Datatilsynet

Årsberetning

2019

DATATILSYNET

Datatilsynet

Årsberetning

2019

DATATILSYNET

Indhold

Til Folketinget

Datatilsynet har i 2019 brugt betydelige ressourcer på at rådgive og vejlede om EU's databeskyttelsesforordning og databeskyttelsesloven, der har fundet anvendelse siden 25. maj 2018, samt retshåndhævelsesloven, der blev gennemført i dansk ret ved lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

Hver dag håndterer Datatilsynet mange telefoniske og skriftlige forespørgsler og træffer samtidig løbende afgørelser i konkrete sager, der kan tjene som vejledning for andre, ligesom tilsynet udarbejder vejledninger mv. Datatilsynet har i 2019 således offentliggjort 11 nye nationale vejledninger, som supplerer de 13 vejledninger, som tilsynet offentliggjorde i 2017 og 2018, ligesom der løbende er blevet udarbejdet mindre tekster under forskellige databeskyttelsesretlige emner. Datatilsynet har endvidere udgivet en podcast med 15 episoder om databeskyttelsesforordningen, der skal hjælpe små og mellemstore virksomheder til at få et overblik over reglerne, ligesom tilsynet har offentliggjort 10 små animerede videoer om databeskyttelsesreglerne, der er målrettet borgerne.

Datatilsynet yder også en aktiv indsats på dette område i europæiske sammenhænge. Tilsynet har i 2019 – i regi af Det Europæiske Databeskyttelsesråd – bidraget til udarbejdelsen af to nye fælleseuropæiske vejledninger mv. om forordningen.

Alle de nævnte vejledninger – nationale som fælleseuropæiske – kan sammen med en række praktisk anvendelige skabeloner til f. eks. opfyldelse af oplysningspligten, som Datatilsynet har udarbejdet, findes på tilsynets hjemmeside.

Datatilsynet prioriterer endvidere at deltage med bl.a. indlæg på konferencer, seminarer mv. for at informere om databeskyttelsesreglerne og tilsynets praksis, 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. I juni 2019 deltog Datatilsynet for første gang med oplæg og en stand med diverse aktiviteter på Folkemødet på Bornholm, ligesom tilsynet som noget nyt i år havde en stand på Ungdommens Folkemøde i september 2019, hvor de unge kunne komme forbi til quiz, debat og workshops, og hvor de kunne høre mere om, hvilke rettigheder de har. Herudover var Datatilsynet aktiv med oplæg og en stand på både Digitaliseringsmessen i Odense den 3. oktober 2019, der henvendte sig til den offentlige sektor, og Digitaliseringsmessen for erhvervslivet, der blev afholdt dagen efter samme sted.

Fra og med den 25. maj 2018 er alle dataansvarlige – som noget nyt – forpligtet til som udgangspunkt at anmelde brud på persondatasikkerheden til Datatilsynet. For at gøre det nemt og enkelt for virksomheder og myndigheder at indberette sikkerhedshændelser på databeskyttelsesområdet og en række andre områder, udviklede og lancerede Datatilsynet og en række andre myndigheder i samarbejde med Erhvervsstyrelsen i maj 2018 på Virk.dk en fælles digital løsning for anmeldelser af sikkerhedshændelser. Initiativet skal understøtte, at virksomhederne og myndighederne kun skal indberette hændelser én gang og ét sted frem for at skulle indberette stort set samme information flere steder. Datatilsynet har i hele 2019 brugt mange ressourcer på at behandle de anmeldelser af brud på persondatasikkerheden, som tilsynet hver dag modtager.

Datatilsynet har i 2019 endvidere offentliggjort en endelig liste over situationer, hvor dataansvarlige altid skal udarbejde konsekvensanalyser. Herudover har Datatilsynet i år anmodet Det Europæiske Databeskyttelsesråd om en udtalelse over tilsynets skabelon til standarddatabehandleraftale og herefter revideret aftalen i lyset af den afgivne udtalelse, hvorefter skabelonen har fået karakter af standardkontraktbestemmelser, som den første af sin slags i EU.

For at sikre en effektiv beskyttelse af personoplysninger styrkes og præciseres med databeskyttelsesforordningen bl.a. de forpligtelser, der påhviler dem, der behandler og træffer afgørelse om behandling af personoplysninger, ligesom tilsynsmyndighedernes beføjelser til at føre tilsyn med og sikre overholdelse af reglerne øges.

Datatilsynets tilsynsvirksomhed kan føre til, at der tages strafferetlige skridt. Det er derfor væsentligt, at tilsynets medarbejdere har et godt kendskab til de mange forhold, som det er vigtigt at være opmærksom på helt fra en sags begyndelse til dens afgørelse ved domstolene, herunder bevissikring, retssik-

kerhedslov og udformning af anklageskrift. Datatilsynet har derfor i 2019 også rekrutteret et mindre antal medarbejdere med baggrund i politi- og anklagemyndigheden, der kan bistå i dette arbejde. Herudover har Datatilsynet deltaget i et samarbejde med Rigsadvokaten og Rigspolitiet, der har til formål at tilrettelægge den samlede håndtering af straffesager vedrørende overtrædelse af databeskyttelsesreglerne på tværs af myndighederne.

Efter databeskyttelseslovens § 10, stk. 3, kan oplysninger, der er behandlet i statistisk eller videnskabeligt øjemed, i nærmere angivne tilfælde kun videregives med tilladelse fra Datatilsynet. Efter lovens § 10, stk. 4, kan Datatilsynet fastsætte generelle vilkår for videregivelse af sådanne oplysninger, herunder videregivelse, der ikke kræver tilsynets tilladelse. Tilsynet har fastsat sådanne generelle vilkår ved bekendtgørelse nr. 1509 af 18. december 2019. Datatilsynet har endvidere fastsat standardvilkår for meddelelse af tilladelse efter databeskyttelseslovens § 26 til private dataansvarliges behandling af oplysninger i form af advarselsregistre og spærrelister, kreditoplysningsbureauer samt retsinformationssystemer. Vilkårene og en række vejledende tekster herom er offentliggjort på Datatilsynets hjemmeside.

Valby, maj 2020

Kristian Korfits Nielsen
Formand, Datarådet

Cristina Angela Gulisano
Direktør, Datatilsynet

Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2019 afgives i medfør af databeskyttelsesforordningens artikel 59, hvorefter tilsynet afgiver en årlig beretning om sin virksomhed til det nationale parlament, regeringen og andre myndigheder, der er udpeget efter medlemsstaternes nationale ret. Årsberetningen indeholder omtale af væsentlige aktiviteter for Datatilsynet i 2019, herunder aktiviteter i henhold til artikel 58, stk. 2. Der henvises endvidere til retshåndhævelseslovens § 45, som indeholder en lignende bestemmelse om, at Datatilsynet skal afgive en årlig beretning til Folketinget og justitsministeren.

På Datatilsynets hjemmeside www.datatilsynet.dk offentliggør tilsynet løbende udtalelser og afgørelser i sager, som vurderes at være af generel interesse. Datatilsynet kan således henvende til sin hjemmeside for yderligere oplysninger. Årsberetningen sendes endvidere til EU-Kommissionen og Det Europæiske Databeskyttelsesråd, ligesom den offentliggøres på Datatilsynets hjemmeside.

Om Datatilsynet

Datatilsynets opgaver

Datatilsynet er den centrale, uafhængige myndighed, der fører tilsyn med, at reglerne på databeskyttelsesområdet overholdes. Tilsynet med domstolenes behandling af personoplysninger ligger dog hos Domstolsstyrelsen.

Tilsynet med reglerne på databeskyttelsesområdet indebærer et stort antal forskelligartede opgaver, og Datatilsynet har i 2019 bl.a. haft følgende opgaver:

- Information, rådgivning og vejledning
- Behandling af klagesager
- Udtalelser om lovforslag og udkast til bekendtgørelser og cirkulærer mv.

- Behandling af anmeldelser af brud på persondatasikkerheden
- Bidrag til besvarelse af spørgsmål fra Folketinget
- Sager på Datatilsynets eget initiativ (inkl. ad hoc tilsyn) herunder tilsyn hos offentlige myndigheder og private dataansvarlige mv.
- Deltagelse i internationale tilsynsmyndigheder og internationalt samarbejde med andre datatilsynsmyndigheder
- Deltagelse i arbejdsgrupper, udvalg mv. i f.eks. EU
- Oplæg på konferencer, seminarer o. lign.

Datatilsynet er endvidere national tilsynsmyndighed for behandling af personoplysninger i en række fælleseuropæiske informationssystemer (bl.a. Schengen-, visum og toldområdet), hvilket betyder, at tilsynet fører tilsyn med de danske myndigheders behandling af oplysninger i forbindelse med disse systemer.

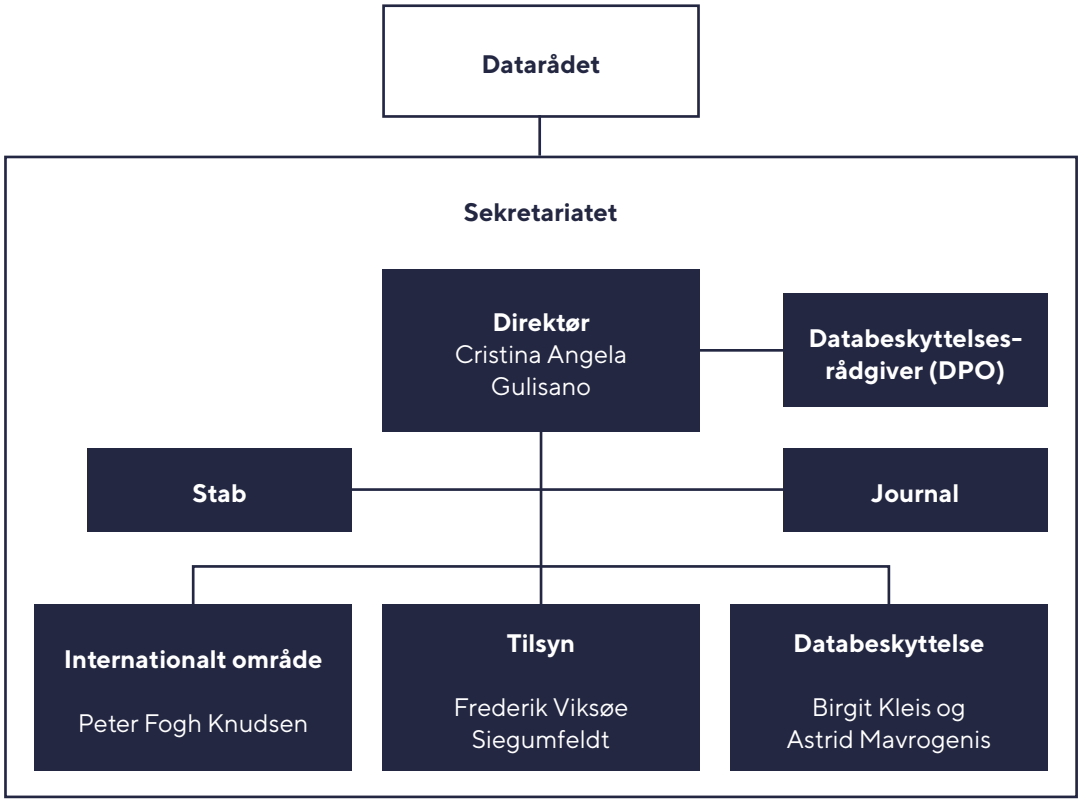
Datatilsynets vision er, at myndigheder og private kender og overholder reglerne for behandling af personoplysninger, og at borgerne kender og kan bruge deres rettigheder. Datatilsynet søger at gøre dette muligt og lettere gennem synlighed, information, dialog og kontrol.

Det er endvidere Datatilsynets mission at rådgive om registrering, videregivelse og anden behandling af personoplysninger og føre tilsyn med, at myndigheder, virksomheder og andre dataansvarlige overholder reglerne på området.

Datatilsynets organisation

Datatilsynet består af et råd – Datarådet – og et sekretariat. Datatilsynet udøver sine funktioner i fuld uafhængighed. Datatilsynet har en finanslovsmæssig og en vis personalemæssig tilknytning til Justitsministeriet.

Datatilsynets afgørelser er endelige og kan ikke indbringes for anden administrativ myndighed. Datatilsynets afgørelser kan indbringes for domstolene. Datatilsynet er en del af den offentlige forvaltning og er dermed i forbindelse med sin virksomhed omfattet af den regulering, der gælder for forvaltningsmyndigheder. Det vil bl.a. sige offentlighedsloven og forvaltningsloven. Datatilsynet er derfor undergivet sædvanlig kontrol af Folketingets Ombudsmand.



Datarådet

I forbindelse med overgangen til nyt retsgrundlag blev der efter 25. maj 2018 nedsat et nyt Dataråd. Justitsministeren nedsætter Datarådet, som består af 1 formand, der skal være højesteretsdommer eller landsdommer, og af 7 andre medlemmer. Erhvervsministeren og ministeren for offentlig innovation udnævner hver 1 af de 7 andre medlemmer. Datarådet træffer primært afgørelse i sager af principiel karakter. Datarådets forretningsorden, der fastsættes af rådet selv, blev vedtaget på Datarådets første møde den 20. december 2018. Datarådet udnævnes for 4 år. Der kan ske genudpegning to gange. Udpegelsen sker på baggrund af medlemmernes faglige kvalifikationer.

Datarådets medlemmer (pr. 31. december 2019)

Formand, højesteretsdommer Kristian Korfits Nielsen
Professor, dr.jur. Henrik Udsen
Kommunaldirektør, Jesper Thyrring Møller
Advokat, Pia Kirstine Voldmester
Formand for Rådet for Digital Sikkerhed, Henning Mortensen
Sundhedsdirektør, Svend Hartling
Advokat, Martin von Haller Grønbæk
Vicedirektør, Mette Raun Fjordside

Sekretariatet

Sekretariatet beskæftiger omkring 66 medarbejdere (jurister, it-sikkerhedskonsulenter, kontorpersonale og studenter m.fl.) og varetager Datatilsynets daglige drift under ledelse af en direktør, cand. jur. Cristina Angela Gulisano. De bevillingsmæssige forhold mv. fremgår af Datatilsynets årsrapport for 2019.

