesforordningen, hvori det bl.a. er anført, at den tidligere generelle anmeldelsespligt medførte en administrativ og finansiel byrde, men ikke i alle tilfælde bidrog til at forbedre beskyttelsen af personoplysninger.

Datatilsynet tilsluttede sig det anførte i præambelbetragtningen og bemærkede, at tilsynet umiddelbart var uforstående overfor, at der efter udkastet til lovforslag fortsat skulle være anmeldelsespligt på flere områder. Tilsynet fremsatte endvidere bemærkninger af mere redaktionel karakter til de foreslåede bestemmelser om tilladelsesordninger, ligesom tilsynet foreslog indsættelse af en overgangsbestemmelse i forhold til tidligere udstedte tilladelser.

I august 2018 sendte Justitsministeriet endvidere udkast til lovforslag om konsekvensændringer som følge af databeskyttelsesloven og databeskyttelsesforordningen i høring. Datatilsynet havde kun få bemærkninger til dette udkast til lovforslag.

Lovforslagene blev fremsat som hhv. L 68 og L 69 i oktober 2017 med henblik på vedtagelse af Folketinget i 2018.

Nationale vejledninger

I forlængelse af offentliggørelsen af betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning offentliggjorde Datatilsynet sammen med Justitsministeriet og til dels Erhvervsstyrelsen og Digitaliseringsstyrelsen i ef-

teråret 2017 en række nationale vejledninger, der med eksempler og et mere let tilgængeligt sprog forklarer de nye databeskyttelsesregler.

De vejledninger, der blev offentliggjort i efteråret 2017, var:

- Generel informationspjece om databeskyttelsesforordningen
- Vejledning om overførsel af personoplysninger til tredjelande
- Vejledning om samtykke
- Vejledning om dataansvarlige og databehandlere
- Vejledning om databeskyttelsesrådgivere.

Ovennævnte vejledninger – som Datatilsynet har fået gode og positive tilbagemeldinger på fra offentligheden – kan alle findes på Datatilsynets hjemmeside under punktet "Generelt om databeskyttelse".

Vejledninger mv. fra Artikel 29-gruppen

Artikel 29-gruppen, der er nedsat i henhold til artikel 29 i det generelle databeskyttelsesdirektiv fra 1995, har i 2017 bl.a. lagt mange ressourcer i udarbejdelsen af vejledninger i relation til det nye retsgrundlag forud for, at databeskyttelsesforordningen begynder at finde anvendelse i 2018.

Arbejdet har resulteret i et større antal vejledninger om bl.a. følgende emner:

- Dataportabilitet (wp242)
- Databeskyttelsesrådgivere, DPO'ere (wp243)
- Udpegelse af ledende tilsynsmyndighed (wp244)
- Konsekvensanalyser vedrørende databeskyttelse, DPIA (wp248)
- Anmeldelse af brud på persondatasikkerheden (wp250)*
- Automatiske afgørelser og profilering (wp251)*
- Administrative bøder i henhold til databeskyttelsesforordningen (wp253)
- Tredjelandsoverførsler, tilstrækkeligt databeskyttelsesniveau (wp254)*
- Bindende virksomhedsregler (BCR) (wp256 m.fl.)*
- Samtykke (wp259)*
- Gennemsigtighed og oplysningsforpligtelser (wp260)*

Vejledningerne er udtryk for Artikel 29-gruppens opfattelse af, hvordan det nye retsgrundlag skal fortolkes i relation til de nævnte emner. Vejledningerne har i forbindelse med tilblivelsen været igennem en offentlig høring, hvor både virksomheder, borgere, myndigheder og andre har haft mulighed for at komme med input, der er blevet inddraget i de endelige versioner af vejledningerne.

Vejledningerne markeret med en * blev sendt i offentlig høring i 2017 og udgives i en endelig version i 2018.

Internationalt samarbejde

Artikel 29-gruppen

Artikel 29-gruppen er nedsat i henhold til artikel 29 i det generelle databeskyttelsesdirektiv fra 1995. Gruppen er uafhængig og rådgiver EU-Kommissionen om persondataretlige emner. Den består af repræsentanter for de nationale tilsynsmyndigheder i EU (samt andre europæiske lande, der har status som observatører), en repræsentant for Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) og en repræsentant for EU-Kommissionen. Datatilsynets direktør repræsenterer Danmark.