Datatilsynets medarbejdere (pr. 31. december 2019)

Direktør, cand.jur. Cristina Angela Gulisano
Kommitteret, cand.jur. Birgit Kleis
Kontorchef, cand.jur. Astrid Mavrogenis
Kontorchef, cand.jur. Frederik Viksøe Siegumfeldt
Kontorchef, cand.jur. Peter Fogh Knudsen
Chefkonsulent, cand.jur. Anders Aagaard
Chefkonsulent, cand.jur. Karina Kok Sanderhoff
Chefkonsulent, cand.jur. Katrine Valbjørn Trebbien
Chefkonsulent, cand.jur. Kia Hee Gade
Chefkonsulent, cand.jur. Mia Staal Klintrup
Chefkonsulent, cand.jur. Susanne Richter
Specialkonsulent, cand.jur. Eva Volfing
Specialkonsulent, cand.jur. Makar Juhl Holst
Specialkonsulent, cand.jur. Sarah Hersom Kublitz
Stabsmedarbejder, cand.soc. Anne Bech (Orlov)
Stabsmedarbejder, cand.scient.adm. Sofie Astrup Malm
Kommunikationskonsulent, cand. mag. Anders Due
It-sikkerhedskonsulent, cand. jur. Allan Frank
It-sikkerhedskonsulent, diplomingeniør Erik Stig Christensen
It-sikkerhedskonsulent, cand.polyt. Julia Ilu Sommer
It-sikkerhedskonsulent, cand.polyt. Marcus Vinther Tanghøj
It-sikkerhedskonsulent, Ph.d., Martin Mehl Lauridsen Schadegg
It-sikkerhedskonsulent, politibetjent Poul Erik Høj Weidick
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
It-ansvarlig og It-sikkerhedskoordinator, maskinmester Per Mortensen
Kontorfuldmægtig Anne-Marie Müller
Kontorfuldmægtig Helle Jensen
Kontorfuldmægtig Lisbeth Søndberg Liljekrans (Vikar)
Kontorfuldmægtig Mette-Maj Aner Leilund
Kontorfuldmægtig Pernille Jensen
Assistent Camilla Knutsdotter Hallingby
Fuldmægtig, cand.jur. Andreas Arnsel
Fuldmægtig, cand.jur. Andreas Droob Kristensen
Fuldmægtig, cand.jur. Anette Borring-Møller
Fuldmægtig, cand.jur. Astrid Malte Ivens De Carvalho
Fuldmægtig, cand.jur. Betty Nielsen Husted
Fuldmægtig, cand.jur. Camilla Andersen
Fuldmægtig, cand.jur. Camilla Meineche
Fuldmægtig, cand.jur. Cecilie Spendrup Slagslunde

Fuldmægtig, cand.jur. Charlotte Nørtoft Poulsen
Fuldmægtig, cand.jur. Christine Børglum Sørensen
Fuldmægtig, cand.jur. Ditte Malene Kieler Koefoed
Fuldmægtig, cand.jur. Eva Poskute Winther
Fuldmægtig, cand.jur. Kasper Viftrup
Fuldmægtig, cand.jur. Kenni Elm Olsen
Fuldmægtig, cand.jur. Lea Bruun
Fuldmægtig, cand.jur. Lise Fredskov
Fuldmægtig, cand.jur. Mads Nordstrøm Kjær
Fuldmægtig, cand.jur. Marie Raahauge Christiansen
Fuldmægtig, cand.jur. Mikkel Brandenborg Stenalt
Fuldmægtig, cand.jur. Neda Marica
Fuldmægtig, cand.jur. Nicklas Irgens Villien
Fuldmægtig, cand.jur. Nikolaj Niss Rohde
Fuldmægtig, cand.jur. Nina Donovan Anker (Orlov)
Fuldmægtig, cand.jur. Pernille Ørum Walther
Fuldmægtig, cand.jur. Rasmus Arslev
Fuldmægtig, cand.jur. Rasmus Møller Jakobsen
Fuldmægtig, cand.jur. Sara Koch Jørgensen (Orlov)
Fuldmægtig, cand.jur. Sara Thorning Hansen
Fuldmægtig, cand.jur. Sofie Eberhard Bendtz
Fuldmægtig, cand.jur. Susanne Dige Nielsen
Fuldmægtig, cand.jur. Victoria Lenchler-Huebertz
Fuldmægtig, cand.jur. Viktor Herskind Ingemann
Fuldmægtig, cand.jur. Zenia Dinesen
Stud.jur. Asta Sprogøe Biilmann
Stud.jur. Freja Gudmundsson
Stud.jur. Amalie Pilgaard Stubdrup
Stud.jur. Pernille Elisabeth Jensen
Stud.jur. Vincent Ollantay Murillo Valdez
Stud.mag. Natascha Helverskov Jørgensen

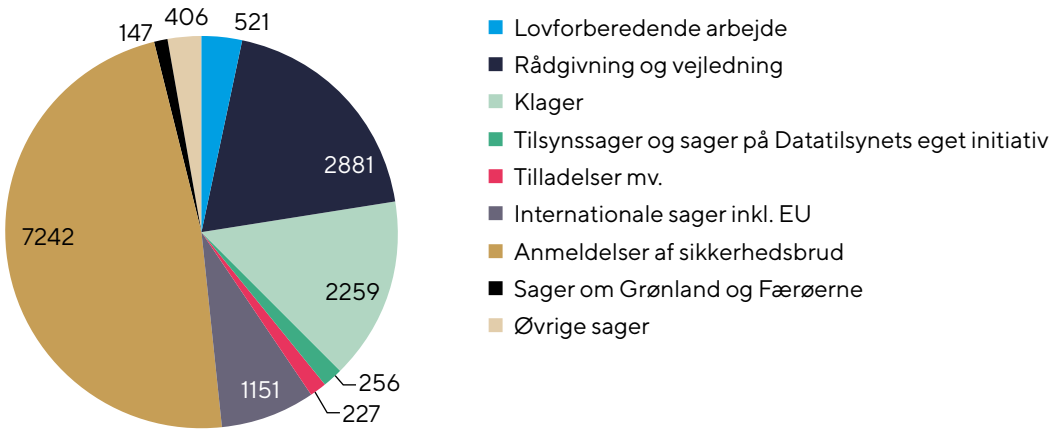
Året i tal

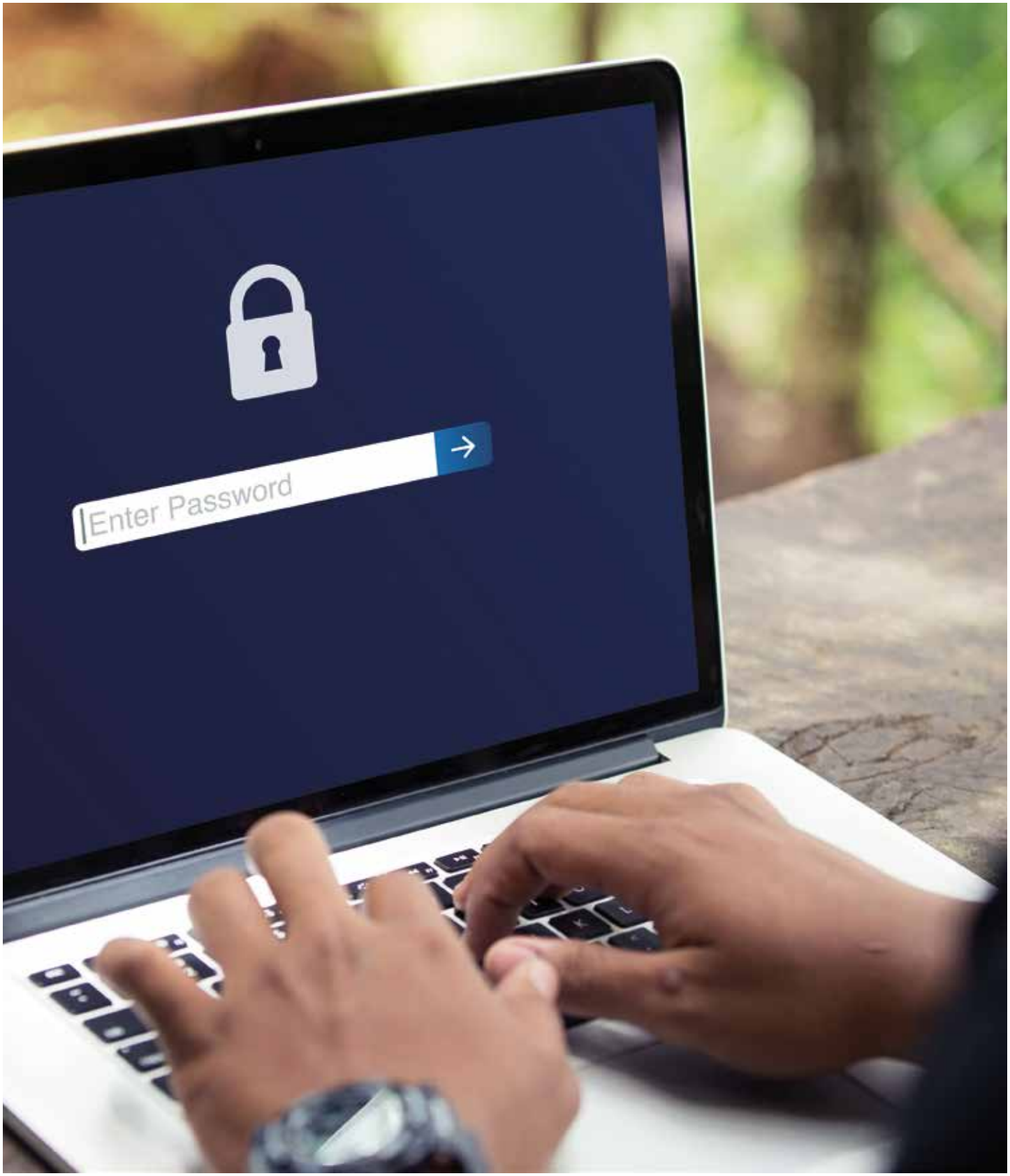
Nedenfor er oplysninger om antallet af nye sager, som er oprettet i Datatilsynets journalsystem i 2019. En del af Datatilsynets sagsbehandling er imidlertid en fortsættelse af eksisterende sager. Dette er for eksempel tilfældet, når en anmeldelse ændres, eller en tilladelse forlænges. Disse sager er af praktiske årsager ikke medtaget i statistikken.

Datatilsynet registrerede i alt 15.090 nye sager i 2019.

Fordelingen af oprettede sager i 2019	
Lovforberedende arbejde	521
Rådgivning og vejledning	2881
Klager	2259
Tilsynssager og sager på Datatilsynets eget initiativ	256
Tilladelser mv.	227
Internationale sager inkl. EU	1151
Anmeldelser af brud på persondatasikkerheden	7242
Sager om Grønland og Færøerne	147
Øvrige sager	406
Sager i alt	15090

Oprettede sager i 2019

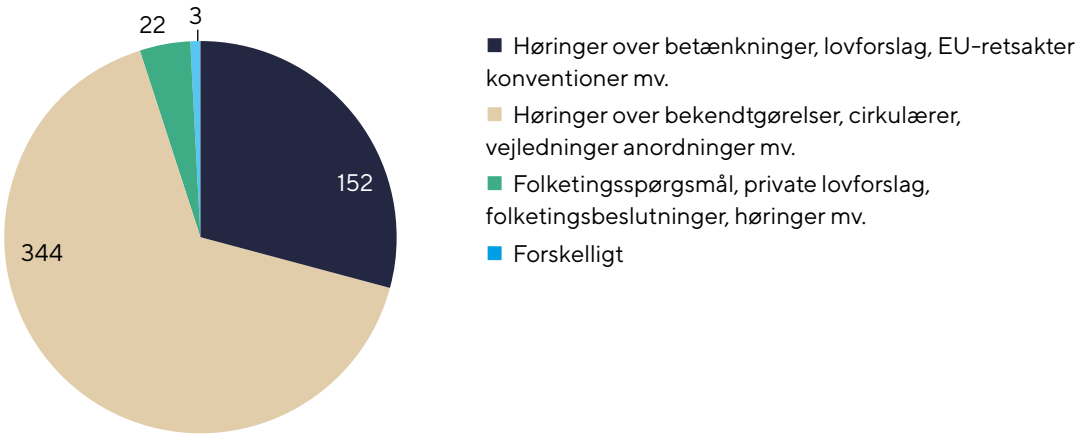



Enter Password

Lovforberedende arbejde, folketingsspørgsmål mv.

Sager vedrørende lovforberedende arbejde, folketingsspørgsmål o. lign.	
Høringer over betænkninger, lovforslag, EU-retsakter, konventioner mv.	152
Høringer over bekendtgørelser, cirkulærer, vejledninger, anordninger mv.	344
Folketingsspørgsmål, private lovforslag, folketingsbeslutninger, høringer mv.	22
Forskelligt	3
Sager i alt	521

Sager vedrørende lovforberedende arbejde, folketingsspørgsmål o. lign.



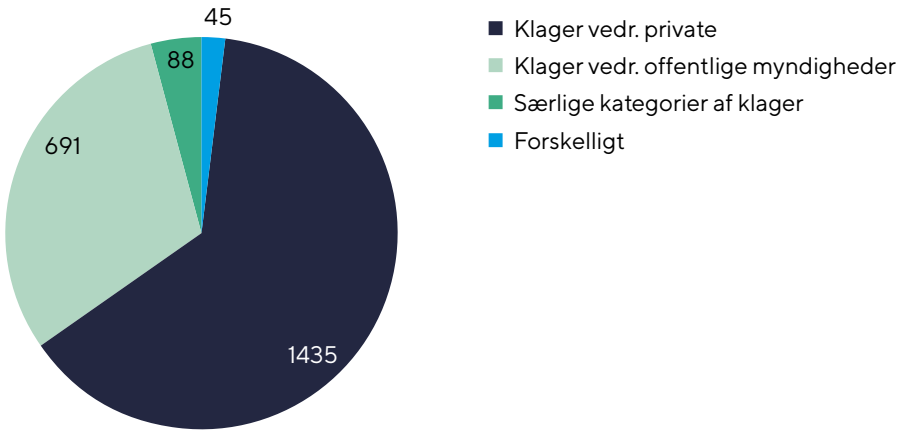
Klager

Klagesager	
Klager vedr. private	1435
Klager vedr. offentlige myndigheder	691
Særlige kategorier af klager	88
Forskelligt	45
I alt	2259

Med til klagesager hører også sager fra IMI, som er en større gruppe sager, der behandles særskilt, jf. tabellen om Internationale sager. Indre Markeds-Informationssystemet (IMI) er et informationssystem, som overordnet har til formål at lette europæiske myndigheders grænseoverskridende samarbejde og sagsbehandling i henhold til en given EU-retsakt. Datatilsynet er udpeget som tilsynsmyndighed i relation til behandlingen af personoplysninger i den danske del af systemet

Særlige kategorier af klager dækker over klager over kreditoplysningsbureauer.

Klagesager



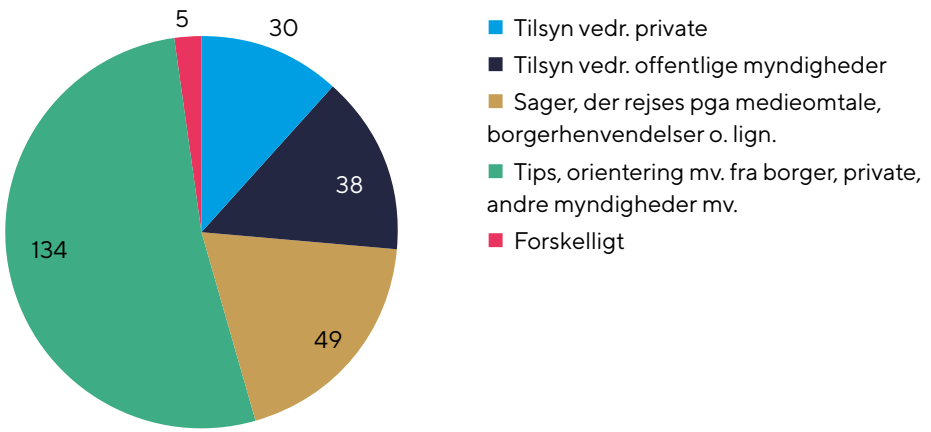
Tilsynssager og sager på Datatilsynets eget initiativ

Tilsynssager og sager på Datatilsynets eget initiativ	
Tilsyn vedr. private	30
Tilsyn vedr. offentlige myndigheder	38
Sager, der rejses pga. medieomtale, borgerhenvendelse og lign.	49
Tips, orientering mv. fra borgere, private, andre myndigheder mv.	134
Forskelligt (f.eks. årsplan, forretningsgange, processer mv.)	5
I alt	256

Med til tilsynssager hører også anmeldelser af brud på persondatasikkerheden, som er en større gruppe sager, der behandles særskilt.