I 2017 afholdt Artikel 29-gruppen fem møder i Bruxelles.

Artikel 29-gruppen har i 2017 især arbejdet med forberedelserne til den 25. maj 2018; dagen, hvorfra databeskyttelsesforordningen finder anvendelse. Gruppen har i den forbindelse udarbejdet en række vejledninger til de dataansvarlige om forståelsen af det nye retsgrundlag samt vedtaget en række interne procedurer i relation til det fremtidige samarbejde mellem tilsynsmyndighederne. Se mere om dette i afsnittet om det nye retsgrundlag.

Artikel 29-gruppen har endvidere vedtaget en række henstillinger, udtalelser mv. om andre emner inden for databeskyttelsesområdet. Gruppen har bl.a. afgivet udtalelser om:

- Forslaget til en ny e-privacy-forordning. Gruppen bakker i udtalelsen op om: at regulere området fremover i en forordning, at placere tilsynet med området hos medlemsstaternes datatilsyn, og at de såkaldte "Over-The-Top" tjenester bliver omfattet af regelsættet. Omvendt er Artikel 29-gruppen bekymret for, at beskyttelsen på områder som lokationssporing, kommunikationsindhold og –metadata. Ifølge Artikel 29-gruppen bør beskyttelsen ikke forringes i det nye regelsæt, og gruppen kommer derfor i sin udtalelse med konkrete forslag til, hvordan man kan sikre samme eller en bedre beskyttelse fremadrettet,
- resultatet af den første evaluering af EU-U.S. Privacy Shield. Artikel 29-gruppen konstaterer, at Privacy Shield er et bedre grundlag for overførsel af personoplysninger end den tidligere Safe Harbour-ordning, og at der i løbet af det første år er blevet arbejdet med implementeringen af ordningen. Artikel 29-gruppen understreger dog samtidig, at der stadig er udeståender, som bør adresseres, herunder især, at der endnu ikke er udpeget en permanent ombudsmand, at de formelle udnævnelser inden for Privacy and Civil Liberties Oversight Board (PCLOB) ikke har fundet sted, og at der mangler supplerende oplysninger, dels om ombudsmandsmekanismen, dels om yderligere af-

klassificering af procedurereglerne, især vedrørende ombudsmandens samarbejde med efterretningstjenesterne, og
- persondatabehandling på arbejdspladsen. Udtalelsen er en opdatering og et supplement til to tidligere udtalelser herom fra 2001 og 2002 med udgangspunkt i de mange nye teknologiske muligheder, der er kommet til for behandling af personoplysninger i en ansættelsesretlig sammenhæng siden årtusindskiftet. Udtalelsen beskæftiger sig især med persondataretlige spørgsmål i forhold til ansættelsesprocessen, it-overvågning af medarbejdere, videoovervågning og videregivelse af oplysninger.

Det bemærkes, at fra og med den 25. maj 2018 erstattes Artikel 29-gruppen af Det Europæiske Databeskyttelsesråd. Gruppens dokumenter er dog fortsat tilgængelige på EU-Kommissionens hjemmeside, http://ec.europa.eu/justice/article-29/documentation/index_en.htm.

Schengen-informationssystemet (SIS)

Som en del af Schengen-samarbejdet om et fælles område uden indre grænser samarbejder medlemslandene om kriminalitetsbekæmpelse og kontrol ved de ydre grænser via bl.a. et fælles informationssystem (SIS II), som indeholder personoplysninger. Datatilsynet fører tilsyn med, at de danske myndigheder med adgang til systemet overholder en række regler i den forbindelse.

Som led i tilsynet med behandling af personoplysninger i SIS II deltager Datatilsynet i Koordinationsgruppen for tilsynet med anden generation af Schengen-informationssystemet (SIS II SCG), hvilket er en gruppe bestående af repræsentanter for Den Europæiske Tilsynsførende for Databeskyttelse, de nationale datatilsyn i EU-medlemslandene samt for de nationale datatilsyn i Island, Norge, Liechtenstein og Schweiz.

I 2017 har der været afholdt to møder i koordinationsgruppen, hvor man bl.a. har udarbejdet en rapport om adgangen til SIS II på nationalt niveau. Gruppen har også udarbejdet og vedtaget et brev til EU-institutionerne og de nationale parlamenter med henblik på at gøre opmærksom på manglen på finansielle og personalemæssige ressourcer hos de nationale tilsyn og den manglende efterlevelse af forpligtelsen til at tildele de nationale tilsyn tilstrækkelige ressourcer til at kunne udføre deres opgaver.