De 49 sager, der rejses pga. medieomtale, borgerhenvendelse og lign. fordeler sig på 37 sager vedrørende private og 12 sager vedrørende offentlige myndigheder.

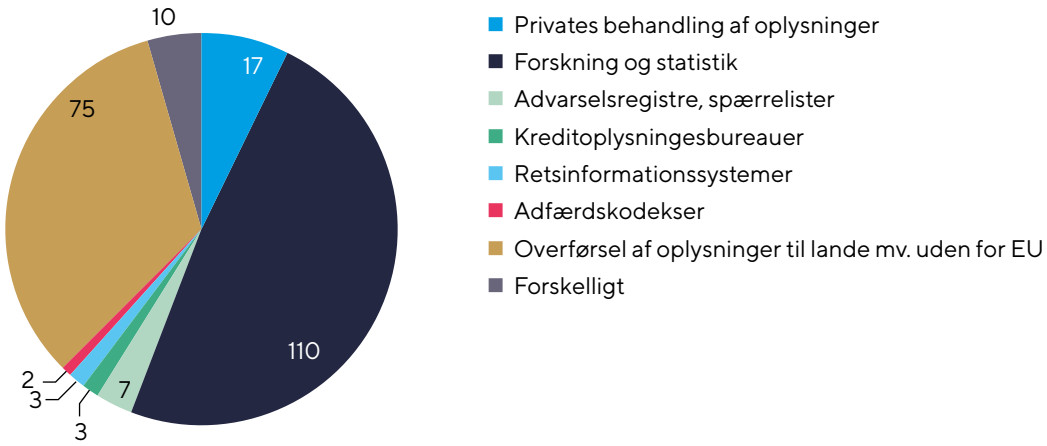
Tilsynssager og sager på Datatilsynets eget initiativ



Tilladelser mv.

Tilladelser mv.	
Privates behandling af oplysninger	17
Forskning og statistik	110
Advarselsregistre, spærrelister	7
Kreditoplysningsbureauer	3
Retsinformationssystemer	3
Adfærdskodekser	2
Overførsel af oplysninger til lande mv. uden for EU	75
Forskelligt	10
I alt	227

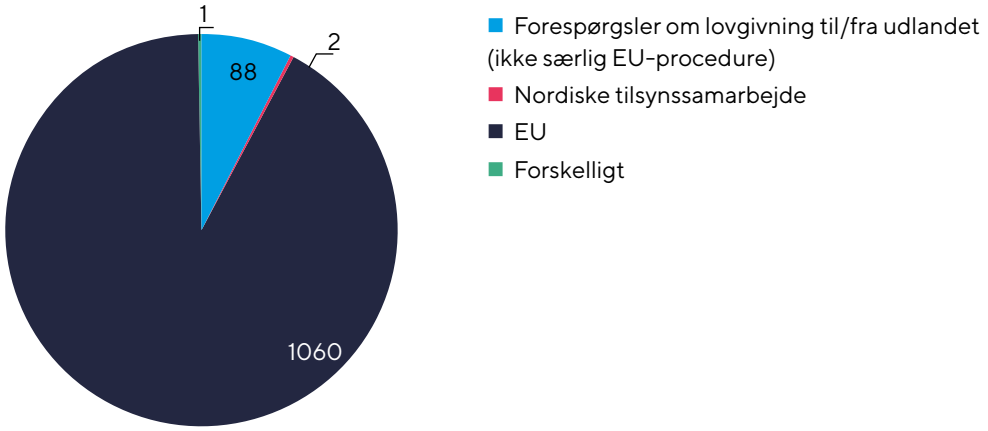
Tilladelser mv.



Internationale sager

Internationale sager	
Forespørgsler om lovgivning til/fra udlandet (ikke særlig EU-procedure)	88
Nordiske tilsynssamarbejde	2
EU	1060
Forskelligt	1
I alt	1151

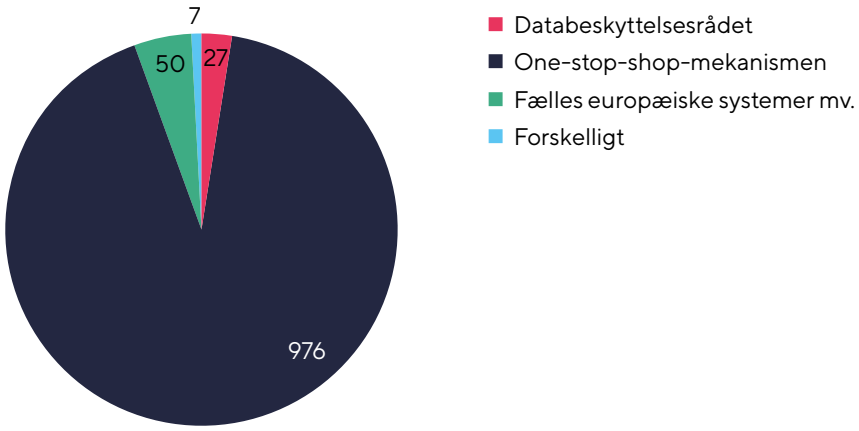
Internationale sager



De 1060 sager om EU fordeler sig på forskellige sagstyper, jf. tabellen nedenfor.

Fordelingen af EU sager	
Databeskyttelsesrådet	27
One-stop-shop-mekanismen	976
Fælles europæiske systemer mv.	50
Forskelligt	7
I alt	1060

EU sager



Rådgivning og vejledning mv.

Det er efter Datatilsynets opfattelse afgørende for at sikre en høj beskyttelse af danskernes personoplysninger – og derfor også tilsynets 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 samtidig Datatilsynets mission at rådgive om registrering, videregivelse og anden behandling af personoplysninger og føre tilsyn med, at myndigheder, virksomheder og andre dataansvarlige overholder reglerne på området.

Datatilsynets forpligtelse til at yde en serviceorienteret og anvendelig rådgivning er imidlertid ikke kun en del af tilsynets vision og mission. Det følger således også direkte af databeskyttelsesforordningen. Dette sikres bl.a. gennem de mange telefoniske og skriftlige forespørgsler om reglerne, som Datatilsynet hver dag håndterer, ligesom tilsynet holder mange møder med bl.a. interesse- og brancheorganisationer, men også enkeltstående dataansvarlige og databehandlere, hvis der måtte være behov herfor.

Datatilsynet har i 2019 offentliggjort 11 nye nationale vejledninger, som supplerer de 13 vejledninger, som tilsynet offentliggjorde i 2017 og 2018, ligesom der løbende er blevet udarbejdet mindre tekster under forskellige databeskyttelsesretlige emner. Datatilsynet har endvidere udgivet en podcast med 15 episoder om databeskyttelsesforordningen, der skal hjælpe små og mellemstore virksomheder med at få et overblik over reglerne, ligesom tilsynet har offentliggjort 10 små animerede videoer om databeskyttelsesreglerne, der er målrettet danskerne generelt. Datatilsynet yder også en aktiv indsats på dette område i europæiske sammenhænge. Tilsynet har i 2019 – i regi af Det Europæiske Databeskyttelsesråd – bidraget til udarbejdelsen af to nye fælleseuropæiske vejledninger mv. om forordningen. Alle de nævnte vejledninger – nationale og fælleseuropæiske – kan sammen med en række praktisk anvendelige skabeloner til f. eks. opfyldelse af oplysningspligten findes på Datatilsynets hjemmeside. Endvidere er der udarbejdet og offentliggjort tre kvartalsvise statistikker og gennemgange af de indkomne anmeldelser af brud på persondatasikkerheden. Sidste kvartalsoversigt, der dækker perioden oktober – december 2019, er offentliggjort primo februar 2020.

Datatilsynet prioriterer endvidere at deltage med bl.a. indlæg på konferencer, seminarer mv. for at informere om databeskyttelsesreglerne og tilsynets praksis, 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 2019 deltaget med 45 oplæg mv. på konferencer, seminarer mv. I juni 2019 deltog Datatilsynet for første gang med oplæg og en stand med diverse aktiviteter på Folkemødet på Bornholm, ligesom tilsynet også som noget nyt i år havde en stand på Ungdommens Folkemøde i september 2019, hvor børn og unge kunne komme forbi til quiz, debat og workshops, og hvor de kunne høre mere om, hvilke rettigheder de har. Herudover var Datatilsynet aktiv med oplæg og en stand på både Digitaliseringsmessen i Odense den 3. oktober 2019, der henvendte sig til den offentlige sektor, og Digitaliseringsmessen for erhvervslivet, der blev afholdt dagen efter samme sted.

Podcast mv. om databeskyttelsesforordningen

I løbet af 2019 udgav Datatilsynet en række videoer og podcastepisoder, som formidlede forskellige emner inden for databeskyttelse.

Podcasten bestod af 15 episoder, som især var målrettet små og mellemstore virksomheder. Hver episode tog fat på et afgrænset emne, som var relevant for målgruppen - eksempelvis samtykke, brug af billeder og sletning. Episoderne udfoldede sig typisk som en dialog på 10-15 minutter mellem to af Datatilsynets medarbejdere, og det tilstræbtes, at formatet var mindre formelt og mere rigt på konkrete eksempler end den skriftlige vejledning, Datatilsynet ellers stiller til rådighed på hjemmesiden. Podcasten var med andre ord tænkt som et alternativ til de andre informationskanaler, der især skulle gøre mindre dataansvarlige opmærksomme på reglerne og opfordre dem til at søge nærmere vejledning efter behov.

Initiativet blev positivt modtaget af målgruppen - og også af en række andre interesserede. Ved udgangen af 2019 var podcastepisoderne blevet afspillet mere end 28.000 gange.

Derudover producerede Datatilsynet 10 korte videoer i 2019. Videoerne er modsat podcastepisoderne rettet direkte mod borgere og har særligt fokus på de rettigheder, man har efter de databeskyttelsesretlige regler. Der var endvidere nogle af filmene, hvis primære formål er at skabe opmærksomhed om emnet – f.eks. en kort film, der gennemgår de data, der potentielt indsamles om den enkelte borger i løbet af en almindelig dag. Filmene blev gjort tilgængelige på Datatilsynets hjemmeside og LinkedIn-profil og fik ligesom podcasten en positiv modtagelse.

Deltagelse på Folkemøder

I 2019 deltog Datatilsynet for første gang på Folkemødet på Bornholm og Ungdommens Folkemøde i Valby. Målet med begge aktiviteter var at udbrede kendskabet til reglerne om databeskyttelse over for nogle målgrupper, som ikke nødvendigvis opsøger informationerne på fx Datatilsynets hjemmeside.

På Folkemødet i Allinge havde Datatilsynet et telt, hvor der både var planlagte arrangementer og løbende aktiviteter. Der var bl.a. flere events, hvor der blev aflivet myter om databeskyttelsesforordningen på scenen. Der var et arrangement, hvor Datatilsynet diskuterede grænsefladerne mellem markedsføringsretten og databeskyttelsesretten med Forbrugerombudsmanden, og der var en meget velbesøgt event med freestyle-rap om GDPR – improviseret efter input fra publikum. GDPR er den engelske forkortelse for forordningen (General Data Protection Regulation).

Ud over de fastsatte aktiviteter var der løbende gennem dagene mulighed for, at såvel borgere som dataansvarlige kunne kigge forbi og stille spørgsmål, teste deres viden om reglerne og få en snak med Datatilsynets eksperter. Der var også en quiz særligt målrettet større børn, der blev taget i brug, når grupper af skoleelever kom forbi.

På Ungdommens Folkemøde i Valbyparken var der tilsvarende både nogle fastsatte events og løbende aktiviteter og quizzer. Derudover var der mange af de unge, der besøgte Datatilsynets telt, som også interviewede medarbejderne fra Datatilsynet til brug for skoleopgaver.

Offentliggørelse af billeder på internettet

Offentliggørelse af billeder på internettet af genkendelige personer betragtes som en behandling af personoplysninger. Et billede med identificerbare personer udgør således oplysninger om disse personer, og de databeskyttelsesretlige regler skal derfor være opfyldt.

I 2019 ændrede Datatilsynet sin tidligere praksis fra 2002 for offentliggørelse af billeder på internettet, så det ikke længere er afgørende, om et billede er et situations- eller et portrætbillede. Der lægges derimod vægt på formålet og billedets karakter mere generelt.

Situationsbilleder var defineret som billeder, hvor en aktivitet eller situation er det egentlige formål med billedet, som f.eks. billeder af publikum til en koncert. Modsætningen hertil var portrætbilleder, hvor formålet er at afbilde en eller flere bestemte personer. Efter den tidligere praksis kunne situationsbilleder normalt offentliggøres på internettet, uden at personerne på billedet havde givet lov til det, mens det som udgangspunkt krævede et samtykke at offentliggøre portrætbilleder.

Datatilsynet genovervejede sin praksis, fordi især afgrænsningen mellem situations- og portrætbilleder i praksis voldte problemer. Tilsynet lagde også vægt på den teknologiske og samfundsmæssige udvikling, der var sket siden 2002. Billeder af identificerbare personer offentliggøres således i dag i vidt omfang på hjemmesider og på sociale medier. Det er Datatilsynets opfattelse, at mange mennesker opfatter dette som ganske uproblematisk, så længe der er tale om, at der sker offentliggørelse af helt harmløse billeder af dem på internettet.

På den baggrund – og efter drøftelse i Datarådet – besluttede Datatilsynet at ændre sin praksis. Datatilsynet tilkendegav således, at tilsynet ikke længere vil sondre mellem situations- og portrætbilleder, og at det fremadrettet vil være tilsynets opfattelse, at spørgsmålet, om der vil kunne offentliggøres et billede på internettet – uden samtykke fra den berørte person – beror på en helhedsvurdering af billedet og formålet med offentliggørelsen. Her skal man især forholde sig til, om personen på billedet med rimelighed kan føle sig udstillet, udnyttet eller krænket.

Anvendelse af fingeraftryk i forbindelse med ansattes komme- og gåtider

Datatilsynet behandlede i 2019 en henvendelse fra en advokat, som på vegne af en klient ønskede tilsynets stillingtagen til, om behandling af oplysninger om ansattes fingeraftryk (templates) til brug for registrering af komme- og gåtider som led i kontrol af de ansattes arbejdstid kan anses for nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra f.

Datatilsynet udtalte – efter sagen havde været behandlet i Datarådet – at forbuddet mod behandling af oplysninger om en ansats fingeraftryk, herunder templates, i forordningens artikel 9, stk. 1, til brug for registrering af komme- og gåtider ikke kan fraviges med henvisning til databeskyttelsesforordningens artikel 9, stk. 2, litra f (retskrav), når behandling sker som led i kontrol af en ansats arbejdstid, selvom en ansats krav på (retmæssig) løn – og arbejdsgiverens krav på alene at udbetale den løn, som den ansatte er berettiget til – kan anses for at udgøre et retskrav.

Baggrunden herfor var, at Datatilsynet vurderede, at kravet om nødvendighed i databeskyttelsesforordningens artikel 9, stk. 2, litra f, ikke er opfyldt.

Kravet om nødvendighed indebærer, at behandling skal være mere end blot en praktisk måde at opfylde formålet på, ligesom kravet om nødvendighed indebærer, at formålet objektivt set ikke med rimelighed må kunne opnås ved mindre indgribende midler.

Kontrol af ansattes komme- og gåtider kan efter Datatilsynets opfattelse foretages med mindre indgribende midler, som ikke nødvendiggør behandling af følsomme oplysninger. Det vil f.eks. være muligt at kontrollere, hvornår en ansat er kommet og gået fra arbejdspladsen ved at anvende adgangskort eller andre lignende foranstaltninger – eventuelt i kombination med andre foranstaltninger, herunder stikprøvekontroller eller manuel (personlig) kontrol ved indgangen.

Datatilsynet fandt endvidere anledning til at overveje, om behandling af ansattes fingeraftryk med henblik på at kontrollere komme- og gåtider som led i tidskontrol vil kunne ske på baggrund af et samtykke fra den ansatte.

Efter Datatilsynets opfattelse er det tvivlsomt – som følge af det afhængighedsforhold, der er mellem en arbejdsgiver og en ansat – om en ansat kan afvise at give en arbejdsgiver sit samtykke til behandlingen af oplysninger om vedkommendes fingeraftryk med henblik på at kontrollere komme- og gåtider uden frygt eller reel risiko for, at afvisningen vil være til skade for den pågældende eller uden at føle et vist pres.

I lyset heraf vurderede Datatilsynet, at en ansats samtykke til, at en arbejdsgiver kan behandle oplysninger om vedkommendes fingeraftryk i forbindelse med tidskontrol, som det klare udgangspunkt ikke kan anses for at være givet frivilligt og dermed udgøre et gyldigt behandlingsgrundlag.

Datatilsynet kunne dog ikke afvise, at der kan foreligge særlige omstændigheder, hvorunder et samtykke kan anses for frivilligt, ligesom tilsynet i besvarelsen ikke tog stilling til, om behandlingen vil kunne ske på baggrund af andre bestemmelser i databeskyttelsesforordningen eller databeskyttelsesloven.

Sletning af personoplysninger

I januar 2019 offentliggjorde Datatilsynet en vejledende tekst om sletning af personoplysninger.

Teksten skal understøtte den dataansvarliges arbejde i forhold til at sikre den fornødne sletning af personoplysninger i sine systemer. Teksten vejleder derfor både om slettefrister, procedure for sletning, opfølgning på sletteprocedurer, "retten til at blive glemt" og eventuel sletning i backup.

Teksten anviser endvidere 6 konkrete områder (gode råd), som den dataansvarlige skal forholde sig til:

1. Tag stilling til slettefrister for de forskellige personoplysninger, der behandles, med baggrund i behandlingens formål.
2. Dokumenter de fastsatte slettefrister.
3. Vær opmærksom på lovmæssige krav, som kan påvirke slettefristerne.
4. Fastlæg og dokumenter en procedure for sletning.
5. Fastlæg og dokumenter en procedure for opfølgning på, at sletning forløber som forventet.
6. Tænk sletning ind i behandlingen, så behandlingen indrettes således, at eventuelle forskellige slettefrister kan opfyldes på en hensigtsmæssig måde i forhold til systemet, der anvendes.

Skabelon til databehandleraftale – ny status

Efter databeskyttelsesforordningen har Datatilsynet mulighed for at vedtage såkaldte standardkontraktbestemmelser, som organisationer mv. kan anvende, når de skal indgå en databehandleraftale. Formålet hermed er at bidrage til at sikre, at dataansvarlige og databehandlere lever op til de krav, der stilles til dem i databeskyttelsesforordningen.

Vedtagelsen af sådanne standardkontraktbestemmelser skal – i overensstemmelse med den såkaldte sammenhængsmekanisme, der følger af forordningen – ske i samarbejde med de øvrige EU-landes tilsynsmyndigheder for at sikre en ensartet anvendelse af databeskyttelsesreglerne.

Med henblik på at vedtage sådanne standardkontraktbestemmelser anmodede Datatilsynet i april 2019 om Det Europæiske Databeskyttelsesråds stillingtagen til en skabelon til en databehandleraftale, som tilsynet havde anvendt siden 2018.

Det Europæiske Databeskyttelsesråd vedtog i juli 2019 en udtalelse, som indeholdt en række bemærkninger til Datatilsynets skabelon. Herefter fulgte en proces, som mundede ud i, at Datatilsynet i december 2019 – som det første og hidtil eneste EU-land – vedtog en revideret udgave af skabelonen som standardkontraktbestemmelser for databehandleraftaler.

Som det var tilfældet med Datatilsynets oprindelige skabelon, er det ikke et krav for organisationer mv. at benytte Datatilsynets standardkontraktbestemmelser for at overholde databeskyttelsesforordningens regler om databehandleraftaler.

Der er dog en væsentlig sikkerhed forbundet med brugen af standardkontraktbestemmelserne, hvis juridisk bindende status indebærer, at Datatilsynet – f.eks. i forbindelse med et tilsynsbesøg – ikke vil efterprøve det allerede fastsatte indhold af bestemmelserne.

Kontrol med databehandlere mv.

Når en dataansvarlig benytter sig af databehandlere, skal der indgås en aftale mellem den dataansvarlige og databehandleren om behandlingen af personoplysninger hos databehandleren (databehandleraftale). Den dataansvarlige skal endvidere efterfølgende kontrollere behandlingen af personoplysninger hos databehandleren.

Datatilsynet offentliggjorde i maj 2018 en ny vejledende tekst om tilsyn med databehandlere og underdatabehandlere. I teksten redegøres der for, hvorfor det er vigtigt, at en dataansvarlig løbende følger op på den behandling af personoplysninger, der sker hos databehandlere og eventuelle underdatabehandlere.

Som supplement til den vejledende tekst offentliggjorde Datatilsynet i februar 2019 en tekst med vejledende principper for placeringen af dataansvaret i forbindelse med, at en dataansvarlig virksomhed eller myndighed gør brug af konsulenter (herunder IT-konsulenter) og vikarer (fra fx vikarbureauer) til behandling af personoplysninger.

Med henblik på at styrke de dataansvarliges tilsyn med databehandlere udarbejdede Datatilsynet endvidere i samarbejde med Forenede Revisorer (FSR) en revisionserklæring. Erklæringen, der blev offentliggjort i februar 2019, kan enten anvendes som egentlig revisionserklæring eller fungere som inspiration ved tilsynet med databehandlere.

Vejledning om risikovurdering og risikostyring

Datatilsynet offentliggjorde i juni 2019 en ny vejledende tekst med operationelle råd om risikovurdering. Teksten blev udarbejdet i samarbejde med Rådet for Digital Sikkerhed.

Den vejledende tekst omhandler, hvordan man vurderer risici for de registrerede, når man behandler deres personoplysninger. Teksten henvender sig til alle, som behandler personoplysninger, og har særlig relevans i forhold til de foranstaltninger og andre tiltag, som skal iværksættes, da disse skal ske på baggrund af en risikovurdering.

Det er risikovurderingen, som bidrager til at skabe den røde tråd i arbejdet med at beskytte de personer, som virksomheder og myndigheder behandler oplysninger om. Risikovurderingen spiller således en central rolle i databeskyttelsesforordningen og databeskyttelsesloven.

Den vejledende tekst kan bruges som et rammeværk til at identificere risici og estimere sandsynligheden for, at risici udløser en sikkerhedshændelse, og hvad konsekvensen herved vil være. På den baggrund kan man vurdere risikoen, og iværksætte sikkerhedsforanstaltninger for at imødegå risikoen. Sikkerhedsforanstaltningerne kan f.eks. være instruktioner til medarbejderne i, hvordan de skal behandle personoplysninger eller tekniske installationer, som blokerer for skadelige sites eller opdager huller i de programmer, der behandler personoplysninger.

Den vejledende tekst kan hjælpe de dataansvarlige med inspiration til, hvordan de skal gennemføre risikovurderinger og dermed få grundlaget for sikker databehandling på plads.

Sikkerhed ved transmission af personoplysninger via SMS

Efter at have forelagt sagen for Datarådet offentliggjorde Datatilsynet i juli 2019 en tekst med vejledning om sikkerheden ved behandlinger af personoplysninger foretaget med SMS.

Overgangen fra persondataloven til databeskyttelsesforordningen indebærer, at de dataansvarlige i begge sektorer skal tænke persondatasikkerhed på en grundlæggende ny måde. Der er lagt op til en mere risikobaseret tilgang til, hvad der må anses som passende sikkerhed. Udgangspunktet efter forordningen er således, at behandling af personoplysninger er forbundet med risici for fysiske personers rettigheder og frihedsrettigheder, og at der skal etableres et sikkerhedsniveau, som passer til disse risici.

Det er i den forbindelse Datatilsynets opfattelse, at SMS er en både brugbar og god måde at give de registrerede påmindelser og kortere servicebeskeder på. Samtidig er det dog tilsynets vurdering, at transmission via SMS af følsomme oplysninger og oplysninger, som skal undergives fortrolighed, normalt indebærer en så betydelig risiko for de registreredes rettigheder og frihedsrettigheder, at de ikke bør sendes som SMS.

Der findes i dag brugbare alternativer til SMS ved transmission af følsomme oplysninger og oplysninger, som skal undergives fortrolighed. Datatilsynet skal endvidere opfordre de dataansvarlige til – mere aktivt – at begrænse indholdet af SMS-teksten mest muligt, jf. princippet om dataminimering, ligesom de dataansvarlige – der har mulighed for det – efter Datatilsynets opfattelse kan bruge NemSMS til at mindske risikobilledet for at sende SMS til en forkert modtager.

Sikkerhed ved beskeder til bibliotekslånere om bogreserveringer

Datatilsynet havde siden 2005 undtagelsesvist givet dispensation til, at de danske biblioteker kunne sende reserveringsmeddelelser om bøger ved brug af ikke-krypterede e-mails. Denne dispensation kunne Datatilsynet give efter den tidligere gældende sikkerhedsbekendtgørelse. Da databeskyttelsesforordningen den 25. maj 2018 trådte i kraft, bortfaldt persondataloven med tilhørende bekendtgørelser, herunder sikkerhedsbekendtgørelsen og Datatilsynets vejledning til sikkerhedsbekendtgørelsen.

Efter dialog med Danskernes Digitale Bibliotek fandt Datatilsynet i 2019, at der var grundlag for at tage fornyet stilling til spørgsmålet om, hvorvidt der skal ske kryptering af fremsendelser af elektroniske reserveringsmeddelelser, som indeholder titel og forfatter på det materiale, som en låner har reserveret.

Efter at sagen havde været forelagt Datarådet, kom Datatilsynet frem til, at der ikke var grundlag for at fastslå, at indholdet af reserveret materiale afspejler oplysninger om en potentiel låner i en sådan grad, at reserveringsmeddelelser skal krypteres. Tilsynet fandt i den forbindelse, at en eventuel adgang for uvedkommende til oplysninger om reserveret materiale som udgangspunkt indebærer en meget beskeden risiko for bibliotekslånernes rettigheder.

Datatilsynet lagde således bl.a. vægt på karakteren af meddelelserne og det potentielle indhold heraf. Tilsynet lagde i tilknytning hertil også vægt på, at Danskenes Digitale Bibliotek havde oplyst, at folkebibliotekerne – på baggrund af biblioteksloven – udvælger materiale med henblik på at opfylde folkebibliotekernes formål gennem kvalitet, alsidighed og aktualitet, og at folkebibliotekerne derfor ikke vil have kompromitterende og odiøst materiale.

Liste over obligatoriske konsekvensanalyser

Datatilsynet offentliggjorde i januar 2019 den godkendte liste over situationer hvor der altid skal laves en konsekvensanalyse i medfør af databeskyttelsesforordningens artikel 35, stk. 4.

Listen supplerer de situationer, hvor en dataansvarlig – i øvrigt – har pligt til at foretage en konsekvensanalyse, hvilket altid er tilfældet, når der sandsynligvis vil være en høj risiko for fysiske personers rettigheder og frihedsrettigheder i forbindelse med den dataansvarliges behandling af personoplysninger.

Listen skal udarbejdes af alle de nationale datatilsyn i EU-landene. Den beskriver de situationer, hvor det er obligatorisk at foretage konsekvensanalyser. Det Europæiske Databeskyttelsesråd kom med en udtalelse om listen, inden den blev offentliggjort.

Den danske liste – der blev godkendt uden bemærkninger – indeholder 8 typetilfælde, der er baseret på en vejledning fra Artikel 29-gruppen (nu Det Europæiske Databeskyttelsesråd) fra oktober 2017 om konsekvensanalyse vedrørende databeskyttelse (DPIA) mv, som fastslår, at en dataansvarlig i de fleste tilfælde skal overveje at udføre en DPIA, hvor to af nogle givne kriterier er opfyldt, men at dette også – i nogle tilfælde – kan overvejes for behandlinger, der alene opfylder et af kriterierne.

Listen fra Datatilsynet supplerer og specificerer vejledningen yderligere, og det er væsentligt at fastslå, at den ikke er en udtømmende liste over de tilfælde, hvor der skal udarbejdes en DPIA.

De 8 tilfælde, hvor behandlingsaktiviteter sandsynligvis altid vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og der derfor skal udarbejdes en DPIA er:

1. Behandling af biometriske data med det formål entydigt at identificere en fysisk person i sammenhæng med mindst et yderligere kriterie fra Artikel 29-gruppens retningslinjer.
2. Behandling af genetiske data i sammenhæng med mindst et yderligere kriterie fra Artikel 29-gruppens retningslinjer.
3. Behandling af lokationsdata i sammenhæng med mindst et yderligere kriterie fra Artikel 29-gruppens retningslinjer.
4. Behandling ved brug af nye teknologier i sammenhæng med mindst et yderligere kriterie fra Artikel 29-gruppens retningslinjer.
5. Behandling der fører til afgørelser om en fysisk persons rettigheder til et produkt, en service, en potentiel mulighed eller begunstigelse, der er baseret på en hvilken som helst form for automatiseret afgørelse (herunder profilering).
6. Behandling der omfatter profilering af fysiske personer i stor skala, sådan som dette er defineret i Artikel 29-gruppens retningslinjer.
7. Behandling af personoplysninger om sårbare personer eller hvor der er tale om behandling af følsomme oplysninger (særlige kategorier) og hvor, der benyttes profilering eller andre former for automatiserede afgørelser.
8. Behandlinger hvor et brud på persondatasikkerheden kan have en direkte effekt på en persons fysiske helbred eller på sikkerheden for en fysisk person.