Derudover har gruppen drøftet følgende emner:

- Lovgivningspakken fremlagt af EU-Kommissionen den 21. december 2016 bestående af tre udkast til forordninger om henholdsvis politisamarbejde og retligt samarbejde,

grænsekontrol og tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold, der skal erstatte det eksisterende retsgrundlag for SIS-II,
- opbevaring af SIS II-logs på nationalt niveau,
- anbefalinger givet ved seneste Schengen-evaluering af medlemsstaterne,
- opslag i SIS II i forbindelse med administrative procedurer og
- nationale kriterier for anvendelse af artikel 24-indberetninger

Repræsentanter for EU-Kommissionen og eu-LISA[3] har endvidere deltaget på møderne med henblik på at drøfte aktuelle databeskyttelsesretlige spørgsmål og holde gruppen underrettet om den aktuelle situation for SIS II.

På Datatilsynets hjemmeside under punktet "Internationalt" findes generel information om Schengen-samarbejdet, Schengen-informationssystemet (SIS II) og Datatilsynets opgaver i relation til SIS II, herunder muligheden for at klage til Datatilsynet over behandling af personoplysninger i SIS II.

Toldinformationssystemet (CIS)

Toldinformationssystemet har til formål at bekæmpe svig inden for EU ved gennem hurtig deling af informationer mellem EU-landenes myndigheder at kunne forebygge, efterforske og retsforfølge transaktioner, der er i strid med EU's told- og landbrugsbestemmelser. Formålet er endvidere at kunne forebygge, efterforske og retsforfølge overtrædelser af nationale love vedrørende toldadministration.

SKAT er dataansvarlig for toldinformationssystemet i Danmark, mens Datatilsynet er tilsynsmyndighed.

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

Der har i 2017 været afholdt et enkelt møde i Koordinationsgruppen for tilsynet med Toldinformationssystemet.

3 Den Europæiske Unions agentur for store it-systemer

Eurodac

Eurodac er et centralt fingeraftryksregister over asylansøgere i EU, som er oprettet med henblik på at fremme asylproceduren i EU. Datatilsynet fører tilsyn med, at de danske myndigheder med adgang til systemet overholder en række regler i den forbindelse.

Som led i tilsynet med Eurodac deltager Datatilsynet i Koordinationsgruppen for tilsynet med Eurodac (Eurodac SCG), hvilket er en gruppe bestående af repræsentanter for Den Europæiske Tilsynsførende for Databeskyttelse, de nationale datatilsyn i EU-medlemslandene samt for de nationale datatilsyn i Island, Norge, Liechtenstein og Schweiz.

I 2017 har der været afholdt to møder, hvor gruppen bl.a. haft besøg af repræsentanter for EU-Kommissionen og eu-LISA med henblik på at drøfte aktuelle databeskyttelsesretlige spørgsmål og at holde gruppen underrettet om den aktuelle situation for Eurodac-systemet.

Gruppen har endvidere udarbejdet et spørgeskema om rettigheder for registrerede i Eurodac med henblik på en generel undersøgelse af efterlevelsen af disse rettigheder i praksis.

Endvidere har gruppen drøftet følgende emner:

- EU-Kommissionens forslag af 4. maj 2016 til omarbejdning af Eurodac-forordningen,
- sikring af sletning af oplysninger i medfør af artikel 13 i Eurodac-forordningen vedrørende asylansøgere, som har opnået statsborgerskab i en medlemsstat og
- anvendelsen af såkaldte kategori 9-søgninger i forbindelse med en registrerets anmodning om indsigt

På Datatilsynets hjemmeside under punktet "Internationalt" findes generel information om Eurodac og Datatilsynets opgaver i relation til Eurodac, herunder muligheden for at klage til Datatilsynet over behandling af personoplysninger i Eurodac.

Visum-informationssystemet (VIS)

Til håndteringen af ansøgninger om visa til kortvarige ophold inden for Schengen-landene er der i EU oprettet et centralt register over visumansøgernes fingeraftryk og ansigtsbilleder. Datatilsynet fører tilsyn med, at de danske myndigheder med adgang til systemet overholder en række regler i den forbindelse.