Behandling af følsomme personoplysninger

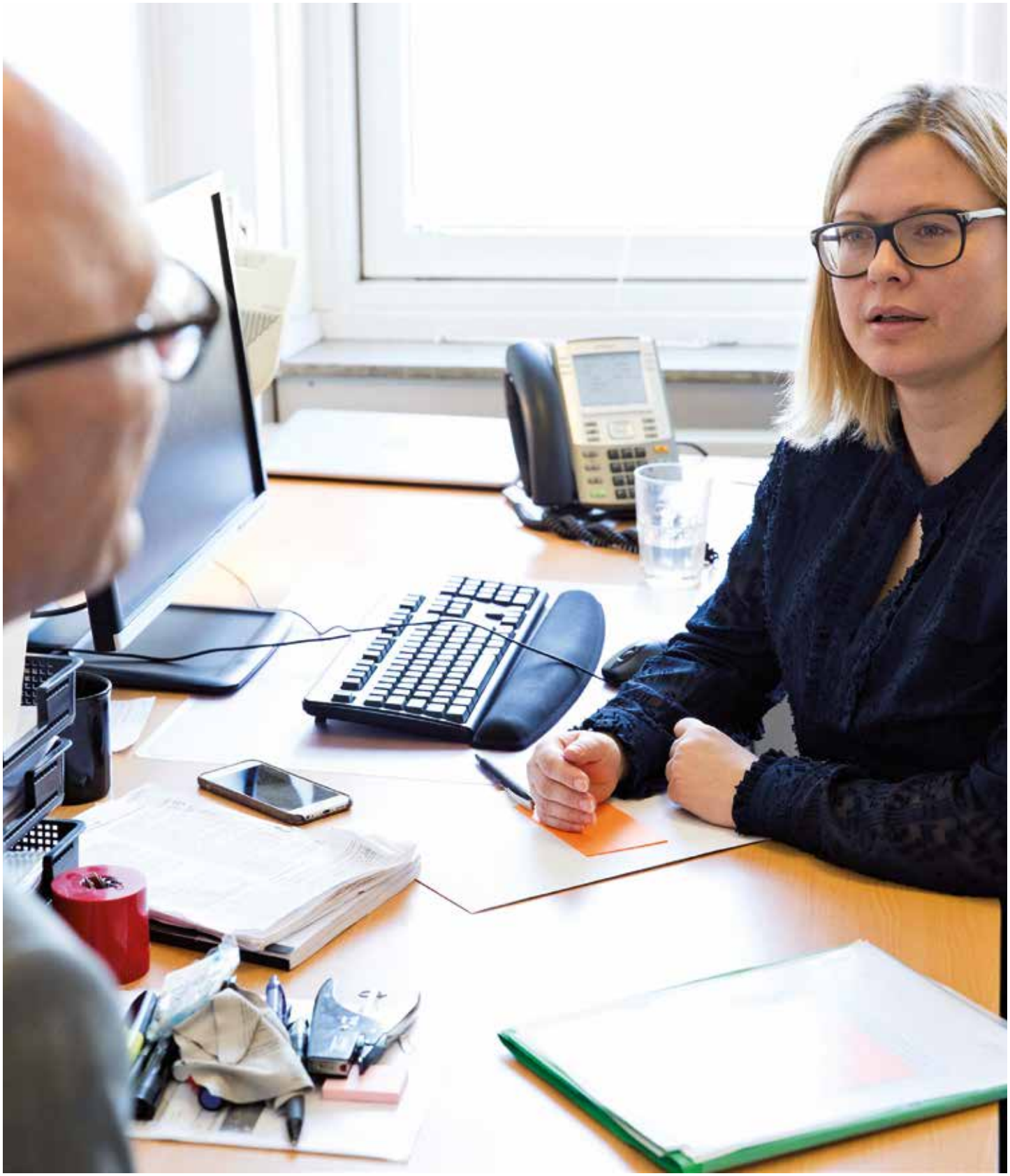
I november 2019 offentliggjorde Datatilsynet sin reviderede opfattelse af grundlaget for behandling af følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 9.

Det havde hidtil været Datatilsynets opfattelse, at dataansvarlige, som behandlede følsomme oplysninger – foruden de grundlæggende principper for behandling af personoplysninger i databeskyttelsesforordningens artikel 5 – alene skulle finde et behandlingsgrundlag i de bestemmelser, der specifikt omhandlede behandlingen heraf, dvs. reglerne i forordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører artikel 9.

På baggrund af bl.a. flere EU-tekster, herunder vejledninger fra Det Europæiske Databeskyttelsesråd (EDPB) og domme afsagt af EU-Domstolen, vurderede Datatilsynet imidlertid, at det ikke længere ville være muligt at opretholde denne retsopfattelse.

Fremadrettet vil det derfor være Datatilsynets opfattelse, at dataansvarlige, som behandler følsomme oplysninger omfattet af forbuddet mod behandling i databeskyttelsesforordningens artikel 9, stk. 1, skal kunne identificere en undtagelse til dette forbud i enten forordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører forordningens artikel 9, og et lovligt grundlag for behandling i forordningens artikel 6. Hertil kommer principperne for behandling af personoplysninger i databeskyttelsesforordningens artikel 5, der altid skal være opfyldt.

Som følge af den højere integritetsbeskyttelse, der i forvejen følger af undtagelserne i databeskyttelsesforordningens artikel 9, stk. 2, er det dog Datatilsynets vurdering, at betingelserne i forordningens artikel 6 sædvanligvis vil være opfyldt, hvis der kan identificeres en undtagelse til forbuddet i forordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører forordningens artikel 9. På Datatilsynets hjemmeside kan man finde et notat, der nærmere gennemgår baggrunden for den ændrede opfattelse og konsekvenserne af ændringen.



Høringer over lovforslag mv.

Datatilsynet registrerede 521 sager i 2019 vedrørende høringer over lovforslag mv.

Datatilsynet forholder sig i sine udtalelser til de eventuelle databeskyttelsesretlige problemstillinger i de 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 databeskyttelsesreglerne udøver sine funktioner i fuld uafhængighed. Datatilsynet prioriterer denne opgave højt.

Der skal efter databeskyttelseslovens § 28 indhentes en udtalelse fra Datatilsynet ved udarbejdelse af lovforslag, bekendtgørelser, cirkulærer eller lign. generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger.

Lovforslag om en aktiv beskæftigelsesindsats

Datatilsynet afgav i starten af 2019 høringssvar til et udkast til forslag til lov om en aktiv beskæftigelsesindsats. På baggrund af lovforslagets betydelige omfang afgrænsede Datatilsynets sit høringssvar til de områder, der – efter oplysning fra Styrelsen for Arbejdsmarked og Rekruttering (STAR) – omfattede behandling af personoplysninger. I den forbindelse havde Datatilsynet en række bemærkninger til enkelte dele af lovforslaget, herunder om dataansvaret for behandling af personoplysninger på Jobnet og det fælles it-baserede datagrundlag.

Efterfølgende blev Datatilsynet via bl.a. presseomtale opmærksom på, at der var dele af lovforslaget, som vedrørte behandling af personoplysninger, men som tilsynet ikke havde taget stilling til i forbindelse med høringen. På den baggrund besluttede Datatilsynet at foretage en fornyet vurdering af lovforslaget og den vedtagne lov. Datatilsynet konstaterede i den forbindelse, at de omhandlede dele af lovforslaget ikke fremgik af det udkast til lovforslag, som tilsynet havde haft i høring. STAR havde på grund af tidspres været nødsaget til at sende lovforslaget i høring, inden det var endeligt gennemarbejdet.

Datatilsynets fornyede vurdering koncentrerede sig herefter om de dele af lovforslaget, som omhandlede et landsdækkende digitalt afklarings- og dialogværktøj, som kunne benyttes af jobcentre og arbejdsløshedskasser. Med værktøjet kunne der foretages en statistisk baseret analyse af borgerens risiko for at blive langtidsledig ud fra oplysninger fra borgeren selv og oplysninger om borgeren, som blev indhentet via Beskæftigelsesministeriets egne registre og registre fra andre offentlige myndigheder.

Efter en gennemgang af denne del af lovforslaget udtalte Datatilsynet i et supplerende høringssvar til STAR, at behandlingen af personoplysninger i forbindelse med anvendelsen af afklaringsværktøjet efter tilsynets opfattelse lå inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven. Datatilsynet lagde i den forbindelse bl.a. vægt på, at afklaringsværktøjet skal bruges til at understøtte sagsbehandlernes faglige vurdering med henblik på at forbedre muligheden for at tilbyde den rette indsats, men at der ikke skal træffes afgørelser udelukkende på baggrund af den behandling af oplysninger, som foretages ved brug af afklaringsværktøjet. Det var på den baggrund Datatilsynets opfattelse, at den omtalte profilering ikke falder ind under databeskyttelsesforordningens artikel 22.

Datatilsynet pegede imidlertid på, at det efter tilsynets opfattelse er væsentligt, at der løbende foretages en evaluering af anvendelsen af værktøjet, bl.a. med henblik på en vurdering af, om de anvendte variable i den matematiske model fortsat er relevante og brugen heraf sagligt begrundet. En sådan løbende evaluering og fornøden justering af den anvendte analysemodel må efter tilsynets opfattelse

anses for at være af afgørende betydning for at sikre de registreredes rettigheder og herunder undgå usaglig forskelsbehandling.

Lovforslag om ændring af lov om Center for Cybersikkerhed

Forsvarsministeriet anmodede i starten af 2019 Datatilsynet om eventuelle bemærkninger til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden).

Formålet med ændringen var at tilpasse lovgivningen til den hastige udvikling, der er i trusselsbilledet for cybersikkerheden og give Center for Cybersikkerhed (herefter CFCS) de relevante redskaber hertil.

Udkastet indebar en udvidelse af CFCS' mulighed for at yde et aktivt cyberforsvar, bl. a. ved at tillade installation af sikkerhedssoftware på eksempelvis pc'ere og servere hos de myndigheder og virksomheder, der tilsluttes CFCS' netsikkerhedstjeneste. Samtidig blev CFCS' muligheder for at kunne foretage forebyggende sikkerhedstekniske undersøgelser efter aftale med den tilsluttede myndighed eller virksomhed udvidet, herunder til at gennemføre simulerede angreb for at teste sikkerheden.

CFCS fik endvidere mulighed for gennem en editionskendelse at få udleveret oplysninger om brugeren af en e-mailkonto, en ip-adresse eller et domænenavn, ligesom rammerne for CFCS' videregivelse af data blev lempet og slettefristerne blev forlænget.

Selvom CFCS er en del af Forsvarets Efterretningstjeneste, og at databeskyttelsesforordningen og databeskyttelsesloven derfor ikke finder anvendelse på de behandlinger af personoplysninger, CFCS som dataansvarlig foretager, jf. databeskyttelseslovens § 3, stk. 2, fandt Datatilsynet anledning til at fremkomme med bemærkninger.

Datatilsynet lagde i den forbindelse vægt på, at reglerne i databeskyttelsesforordningen og databeskyttelsesloven vil finde anvendelse på behandlinger af personoplysninger foretaget af myndigheder og private virksomheder, som er tilsluttet CFCS' netsikkerhedstjeneste, eller som på anden måde anmoder om bistand fra centeret og i den forbindelse bl.a. videregiver personoplysninger til CFCS. Udkastet til lovforslaget åbnede dermed op for en bred behandling af personoplysninger, der vil høre under databeskyttelsesforordningens og databeskyttelseslovens anvendelsesområde.

Datatilsynet bemærkede, at rapporten om erfaringerne med den nye lovgivning burde oversendes til Folketinget allerede et år efter lovens ikrafttræden – i stedet for som foreslået i lovforslaget efter tre år – som følge af den hastige udvikling på området og det forhold, at der med udkastet ville ske en bred behandling af personoplysninger.

Endvidere var det Datatilsynets vurdering, at udkastet på en række punkter gav anledning til væsentlige uklarheder om de databeskyttelsesretlige regler i forhold til:

- De definitioner, der fulgte af udkastets § 1, nr. 1.
- Fordelingen af dataansvaret i forbindelse med behandling af personoplysninger, herunder særligt indsamling og videregivelse til de tilsluttede myndigheder og virksomheder.
- Behandlingsgrundlaget i henhold til databeskyttelsesforordningens artikel 6 og 9 samt databeskyttelseslovens § 8 for de tilsluttede myndigheder og virksomheder.
- Behandlingssikkerheden og forpligtelserne, der følger af databeskyttelsesforordningens artikel 32-34 for de tilsluttede myndigheder og virksomheder.

Tilsyn

For at sikre en effektiv beskyttelse af personoplysninger er bl.a. de forpligtelser, der påhviler dem, der behandler og træffer afgørelse om behandling af personoplysninger blevet styrket og præciseret med databeskyttelsesforordningen, ligesom tilsynsmyndighedernes beføjelser til at føre tilsyn med og sikre overholdelse af reglerne er blevet øget.

Datatilsynets tilsynsvirksomhed kan føre til, at der tages strafferetlige skridt, og Datatilsynet har også i 2019 indgivet de to første politianmeldelser med indstilling om bøde efter databeskyttelsesforordningen. Begge sager udsprang af planlagte tilsyn, som Datatilsynet havde opstartet i 2018.

Det er derfor væsentligt, at Datatilsynets medarbejdere har et godt kendskab til de mange forhold, som det er vigtigt at være opmærksomme på helt fra en sags begyndelse til dens endelige afgørelse ved domstolene, herunder bevissikring, retssikkerhedslov og udformning af anklageskrift. Datatilsynet gennemfører derfor sin tilsynsvirksomhed under iagttagelse af retningslinjer, som tilsynet tidligere har

udarbejdet i sammen med Rigspolitiet (herunder Nationalt Cyber Crime Center, NC3) og Rigsadvokaten. Datatilsynet har ligeledes bidraget til udarbejdelsen af en Rigsadvokatmeddelelse om håndteringen af sådanne sager og aftalt løbende opfølgninger med såvel Rigspolitiet som Rigsadvokaten. Herudover har Datatilsynet i 2019 ansat to tidligere anklagere, som bl.a. skal styrke tilsynets håndtering af straffesager.

Datatilsynet har endvidere i samarbejde med Erhvervsstyrelsen implementeret et system på Virk.dk, hvor dataansvarlige kan anmelde brud på persondatasikkerheden. Systemet har været operationelt fra den 25. maj 2018, hvor databeskyttelsesforordningen fandt anvendelse.

På Datatilsynets hjemmeside er en klageformular, som alle, der ønsker at klage til Datatilsynet, opfordres til at benytte. Klageformularen gør det lettere for borgerne at indgive en klage til Datatilsynet, idet det med klageformularen er tydeliggjort, hvilke oplysninger Datatilsynet har brug for, for at kunne behandle klagen.

Klagesagsbehandling

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

Når Datatilsynet modtager en klage, foretager Datatilsynet indledningsvis en vurdering af, hvad der klages over, herunder om klagen hører under tilsynets kompetence, og om vedkommende er klageberettiget. Hvis klager ikke selv har rettet henvendelse til den dataansvarlige om det forhold, som klager anmoder Datatilsynet om at tage stilling til, vil tilsynet som udgangspunkt sende klagen videre til den dataansvarlige eller bede klager om selv at gøre det. Det sker med henblik på, at den dataansvarlige i første omgang kan foretage en vurdering af, om behandling af klagers personoplysninger er berettiget, eller om klagers anmodning om f.eks. sletning af personoplysninger kan imødekommes. Datatilsynet vejleder samtidig klageren og den dataansvarlige om muligheden for på ny at rette henvendelse til tilsynet, hvis borgeren ikke er tilfreds med den dataansvarliges besvarelse.

I de sager, hvor Datatilsynet kan konstatere, at den dataansvarlige har forholdt sig til klagers indsigelse, vil tilsynet foretage en vurdering af, om der er grundlag for at indlede en egentlig klagesag. Hvis det er tilfældet, beder Datatilsynet den dataansvarlige om en udtalelse. Svaret fra den dataansvarlige vil som udgangspunkt blive sendt til klageren med henblik på, at denne kan komme med eventuelle yderligere bemærkninger til sagen. I nogle tilfælde kan bemærkningerne fra klager give anledning til endnu en høring af den dataansvarlige, inden Datatilsynet kan træffe afgørelse i sagen.

Datatilsynet har også mulighed for at afvise at indlede en sag over for den dataansvarlige, hvis klagen vurderes at være åbenbart grundløs eller uforholdsmæssig, jf. databeskyttelsesforordningens artikel 57, stk. 4. En klage anses bl.a. for at være åbenbart grundløs, hvis den ikke indeholder relevante elementer omfattet af databeskyttelsesforordningen, eller hvis klagen allerede på det foreliggende grundlag anses for udsigtsløs. Ved vurderingen af, om en anmodning om indledning af en klagesag kan anses for uforholdsmæssig, inddrages Datatilsynets opgaver og forpligtelser, ligesom styrken af den interesse, der er i, at sagen behandles, og den beskyttelse af privatlivet, som en behandling af sagen vil medføre, indgår i vurderingen. Datatilsynet kan f.eks. inddrage ressourcehensyn ved vurderingen af, om en anmodning skal afvises.

Datatilsynet vil i forbindelse med sin behandling af klagesager derudover vurdere, om klagen omhandler grænseoverskridende behandling af personoplysninger, jf. databeskyttelsesforordningens artikel 4, nr. 23. En behandling af personoplysninger anses for at være grænseoverskridende bl.a., hvis behandlingen finder sted som led i aktiviteter, som udføres for en dataansvarlig i flere medlemsstater, og hvor den dataansvarlige samtidig er etableret i flere medlemsstater. Datatilsynet vil i forbindelse med sin

vurdering af, om en klage omhandler grænseoverskridende behandling inddrage offentligt tilgængelig information, tidligere sager, og hvis der forsat er uklarhed, vil tilsynet bede den dataansvarlige om en udtalelse. Hvis Datatilsynet vurderer, at behandlingen er grænseoverskridende, skal sagen behandles i den såkaldte One-stop-shop mekanisme. Dette indebærer, at klagesagen skal oprettes i informationssystemet for det indre marked (IMI), og via dette system vil Datatilsynet i samarbejde med andre datatilsyn i EU behandle klagesagen.

Der vil i den forbindelse blive udpeget en ledende tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 56, stk. 1, og det er denne tilsynsmyndighed, der vil stå for selve behandlingen af klagesagen. Den ledende tilsynsmyndighed er tilsynsmyndigheden for den dataansvarliges hovedvirksomhed eller eneste etablering i Unionen. Dette betyder, at en klage, der indgives til Datatilsynet over en dataansvarlig, hvis hovedvirksomhed er i en anden medlemsstat, vil blive behandlet af den pågældende medlemsstats datatilsyn og efter medlemsstatens nationale forskrifter. Datatilsynet vil i denne situation varetage kommunikationen mellem klager og den ledende tilsynsmyndighed. Datatilsynet, samt andre datatilsyn, der er berørte af den pågældende grænseoverskridende behandling, vil via IMI have mulighed for at kommentere på og komme med indsigelser imod den ledende tilsynsmyndigheds afgørelse i sagen.

Nedenfor ses eksempler på klagesager, som Datatilsynet i 2019 traf afgørelse i.

Registrering af trafik- og lokaliseringsdata

Datatilsynet tog i 2019 stilling til en klage over TDC A/S' behandling af personoplysninger om klager i forbindelse med teleselskabets registrering af trafik- og lokaliseringsdata, når klagers mobiltelefon tilgik internettet.

TDC A/S var efter logningsbekendtgørelsen alene forpligtet til at registrere lokaliseringsdata for MMS-kommunikation, men som følge af den tekniske opbygning af teleselskabets mobilnet var dette ikke muligt uden samtidig at registrere lokaliseringsdata for al øvrig mobildatatrafik.

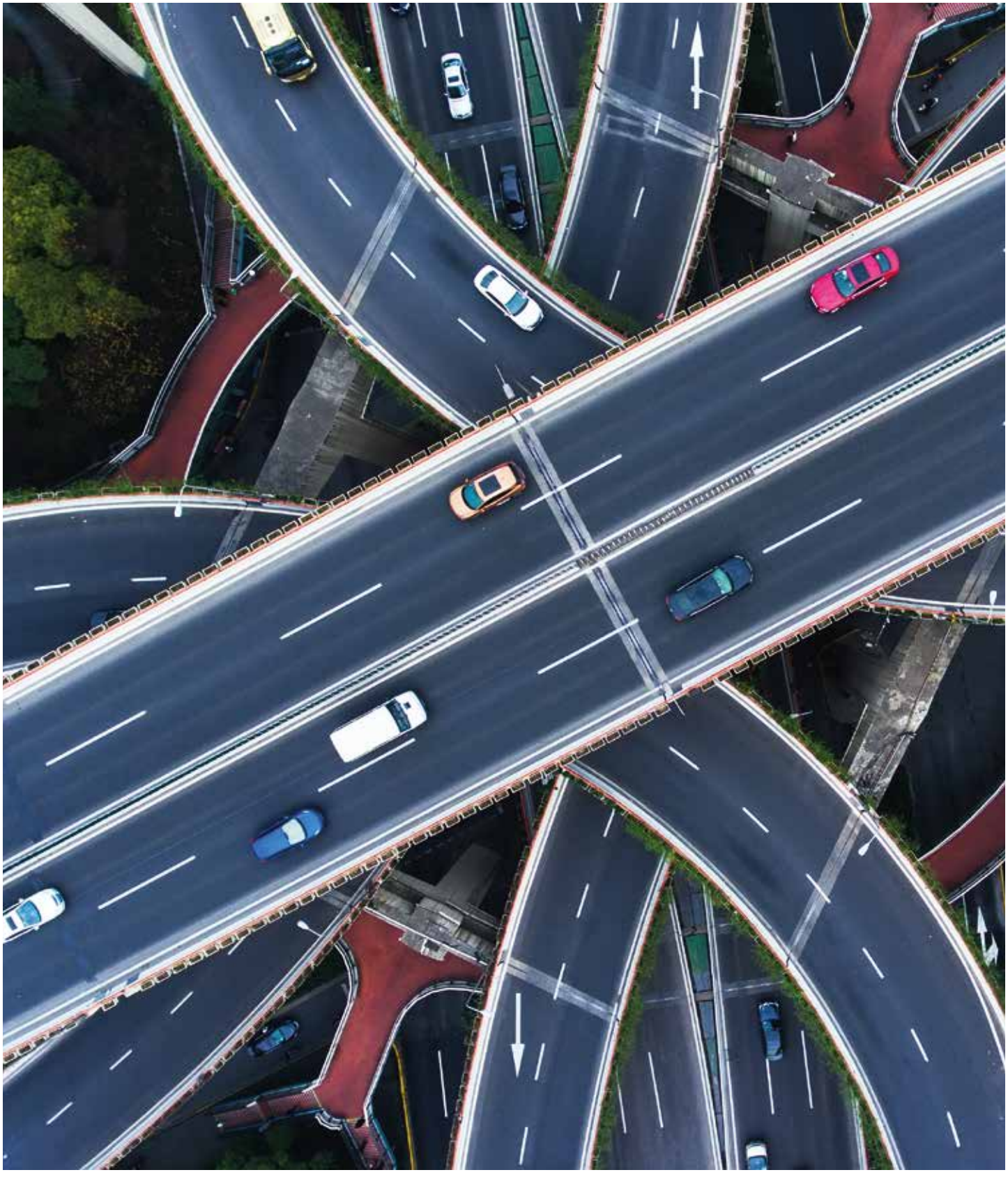
Efter en gennemgang af sagen, og efter at sagen havde været behandlet på et møde i Datarådet, fandt Datatilsynet, at der var grundlag for at udtale alvorlig kritik af, at TDC A/S' behandling af personoplysninger om klager ikke var sket i overensstemmelse med dataminimeringsprincippet i databeskyttelsesforordningens artikel 5, stk. 1, litra c.

Det var således Datatilsynets vurdering, at opbygningen af TDC A/S' it-system ikke kunne begrunde en manglende overholdelse af databeskyttelsesreglerne, ligesom eventuelle omkostninger forbundet med at etablere nye systemer, der ville gøre det muligt alene at registrere de nødvendige oplysninger, heller ikke kunne begrunde en manglende overholdelse af databeskyttelsesreglerne.

Datatilsynet lagde i den forbindelse vægt på, at langt størstedelen af de oplysninger, som TDC A/S havde registreret om klager, ikke var nødvendige for at overholde teleselskabets forpligtelser efter logningsbekendtgørelsen.

Datatilsynet lagde endvidere vægt på, at oplysningerne alene blev registreret på grund af teleselskabets mobilnets opbygning, og at TDC A/S selv havde oplyst, at man ikke havde noget formål med at registrere de pågældende, overskydende oplysninger.

Endelig lagde Datatilsynet vægt på, at det allerede i forbindelse med logningsbekendtgørelsens udstedelse blev fremført af Teleindustrien, at det ville være bekosteligt for teleudbyderne at udvikle systemer, der alene registrerer de nødvendige oplysninger, men at logningsbekendtgørelsen desuagtet blev udstedt indeholdende en sådan forpligtelse.



Berigtigelse af urigtige personoplysninger

Datatilsynet traf i 2019 afgørelse i en sag, hvor en kunde hos Rejsekort A/S klagede til Datatilsynet over, at Rejsekort A/S ikke var i stand til at berigtige urigtige personoplysninger om klager.

Kunden kunne af historikken på sit rejsekort se, at han flere gange skulle have foretaget busrejser, som han ikke havde foretaget. Da kunden rettede henvendelse til Rejsekort A/S, oplyste virksomheden, at man var bevidst om, at der – på grund af menneskelige fejl fra buschaufførerne – kunne ske fejlregistreringer af bussernes rute, inden de påbegyndte en tur. Da det ikke var teknisk muligt efterfølgende at rette oplysningerne om bussernes lokation i Rejsekort A/S' IT-system, tilføjede Rejsekort A/S de af kunden oplyste korrekte lokationsoplysninger som en supplerende note til klagers historik.

Datatilsynet fandt, at den registrerede i medfør af databeskyttelsesforordningens artikel 16 har ret til, at der sker berigtigelse af urigtige oplysninger om lokation, og at Rejsekort A/S – ved at behandle urigtige lokationsoplysninger samt ved ikke at være i stand til at berigtige disse oplysninger – overtrådte databeskyttelsesforordningens artikel 5, stk. 1, litra a, c og d, samt forordningens artikel 12. Datatilsynet udtalte derfor alvorlig kritik af Rejsekort A/S og meddelte Rejsekort A/S påbud om at imødekomme klagers anmodning om berigtigelse i overensstemmelse med databeskyttelsesforordningens artikel 16.

I forhold til Rejsekort A/S' generelle behandling af urigtige personoplysninger i forbindelse med busrejser meddelte Datatilsynet Rejsekort A/S påbud om bringe behandlingen i overensstemmelse med de databeskyttelsesretlige regler.

Indsigt i tv-overvågningsoptagelser

Datatilsynet har i 2019 behandlet en sag, hvor en passager klagede over, at Metro Service A/S havde givet afslag på hans anmodning om indsigt i tv-overvågningsoptagelser fra den pågældendes rejse.

Passageren oplyste bl.a. i sagen, at han havde anmodet om indsigt i optagelser af ham fra tv-overvågningen fra en nærmere bestemt rejse med metroen, da han som regelmæssig bruger af metroen havde en særlig interesse i at vide, hvilke personoplysninger Metro Service A/S indsamlede om ham, når han rejste med metroen.

Metro Service A/S oplyste i sagen, at optagelser fra metroens tv-overvågning kan afsløre placeringen af kameraer og eventuelle blinde vinkler, hvorfor indsigt i disse optagelser medfører en reel risiko for at kompromittere sikkerheden i og på metroens område.

Metro Service A/S foretog ved besvarelsen af passagerens indsigtsanmodning en konkret vurdering af hensynet til hans interesse i at få indsigt i de pågældende optagelser, over for hensynet til offentlige interesser, herunder hensynet til den offentlige sikkerhed og/eller forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed.

Ved afvejningen af ovenstående hensyn lagde Metro Service A/S vægt på, at metroens tv-overvågning hviler på en retlig forpligtelse fastsat ud fra et hensyn til sikkerhed i forbindelse med et stort, offentligt og frit tilgængeligt førerløst transportsystem, der årligt har ca. 60. mio. passagerer og som betjener væsentlige trafikknudepunkter i Danmark. Metro Service A/S lagde endvidere vægt på, at passageren ikke havde anført en særlig begrundelse for sin interesse i at få indsigt, eksempelvis ved at (dele af) optagelserne skulle vise et forhold af særlig betydning, f.eks. en ulykke, overfald, tyveri eller lignende. På baggrund af hensynsafvejningen vurderede Metro Service A/S, at selskabet kunne undlade at imødekomme indsigtsanmodningen, jf. undtagelsesbestemmelserne i databeskyttelseslovens § 22, stk. 2, nr. 3 og 4.

Datatilsynet fandt, at der i det konkrete tilfælde ikke var grundlag for at tilsidesætte Metro Service A/S' vurdering af, at hensynet til passagerens interesse i at få indsigt i oplysningerne, i den pågældende situation, måtte vige for afgørende hensyn til den offentlige sikkerhed, hvorfor undtagelsen til retten til indsigt i databeskyttelseslovens § 22, stk. 2, nr. 3 og nr. 4, kunne finde anvendelse.

På grundlag af sagens omstændigheder fandt Datatilsynet, at Metro Service A/S' håndtering af den pågældende indsigtsanmodning i den konkrete sag ikke var sket i strid med reglerne i databeskyttelsesforordningen og databeskyttelsesloven. Afgørelsen var således en konkret begrundet fravigelse af udgangspunktet om den registreredes ret til indsigt.

Klage over manglende sletning

Datatilsynet traf den 5. juli 2019 afgørelse i en sag, hvor en borger klagede over, at Odense Kommune havde afvist at slette oplysninger om borgeren i forbindelse med borgerens afsluttede sag hos kommunen.

Odense Kommune begrundede den manglende sletning med, at kommunen som offentlig myndighed har pligt til at overholde notat- og journaliseringspligten, og at der på sagen ikke var dokumenter, som var fejljournaliseret. Odense Kommune henviste i den forbindelse til databeskyttelsesforordningens artikel 17, stk. 3, litra b. Efter denne bestemmelse finder retten til sletning ikke anvendelse, hvis den fortsatte behandling af oplysninger om den registrerede er nødvendig for at 1) overholde en retlig forpligtelse eller 2) udøve en opgave i samfundets interesse eller 3) udføre en opgave, som henhører under offentlig myndighedsudøvelse, som den dataansvarlige, altså kommunen, er blevet pålagt.