Som led i tilsynet med behandling af personoplysninger i VIS deltager Datatilsynet i Koordinationsgruppen for tilsynet med Visum-informationssystemet (VIS SCG), hvilket er en gruppe bestående af repræsentanter for Den Europæiske Tilsynsførende for Databeskyttelse, de nationale datatilsyn i EU-medlemslandene samt fra de nationale datatilsyn i Island, Norge, Liechtenstein og Schweiz.

I 2017 har der været afholdt to møder, hvor gruppen bl.a. haft besøg af repræsentanter for EU-Kommissionen og eu-LISA, som har orienteret gruppen om den seneste udvikling på området, herunder Entry-Exit systemet, ETIAS og EU-Kommissionens anbefalinger på baggrund af den generelle evaluering af VIS, som EU-Kommissionen gennemførte i oktober 2016. Gruppen har endvidere etableret en undergruppe, der skal udforme et spørgeskema om træning i databeskyttelse for personer med adgang til VIS med henblik på en generel undersøgelse heraf.

Gruppen har endvidere drøftet følgende emner:

- overholdelse af de databeskyttelsesretlige regler ved anvendelse af underdatabehandlere, herunder kontraktforholdet til underdatabehandlerne og
- implementering af artikel 41 i VIS-forordningen vedrørende audit af de nationale VIS systemer

På Datatilsynets hjemmeside under punktet "Internationalt" findes generel information om VIS og Datatilsynets opgaver i relation til VIS, herunder muligheden for at klage til Datatilsynet over behandling af personoplysninger i VIS.

Indre Markeds-informationssystemet (IMI)

Indre Markeds-informationssystemet, udarbejdet af EU-Kommissionen, giver offentlige myndigheder i EU mulighed for administrativt samarbejde medlemsstaterne imellem.

Datatilsynet er udpeget som tilsynsmyndighed i relation til behandlingen af personoplysninger i den danske del af systemet. På EU-niveau deltager Datatilsynet i Koordinationsgruppen for tilsynet med Indre Markeds-informationssystemet IMI (IMI SCG).

I 2017 blev der ikke afholdt nogen møder i Koordinationsgruppen.

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[4], 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 2017 været afholdt ét møde i den fælles kontrolinstans.

Europarådet

Europarådet blev oprettet i 1949 og danner i dag rammen om et samarbejde mellem 47 lande, herunder de 28 EU-lande. Danmark var blandt de 10 stiftende medlemmer af Europarådet i 1949. Medlemskab af Europarådet kræver, at staterne underskriver Den Europæiske Menneskerettighedskonvention (EMRK).

I databeskyttelsessammenhæng har Danmark ratificeret Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) og tillægsprotokollen om tilsynsmyndigheder og grænseoverskridende dataudveksling (konvention 181). Datatilsynet er udpeget som tilsynsmyndighed i forhold til konvention 108.

Det er Justitsministeriet, der møder i Europarådets arbejdsgruppe for databeskyttelse, hvor man i 2017 bl.a. har arbejdet med en opdatering af konvention 108.

Berlin-gruppen

International Working Group on Data Protection in Telecommunications, også kaldet Berlin-gruppen, arbejder med informationsteknologier og tendenser, med henblik på at afdække implikationer for databeskyttelse og privatliv, samt at give anbefalinger til interes-

4 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

senter. Gruppens arbejde afspejles i rækken af publicerede udtalelser, såkaldte Working Papers, som er tilgængelige på Berlin-gruppens hjemmeside.

Berlin-gruppen har i 2017 afholdt to møder. I april mødtes gruppen i Washington, og i november afholdtes gruppens møde i Paris. Datatilsynet deltog i begge møder.

Gruppens fokus på privatliv og sikkerhed har i 2017 blandt andet haft det såkaldte "internet of things" IOT på programmet. Denne opkobling på internettet af diverse husholdningsartikler, aktivitetsmålere og legetøj til børn, blot for at nævne nogle områder, skaber alle en betydelig informationsindsamling hos den enkelte og med nogle enheder, der typisk har ingen eller ringe sikkerhed. Gruppens mål har været at få lavet beskrivelser og oplæg til standarder, der giver brugere af sådant udstyr mulighed for at vide, hvordan og hvor oplysninger indsamles og lagres, og at enhederne kan opdateres, sådan at sikkerheden ikke kompromitteres.