Datatilsynet fandt på grundlag af sagens omstændigheder, at Odense Kommunes afvisning af at slette klagers oplysninger ikke var sket i strid med reglerne i databeskyttelsesforordningens artikel 17, og at kommunens behandling af oplysninger om klager ikke var gået ud over, hvad der kan ske i henhold til princippet om opbevaringsbegrænsning, jf. forordningens artikel 5, stk. 1, litra e.

Det fremgik imidlertid også af sagen, at kommunen først besvarede borgerens anmodning fem måneder og 21 dage efter, at kommunen modtog anmodningen. Datatilsynet fandt, at Odense Kommune herved ikke havde levet op til databeskyttelsesforordningens artikel 12, stk. 3. Efter denne bestemmelse skal den dataansvarlige behandle en anmodning fra den registrerede om sletning uden unødig forsinkelse og senest en måned efter modtagelsen af anmodningen. Denne periode kan dog forlænges med to måneder, hvis det er nødvendigt under hensyntagen til anmodningernes kompleksitet og antal.

Datatilsynet fandt på baggrund heraf grundlag for at udtale kritik af, at Odense Kommunes behandling af personoplysninger ikke havde været i overensstemmelse med databeskyttelsesforordningens artikel 12, stk. 3.

Udøvelse af registreredes rettigheder – afgørelse om ID-validering

Datatilsynet har i 2019 behandlet en sag, hvor en britisk borger klagede over, at Pandora A/S havde bedt ham om at indsende legitimation i form af pas, kørekort eller et nationalt identitetskort, før Pandora A/S ville tage stilling til hans anmodning om sletning af de personoplysninger, som Pandora havde registreret om ham.

Klager ønskede imidlertid ikke at sende legitimation til Pandora A/S, hvorfor virksomheden ikke imødekom klagers anmodning om sletning, da Pandora A/S efter egen opfattelse ikke med sikkerhed kunne identificere klager uden legitimationen.

Pandora A/S oplyste til Datatilsynet, at virksomheden af sikkerhedsmæssige grunde havde etableret en generel procedure om indsendelse af legitimation i forbindelse med anmodninger om udøvelse af registreredes rettigheder.

Klager oplyste, at han ikke ønskede at give Pandora A/S yderligere personlige oplysninger for at få imødekommet anmodningen om sletning.

Datatilsynet fandt, at Pandora A/S' generelle procedure, hvorefter der uden undtagelse blev stillet krav om ID-validering i forbindelse med behandling af anmodninger om udøvelse af registreredes rettigheder, ikke var i overensstemmelse med databeskyttelsesforordningen.

Datatilsynet lagde blandt andet vægt på, at den dataansvarlige har pligt til at foretage en konkret vurdering af, om der hersker rimelig tvivl om identiteten på den fysiske person, i forbindelse med modtagelse af anmodninger om udøvelse af registreredes rettigheder.

Datatilsynet lagde også vægt på, at en anmodning om yderligere oplysninger med henblik på at identificere den fysiske person skal være proportional, og at den dataansvarlige derfor ikke må kræve flere oplysninger, end hvad der er nødvendigt for at kunne identificere den fysiske person.

Sagen er i øvrigt den første sag, hvor Datatilsynet har truffet afgørelse som ledende tilsynsmyndighed efter den såkaldte "one-stop shop-mekanismen" i forbindelse med grænseoverskridende behandling af personoplysninger, jf. databeskyttelsesforordningens kapitel VII, navnlig artikel 60.

Planlagte tilsyn og sager på eget initiativ

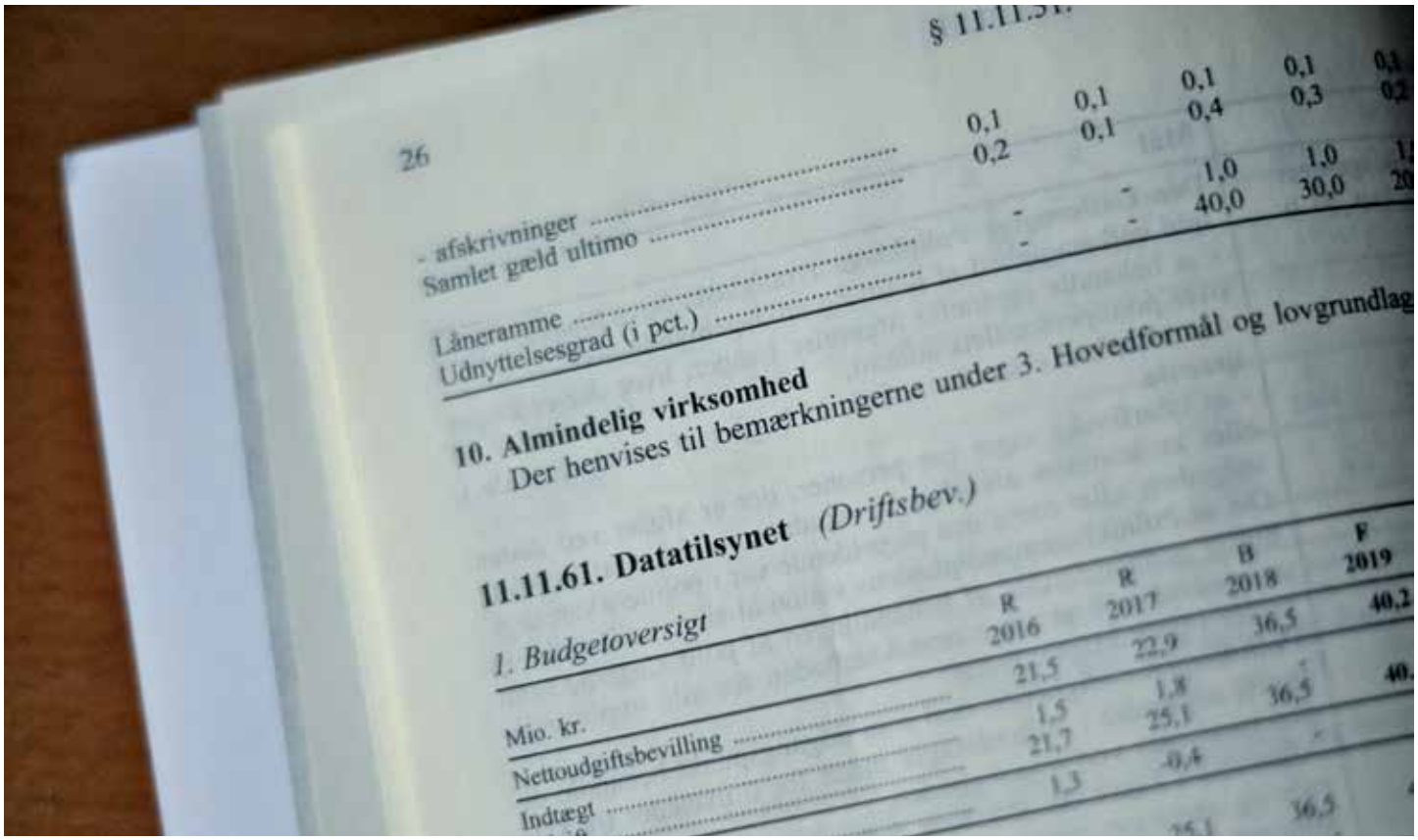
Sager på eget initiativ

Hvert år tager Datatilsynet en række sager op på eget initiativ. Blandt disse sager er Datatilsynets planlagte tilsyn og Datatilsynets behandling af anmeldelser af brud på persondatasikkerhed. Herudover tager Datatilsynet også en række sager op ad hoc på baggrund af konkrete hændelser, herunder på baggrund af presseomtale, henvendelser fra borgere mv.

Plan for tilsyn

Datatilsynet foretager hvert år et antal planlagte tilsyn. Tilsynene bliver planlagt for cirka et halvt år ad gangen, hvor Datatilsynet i første omgang finder frem til, hvilke temaer og myndigheder/virksomhedsbrancher tilsynene skal dække, og herefter finder frem til de enkelte dataansvarlige, som skal være genstand for Datatilsynets tilsyn.

Når Datatilsynet udvælger, hvilke temaer og myndigheder/virksomhedsbrancher tilsynene skal dække, fokuserer Datatilsynet navnlig på behandlinger af personoplysninger, som på grund af deres formål, omfang eller karakter indebærer en særlig risiko for at krænke de registreredes ret til databeskyttelse



og privatliv, samt på behandlinger, som indebærer brug af ny teknologi. Andre parametre indgår også i Datatilsynets vurdering, herunder f.eks. områder, hvor der har vist sig at være udfordringer, henvendelser fra borgere og medier mv. omkring specifikke problemstillinger og en vis geografisk spredning.

Datatilsynet offentliggør en udgave af tilsynsplanen på Datatilsynets hjemmeside med angivelse af det pågældende halvårs temaer og kategorier af myndigheder/virksomhedsbrancher, men uden angivelse af hvilke konkrete dataansvarlige eller databehandlere, der er udvalgt.

Tilsyn i 2019

I 2019 foretog Datatilsynet 67 planlagte tilsyn. Disse planlagte tilsyn var fordelt med 37 tilsyn over for offentlige myndigheder og 30 tilsyn over for private virksomheder. Ved alle tilsynene har der været anvendt oplysningsindsamling bl.a. ved hjælp af spørgeskema. For en række af disse tilsyn har Datatilsynet endvidere suppleret med et fysisk tilsynsbesøg.

Datatilsynet fokuserede i første halvår af 2019 på følgende temaer:

- Brud på persondatasikkerheden hos offentlige myndigheder og private virksomheder
- Databeskyttelsesrådgiverfunktionen hos kommunerne
- Kryptering af e-mails hos private virksomheder
- Autorisation af medarbejdere hos kommunerne
- Den registreredes indsigtsret hos offentlige myndigheder og private virksomheder

Datatilsynet fokuserede i andet halvår af 2019 på følgende fire temaer:

- Databehandlere
- Den daglige overvågning
- Databeskyttelse i forbindelse med ansættelsesforhold
- Automatiske afgørelser og profilering

Under hvert af de fire temaer har Datatilsynet fokuseret på en række underemner.

Datatilsynet har som underemne til temaet "databehandlere" besluttet at kigge på behandlingssikkerhed og brug af underdatabehandlere og har udvalgt et antal leverandører til både den offentlige og den private sektor.

Temaet "den daglige overvågning" omfatter en række tilsyn, hvor Datatilsynet bl.a. har haft fokus på den dataansvarliges opfyldelse af oplysningspligten i forskellige overvågningssituationer, nemlig i forhold til offentlige og private arbejdsgiveres kontrol af medarbejdere og behandling af kunders købs- og rejsehistorik. Herudover har Datatilsynet besluttet at kigge på automatisk nummerpladegenkendelse i indkøbscentre, særligt i forhold til behandlingshjemmel, oplysningspligt og sletning.

Under temaet "databeskyttelse i forbindelse med ansættelsesforhold" har Datatilsynet – ud over tilsynet nævnt ovenfor vedrørende oplysningspligt ved kontrol af medarbejdere – haft fokus på offentlige og private arbejdsgiveres opbevaring og sletning af oplysninger indsamlet i forbindelse med rekruttering.

I forbindelse med temaet "automatiske afgørelser og profilering" har Datatilsynet valgt at sætte fokus på bank- og forsikringsbranchens anvendelse af sådanne afgørelser.

Evaluering af tilsynsordningen

Datatilsynet igangsatte i 2019 en evaluering af måden for at udføre tilsyn (planlagte og ad-hoc). Det har i den forbindelse bl.a. vist sig, at muligheden for at pålægge større bøder, har haft en negativ betydning for bl.a. tilsynets sagsbehandlingstider i tilsynssager. Dette skyldes bl.a. høje krav til bevissikkerhed i straffesager, og at tilsynet oplever en mindre samarbejdsvillighed hos tilsynssubjekterne.

Evalueringen, der vil fortsætte i 2020, har bl.a. ført til, at Datatilsynet vil iværksætte en forsøgsordning i forhold til at teste et supplerende mere ensartet og databaseret tilsynskoncept, ligesom der vil ske en opdatering af tilsynets interne retningslinjer for tilrettelæggelse og afvikling af tilsyn.

Krypteringstilsyn

Ved årets begyndelse skærpede Datatilsynet kravene til kryptering af e-mails i den private sektor. Det betyder, at det siden 1. januar 2019 har været praksis, at private virksomheder – ligesom det har været tilfældet for offentlige myndigheder siden 2000 – normalt skal anvende kryptering ved transmission af fortrolige og følsomme personoplysninger med e-mail via internettet.

På den baggrund har Datatilsynet i løbet af foråret 2019 gennemført fire tilsynsbesøg med dette tema hos Kristelig Fagforening, BDO Statsautoriseret Revisionsaktieselskab, et advokatfirma og et kontorfællesskab af advokatfirmaer.

Datatilsynet har over for kontorfællesskabet af advokatfirmaer udtalt kritik af, at kontorfællesskabet ikke har efterlevet kravene i databeskyttelsesforordningens artikel 32, stk. 1, og artikel 5, stk. 2, jf. stk. 1, litra f, jf. artikel 32, stk. 1 og 2, idet der ikke forud for tilsynsbesøget har været indført procedurer, der sikrer, at der anvendes kryptering på transportlaget via TLS til fremsendelse af fortrolige og følsomme personoplysninger til klienter mv. over internettet. Herudover havde kontorfællesskabet ikke påvist at have udarbejdet en risikovurdering, der tager stilling til risikoen forbundet med fremsendelse af fortrolige og følsomme personoplysninger over internettet.

Over for Kristelig Fagforening har Datatilsynet udtalt kritik af, at fagforeningen ikke har overholdt databeskyttelsesforordningens artikel 32, idet fagforeningen har anvendt personnummeret på den person, som en e-mail vedrører, som password til læsning af en e-mail, der er lagret på fagforeningens sikre webtjeneste til læsning af e-mail.

Herudover har Datatilsynet udtalt kritik af, at Kristelig Fagforening har overtrådt artikel 32 og 33 ved i perioden 1. januar 2019 til 9. april 2019 at have sendt e-mails ukrypteret, hvor der kunne udledes oplysninger om fagforeningsmæssigt tilhørsforhold, og uden at have anmeldt hændelserne til Datatilsynet som brud på persondatasikkerheden. Endelig meddelte Datatilsynet Kristelig Fagforening påbud om at ophøre med at benytte personnummeret på den person, som en e-mail til læsning på fagforeningens sikre webtjeneste vedrører, som password til læsning af e-mailen. Kristelig Fagforening har den 19. november 2019 oplyst, at påbuddet er efterlevet.

I forbindelse med tilsynene hos advokatfirmaet og BDO Statsautoriseret Revisionsaktieselskab fandt Datatilsynet, at behandlingen af personoplysninger i forhold til fremsendelse af fortrolige og følsomme personoplysninger via e-mail over internettet var i overensstemmelse med reglerne i databeskyttelsesforordningen og Datatilsynets retningslinjer.