Berlin-gruppen har fortsat arbejdet med de såkaldte "connected cars". Der bliver arbejdet på at få konsolideret viden fra de forskellige bilproducenter, de forskellige udviklingshuse og serviceleverandører der leverer denne type af teknologi til biler. Alt fra brug af telemetri, færdselsovervågning, kørestilsanalyse til "infotainment" er i fokus hos gruppen. Udviklingen går mere og mere i retning af biler med fast opkobling og brug af internetbaserede apps. Herudover er også de såkaldte autonome køretøjer såsom førerløse biler på dagsordenen i gruppen. Der arbejdes på beskrivelser af de implikationer, teknologien har for såvel privatliv som databeskyttelse, og hvordan brugen kan ske transparent og under brugerens kontrol.

En tilsvarende udvikling ses i det, der kaldes "smart cities" eller "urban connectivity", hvor der via store mængder data, blandt andet mastedata, wi-fi og bluetooth-forbindelser, kan følges og målrettes både fremtidig brug af f.eks. offentlig transport og andre ydelser, eller helt målrettet reklame, der på baggrund af metadataindsamling målrettes det enkelte individ, når dette går forbi bestemte reklameskilte.

Disse emner vil gruppen komme med udtalelser om i 2018-19.

I årets løb har Berlin-gruppen endvidere fortsat arbejdet med aktuelle emner, som indeholder problemstillinger med hensyn til databeskyttelse og beskyttelse af privatliv, eksempelvis anvendelse af biometri i elektronisk online autentifikation, ISO-standardisering, privatlivsbeskyttelse ved ICANN's RDS (Registration Directory Services) for internettet, og forhold omkring forfølgelse og uønsket opmærksomhed i digital forstand, det såkaldte "cyber bullying" and "stalking".

Nordisk samarbejde

Datatilsynet lægger stor vægt på at have et tæt samarbejde med de øvrige nordiske datatilsyn som følge af mange fælles interesser og synspunkter. I den forbindelse afholder tilsynene en gang om året et fællesnordisk samarbejdsmøde med deltagelse af såvel direktører og andre fra ledelsen, som sagsbehandlere og it-eksperter. I 2017 blev mødet afholdt i maj i Tromsø, Norge.

Mødets emner bar præg af, at alle tilsyn var i gang med forberedelserne til anvendelsen af det nye retsgrundlag i databeskyttelsesforordningen i 2018, og på dagsordenen var bl.a. tilsynenes nye rolle og de nye rettigheder og forpligtelser i forordningen, men også emner som kunstig intelligens, overvågning og sundhedsoplysninger blev drøftet.

Den europæiske konference

Som et led i det europæiske samarbejde afholdes hvert forår en konference (forårskonferencen), hvor de europæiske datatilsyn drøfter aktuelle spørgsmål om databeskyttelse.

Datatilsynet var repræsenteret på årets konference, som blev afholdt i Limassol, Cypern. På konferencen drøftedes bl.a. emner som det nye retsgrundlag i form af databeskyttelsesforordningen, opdateringen af Europarådets konvention 108, ligesom dna-databaser var et tema. På konferencen vedtog datatilsynene en resolution med opbakning til arbejdet med moderniseringen af Europarådets konvention 108 blev vedtaget.

Den internationale konference

Hvert år afholdes der en international konference for databeskyttelseskommissærer med deltagere fra hele verden. Konferencen indeholder en åben del og en del kun for datatilsynsmyndighederne, hvor databeskyttelseskommissærerne bl.a. vedtager resolutioner vedrørende aktuelle problemstillinger inden for databeskyttelse og beskyttelse af privatlivet.

I 2017 blev konferencen afholdt i oktober i Hong Kong, hvor man vedtog en række resolutioner om bl.a. "connected vehicles" og et styrket samarbejde mellem databeskyttelsesmyndigheder. Datatilsynet var ikke repræsenteret på årets konference.

Den internationale konference har sin egen hjemmeside på https://icdppc.org/

Datatilsynets tilsyn

Datatilsynets tilsynsvirksomhed skal ses i lyset af tilsynets mission og vision. Tilsynets mission omfatter både rådgivning om registrering, videregivelse og anden behandling af personoplysninger og tilsyn med, at myndigheder, virksomheder og andre dataansvarlige overholder persondataloven. Datatilsynets tilsyn opfylder begge hovedformål med vægten lagt på tilsynsdelen.

Selv om det primære formål med Datatilsynets tilsyn er at foretage konkret kontrol og om nødvendigt at sikre en bedre overholdelse af loven hos de dataansvarlige, er tilsynene også en anledning for Datatilsynet til at komme i dialog med virksomheder og myndigheder. Tilsynet indsamler via sine tilsyn også viden om, hvordan behandlingen af personoplysninger foregår hos forskellige typer af dataansvarlige. Denne viden kan tilsynet på det generelle plan anvende i andre sammenhænge, f.eks. til at vurdere om der er behov for at udarbejde vejledningsmateriale eller skabeloner/blanketter til de dataansvarlige inden for et specifikt område.

Datatilsynets tilsynsstrategi

I 2016 offentliggjorde Datatilsynet en ny tilsynsstrategi - Datatilsynets tilsynsstrategi 2016-2018 "Ny organisation af tilsynsarbejdet" – som fastlægger de overordnede rammer for tilsynsaktiviteterne. Strategien indeholder bl.a. initiativer, som skal sikre et effektivt tilsyn.

Ét af initiativerne i strategien var oprettelse af en ny tilsynsenhed, som har fået ansvaret for alle Datatilsynets planlagte tilsyn og Datatilsynets ad hoc-tilsyn vedrørende brud på persondatalovens sikkerhedskrav.

Planlagte tilsyn og ad hoc-tilsyn

I Datatilsynets tilsynsstrategi sondres der mellem to typer af tilsyn:

- Planlagte tilsyn – dvs. tilsyn, der iværksættes som led i Datatilsynets årlige tilsynsplanlægning, og
- Ad hoc-tilsyn – dvs. tilsyn, der iværksættes som følge af konkrete hændelser.

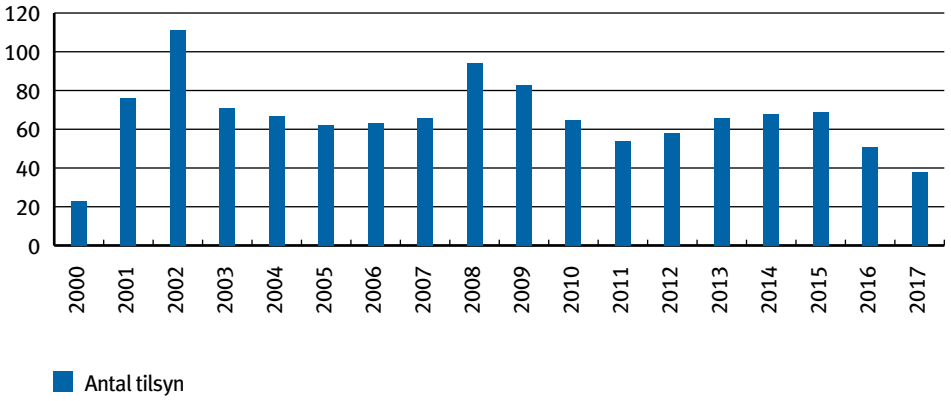
Ved udvælgelse af emner for planlagte tilsyn skal der ifølge tilsynsstrategien for 2016-2018 navnlig fokuseres på behandlinger af personoplysninger, som på grund af deres omfang eller formål kan indebære en særlig risiko for at krænke de registreredes ret til databeskyttelse og privatliv, samt på behandlinger, som indebærer brug af ny teknologi.

Ved udvælgelsen af såvel emner som de dataansvarlige, der skal indgå i de planlagte tilsyn, tager Datatilsynet bl.a. i betragtning, om der på et område er fremkommet oplysninger – herunder ved henvendelser fra borgere eller via medieomtale – der kunne tyde på et særligt behov for tilsyn.

Tilsyn i 2017

I 2017 foretog Datatilsynet 38 planlagte tilsyn. Disse planlagte tilsyn var fordelt med 21 tilsyn over for offentlige myndigheder og 17 tilsyn over for private virksomheder. På alle tilsynene har der været anvendt oplysningsindsamling bl.a. ved hjælp af spørgeskema. Herudover har Datatilsynet over for samtlige 17 private virksomheder fulgt op med et fysisk tilsynsbesøg.

Som det fremgår af tabellen, har der været et fald i det samlede antal tilsyn i 2017 set i forhold til de tidligere år.



Faldet i antallet af tilsyn skyldes bl.a., at Datatilsynet i 2017 har brugt betydelige ressourcer på projekter relateret til databeskyttelsesforordningen. Datatilsynet har i den sammenhæng i stort omfang medvirket til udarbejdelsen af betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, ligesom tilsy-

net som nævnt ovenfor har været forfatter eller medforfatter på en række vejledninger om databeskyttelsesforordningen.

Datatilsynets tilsynsenhed fokuserede i 2017 på udvalgte emner hos en række dataansvarlige.

Hos de offentlige myndigheder er følgende emne som udgangspunkt gået igen:

- efterlevelse af reglerne om oplysningspligt i persondatalovens kapitel 8.

Herudover har Datatilsynet ført kontrol med Erhvervsstyrelsen i forhold til styrelsens eventuelle behandling af personoplysninger i Overtrædelsesregistret for personer med næringsbrev.

Tilsynene med offentlige myndigheder var fordelt på kommuner, regioner og en enkelt statslig myndighed.

Hos de private virksomheder er følgende emner gået igen:

- tv-overvågning hos supermarkeder
- fodboldklubbers håndhævelse af politiets karantæner.

Tilsyn hos kommuner

Datatilsynet foretog i sommeren 2017 planlagte tilsyn med 15 kommuners efterlevelse af reglerne om oplysningspligt i persondatalovens kapitel 8. Tilsynene forventes afsluttet i 2018.

Tilsyn hos regioner

Datatilsynet foretog i sommeren 2017 planlagte tilsyn med de fem regioners efterlevelse af reglerne om oplysningspligt i persondatalovens kapitel 8. Tilsynene forventes afsluttet i 2018.

Tilsyn hos private dataansvarlige

Datatilsynet gennemførte i foråret 2017 planlagte tilsyn med 15 supermarkeder, der behandler personoplysninger i forbindelse med tv-overvågning. Fokus for disse tilsyn var tv-overvågningens formål og indretning, kameraernes placering, de registreredes rettigheder, herunder opfyldelse af oplysningspligten og håndtering af indsigtsanmodninger, og datasikkerhed.

Datatilsynets tilsyn gav det indtryk, at der blandt supermarkederne var stor forskel på, i hvilket omfang de overholdt persondataloven. Datatilsynets tilsyn resulterede således i alt fra ikke at udtale kritik til at udtale, at den manglende efterlevelse var kritisabel.

Datatilsynet kunne med tilsynene konstatere følgende overtrædelser af persondataloven:

- Manglende databehandleraftaler,
- opbevaring af optagelser fra tv-overvågning i mere end 30 dage og
- manglende sletning af overskudsinformation ved berettiget opbevaring af optagelser fra tv-overvågning i mere end 30 dage.

I slutningen af 2017 har Datatilsynet foretaget planlagte tilsyn med to fodboldklubbers behandling af personoplysninger ved håndhævelse af politiets karantæner i forbindelse med afholdelse af fodboldkampe.

Ingen af de to tilsyn gav anledning til, at Datatilsynet udtalte kritik.

Oversigt over udførte tilsyn i 2017

Staten:

Erhvervsstyrelsen

Kommuner (oplysningspligt):

Fanø Kommune
Middelfart Kommune
Frederikssund Kommune
Herlev Kommune
Helsingør Kommune
Hørsholm kommune
Kalundborg Kommune
Sorø Kommune
Aarhus kommune
Billund Kommune
Herning kommune
Haderslev Kommune
Lemvig Kommune
Struer Kommune
Thisted Kommune

Regioner:

Region Nordjylland
Region Midtjylland
Region Syddanmark
Region Hovedstaden
Region Sjælland

Dansk Supermarked (TV-overvågning):

Bilka One Stop, Fields
Bilka, Ishøj Bycenter
Coop Brugsen, St. Kongensgade
Coop Dagli'Brugsen, Islev torv
Coop Kvickly, Strandlodsvej
Føtex, Nordre Fasanvej, Frederiksberg
Føtex, Glostrup Shoppingcenter
Irma, Peter Bangs Vej
KIWI Hvidovre, Frihedens Butikscenter
Meny, Bagsværd
Meny, Valby
Meny, Østerfælled Torv
Netto, Landemærket
Spar, Glostrup
Superbrugsen, Ålekistevej

Fodboldklubber (karantænelister):

Brøndby IF Fodbold A/S
Parken Sport & Entertainment A/S

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

ISSN nr: 1601-5657
ISBN nr: 978-87-999222-2-2