Indsigtstilsyn

I løbet af foråret 2019 gennemførte Datatilsynet tilsyn hos tre private virksomheder og tre offentlige myndigheder med fokus på reglerne om den registreredes indsigtsret. Fem af tilsynene blev udført

som fysiske tilsynsbesøg. For så vidt angår en af de private virksomheder, som efter det oplyste ikke havde modtaget eller behandlet nogle anmodninger om indsigt på tidspunktet for tilsynet, besluttede Datatilsynet at aflyse det planlagte fysiske tilsynsbesøg og i stedet gennemføre et skriftligt tilsyn.

Efter databeskyttelsesforordningens artikel 15 har den registrerede som udgangspunkt ret til at få indsigt i de personoplysninger, den dataansvarlige behandler om vedkommende. Indsigtsretten indebærer også, at den registrerede har ret til at få en række oplysninger om, hvordan vedkommendes personoplysninger behandles, herunder bl.a. hvad formålet med behandlingen er, hvem oplysningerne deles med, hvor længe oplysningerne opbevares, og hvor oplysningerne stammer fra.

Formålet med indsigtsretten er at give den registrerede mulighed for at se, hvilke personoplysninger den dataansvarlige behandler om den pågældende og at skabe mere gennemsigtighed omkring, hvordan den dataansvarlige behandler oplysningerne. På den baggrund kan den registrerede kontrollere, at person-oplysninger om den pågældende er korrekte og i øvrigt behandles lovligt.

Databeskyttelsesforordningens artikel 12 indeholder en række processuelle krav, som den dataansvarlige skal være opmærksom på ved iagttagelsen af den registreredes rettigheder, herunder indsigtsretten. Det indebærer bl.a., at enhver meddelelse, som den dataansvarlige giver efter artikel 15 til den registrerede, skal gives i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog, ligesom den dataansvarlige generelt skal lette udøvelsen af den registreredes rettig-

heder. Herudover skal den dataansvarlige uden unødig forsinkelse og i alle tilfælde senest en måned efter modtagelsen af en anmodning oplyse den registrerede om de foranstaltninger, der træffes på baggrund af bl.a. en indsigtsanmodning.

I forbindelse med de gennemførte tilsyn har Datatilsynet bl.a. påset, om de dataansvarlige ved besvarelse af indsigtsanmodninger har givet de registrerede de fornødne oplysninger i henhold til forordningens artikel 15. Herudover har tilsynet generelt påset, om de dataansvarliges iagttagelse af indsigtsretten er sket i overensstemmelse med de processuelle krav, som følger af forordningens artikel 12.

Datatilsynet har på baggrund af de udførte tilsyn udtalt kritik i fire af de seks sager for manglende overholdelse af kravene i databeskyttelsesforordningens artikel 15 og/eller artikel 12.

Datatilsynet har herudover fundet, at én af de seks dataansvarlige generelt har besvaret anmodninger om indsigt i overensstemmelse med forordningens artikel 15, ligesom den dataansvarlige i alle de gennemgåede tilfælde har besvaret anmodningerne inden for en måned efter modtagelsen. Sagen blev derfor afsluttet uden kritik.

Den sidste af de seks dataansvarlige havde ikke på tidspunktet for tilsynet modtaget eller behandlet nogen indsigtsanmodninger. Sagen blev derfor afsluttet uden kritik men med anbefalinger til udformningen af den dataansvarliges procedurer og retningslinjer samt standardtekster.

Brud på persondatasikkerheden – utilsigtede videregivelser

Datatilsynet havde i perioden frem til den 8. februar 2019 modtaget i alt 66 anmeldelser af brud på persondatasikkerheden fra PFA Pension. Efter en gennemgang af sagerne kunne Datatilsynet konstatere, at 62 ud af 66 anmeldelser vedrørte utilsigtet videregivelse af personoplysninger i forbindelse med fremsendelse af dokumenter via kommunikationsløsningen "Mit PFA", e-Boks, med brevpost eller lignende.

På denne baggrund valgte Datatilsynet i maj at starte en sag af egen drift over for PFA Pension. I den forbindelse bad tilsynet PFA Pension om bl.a. at redegøre for, hvilken risikovurdering selskabet har foretaget jf. databeskyttelsesforordningens artikel 32, i forhold til at sikre sig mod, at personoplysninger kommer til uvedkommendes kendskab. Datatilsynet bad også PFA Pension om at redegøre for, hvilke foranstaltninger PFA Pension har truffet eller vil træffe med henblik på fremadrettet at undgå utilsigtede videregivelser som dem, der er anmeldt som brud på persondatasikkerheden til Datatilsynet.

I sin udtalelse oplyste PFA Pension, at de skete brud er fordelt således, at der for 36 af tilfældene er tale om brug af kommunikationsplatformen "Mit PFA", at der for 17 af tilfælde er tale om brevpost, og at der for de resterende 13 tilfælde er tale om andre løsninger, herunder e-mail, e-Boks og videregivelse til banker. PFA Pension anførte herudover, at tilfældene alene udgør 0,3 promille af det samlede antal årlige udgående kommunikationer til kunder, men at antallet desuagtet er for højt.

PFA Pension oplyste endvidere, at selskabet – som følge af de skete brud på persondatasikkerheden – har indført yderligere tekniske og organisatoriske foranstaltninger mod, at personoplysninger skal blive sendt til uvedkommende. Disse foranstaltninger indebærer bl.a.:

- Ekstra kontrolforanstaltninger i Mit PFA, der indebærer et afkrydsningsfelt med tilkendegivelse af, at afsenderen har kontrolleret vedhæftninger.
- Integration af modulbreve via Word i Mit PFA.
- Indskærpelse af "makker kontrol" i forbindelse med besvarelse af indsigtsanmodninger.

På baggrund af sagen fandt Datatilsynet anledning til at udtale kritik af, at PFA Pensions behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1. Samtidig noterede tilsynet sig dog, at PFA Pension løbende monitorerer det etablerede sikkerhedsniveau, og at selskabet på baggrund af de passerede brud allerede inden tilsynets henvendelse tog skridt til at implementere yderligere sikkerhedsforanstaltninger for at styrke behandlingssikkerheden.

Manglende sikkerhed omkring en udviklingsserver

Datatilsynet behandlede i 2018 en klagesag, hvor KMD som databehandler i forbindelse med overtagelsen af et udviklings- og testmiljø fra en anden leverandør (før databeskyttelsesforordningen fandt anvendelse) ikke havde gennemført passende sikkerhedsforanstaltninger.

Da KMD erhvervede it-løsningen, blev det ikke påset, i hvilket omfang en test- og udviklingsserver indeholdt oplysninger om fysiske personer. Serveren var til brug for udviklingsopgaver koblet til et netværk uden for databehandlerens kontrol (internettet), og serveren blev flere år efter overtagelsen kompromitteret og benyttet uretmæssigt til at "udvinde" kryptovalutaen Bitcoin. Serveren var på grund af den oprindelige klassifikation – som intern udviklingsserver, uden persondata – ikke undergivet databehandlerens ordinære driftssikkerhedssetup (patch- og sikkerhedspolitik).

Da den uretmæssige brug blev konstateret, blev det samtidigt fastslået, at serveren – alligevel – indeholdt personhenførbare informationer fra flere dataansvarlige.

Datatilsynet fandt, at bruddet på persondatasikkerheden kunne have været undgået, hvis der havde været indført helt almindelige tekniske sikkerhedsforanstaltninger, bl.a. firewall-regler, og at de etablerede sikkerhedsforanstaltninger derfor ikke kunne anses som passende. Årsagen hertil var primært, at risikovurderingen alene var baseret på den oprindelige beskrivelse af serveren som "intern server" (uden personoplysninger).

Datatilsynet udtalte kritik af, at KMD's behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, særligt på grund af utilstrækkelig sikkerhed for den behandling, som blev berørt af bruddet på persondatasikkerheden, og fordi sagen fremstod således, at KMD kunne have undgået dette brud, ved almindelige tekniske sikkerhedsforanstaltninger, der ikke ville have hindret, den tiltænkte anvendelse af serveren.

Oversigt over udførte tilsyn i 2019

Offentlige myndigheder:
Albertslund Kommune
Ankestyrelsen
Arbejdsmarkedets Erhvervssikring
Bornholms Regionskommune
Civilstyrelsen
Dragør Kommune
Esbjerg Kommune
Fredensborg Kommune
Frederiksberg Kommune
Frederikssund Kommune
Fødevarestyrelsen
Gribskov Kommune
Halsnæs Kommune
Helsingør Kommune
Hillerød Kommune
Hjørring Kommune
Hvidovre Kommune
Høje-Taastrup Kommune
Hørsholm Kommune
Kolding Kommune
Køge Kommune
Mariagerfjord Kommune
Næstved Kommune
Nævnenes Hus
Odense Kommune
Region Syddanmark
Roskilde Kommune
Roskilde Universitet
Styrelsen for Patientklager
Syddjurs Kommune
Udbetaling Danmark
Vejle Kommune
Vordingborg Kommune
Aalborg Kommune
Aalborg Universitet
Århus Kommune

Private virksomheder:
Alm. Brand Forsikring A/S
Apcoa Parkering Danmark A/S
Aros Privathospital Partnerselskab
A/S Arbejdernes Landsbank
ASE Lønmodtager
BDO Statsautoriseret Revisionsaktieselskab
Carlsberg A/S

COOP Danmark A/S
CP Parking Systems ApS
Danske Bank A/S
DJØF
Fynbus I/S
KMD A/S
Kombit A/S
Et kontorfællesskab for advokater
Kristelig Fagforening
Kræftens Bekæmpelse
Midttrafik I/S
Molslinjen A/S
Nemlig.com A/S
Parkzone A/S
Q-Park A/S
Rejsekort & Rejseplan A/S
SDC A/S
SIF Gruppen A/S
En advokat
TDC A/S
Tryg Forsikring A/S
Ørsted A/S

Anmeldelse af brud på persondata-sikkerheden

Opgørelse af brud på persondatasikkerheden i 2019

Med databeskyttelsesforordningen blev der indført en generel forpligtelse for alle dataansvarlige til at anmelde brud på persondatasikkerheden til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet.

Udgangspunktet er, at brud på persondatasikkerheden altid skal anmeldes, med mindre det er usandsynligt, at det pågældende brud indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Datatilsynet har i 2019 kvartalsvist udgivet en oversigt over anmeldelser af brud på persondatasikkerheden.

Samlet set blev der i 2019 anmeldt 7242 brud på persondatasikkerheden. Af disse tegner de offentlige dataansvarlige sig for godt 60 %, og de private for ca. 40 %.

Der har – over tid – vist sig et relativt fast billede. Det er de aktører, der har meget kommunikation med de registrerede, der har de fleste brud (godt 2/3 af det samlede antal brud) og langt de fleste af disse, skyldes en eller anden form for fejlfremsendelse af oplysninger. Typisk berører disse fejl primært enkelte personer.

Fejltyper med mange berørte registrerede og hvor oplysningerne bliver delt med mange uvedkommende, skyldes oftest situationer, hvor databehandlere eller udviklere af ny software og funktionalitet, ikke har foretaget fyldestgørende test, eller hvor fejl under implementeringen gør, at sikkerhedskonfigurationer konflikter med allerede installeret software eller åbner for utilsigtede adgange i andre services.

Datatilsynet monitorerer disse typetilfælde og prøver med fokus på disse at offentliggøre generelle retningslinjer og vejledende tekster, der kan bistå alle aktører i at undgå tilsvarende fejl fremover.

Anmeldt sikkerhedsbrud – underretning af registrerede

Datatilsynet modtog i 2018 enslydende anmeldelser fra de koncernforbundne dataansvarlige selskaber Intervare A/S og Nemlig.com A/S vedrørende et brud på persondatasikkerheden, hvor kunders ordreoplysninger havde været eksternt tilgængelige for uvedkommende.

I begge sager havde de dataansvarlige vurderet, at der ikke skulle ske underretning af de registrerede. Oplysningerne var primært navn, kontakt- og adresseoplysninger samt købshistorik.

Da der var tale om et betydeligt antal registrerede (mere end 250.000), og da de dataansvarlige ikke havde vurderet risikoen særskilt for den delmængde af de registrerede, der måtte have hemmelig eller udeladt adresse, foretog Datatilsynet en vurdering af risikoen for denne gruppe af registrerede. Da tilsynet vurderede risikoen for disse registrerede som værende høj, pålagde Datatilsynet de dataansvarlige at underrette den del af de registrerede, der havde hemmelig eller udeladt adresse.

Afgørelsen fastslår, at der selv i ellers homogene behandlinger af oplysninger, som generelt ikke har en høj risikoprofil, kan være forhold for den enkelte registrerede, der indebærer en høj risiko. Den risikovurdering, der foretages af den dataansvarlige – med hensyn til om der skal ske underretning – skal afspejle sådanne individuelle forhold.

Placering af dataansvar og alvorlig kritik af manglende sikkerhedsforanstaltninger

Københavns Universitet var dataansvarlig for den behandling af personoplysninger, der udføres af medicinstuderende, der i praktikforløb optager egne konsultationer med henblik på at opfylde sine forpligtelser for hhv. undervisning og eksamen på Københavns Universitet.

Datatilsynet modtog en anmeldelse om et brud på persondatasikkerheden fra en praktiserende læge, hvor en medicinstuderende fra Københavns Universitet i forbindelse med et 4 ugers praktikforløb hos lægen fik stjålet et videokamera med optagelser af patienter til brug for eksamen på Københavns Universitet. Kameraet var ejet og udlånt af Københavns Universitet.

Lægen anså ikke sig selv som dataansvarlig for den pågældende behandling af personoplysninger, og Datatilsynet anmodede på den baggrund Københavns Universitet om en udtalelse til sagen.

Københavns Universitet var af den opfattelse, at den studerende var dataansvarlig for den pågældende behandling af personoplysninger, hvilket også blev anført som årsagen til, at Københavns Universitet ikke havde handlet i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 1, artikel 33, stk. 1, og artikel 34, stk. 1.

Datatilsynet lagde ved afgørelsen om dataansvaret vægt på, at det er Københavns Universitet, der har fastsat ordningen og reglerne for praktikforløb for kurset i almen medicin. Kurset indgår som en del af den medicinstuderendes fag på Københavns Universitet, og det er dermed Københavns Universitet, der afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

Herudover var det Datatilsynets opfattelse, at Københavns Universitet – ved 1) at have mistet et videokamera indeholdende oplysninger om et ukendt antal registrerede, herunder oplysninger om helbred, 2) ikke at have indberettet bruddet på persondatasikkerheden til Datatilsynet og 3) ikke at underrette de registrerede personer omfattet af bruddet på persondatasikkerheden ikke har levet op til kravene i databeskyttelsesforordningens artikel 32, stk. 1, artikel 33, stk. 1, og artikel 34, stk. 1.

Datatilsynet udtalte samlet set alvorlig kritik af, at Københavns Universitets behandling af personoplysninger ikke er sket i overensstemmelse med databeskyttelsesforordningen.

Kryptering af e-mails og af opportunistisk TLS

Datatilsynet har i 2019 behandlet en en klage fra en borger og en sag af egen drift om Lowell Danmark A/S' fremsendelse af oplysninger underlagt fortrolighed via e-mail.

Begge sager skal ses som eksempler på de generelle principper, der gælder, når en dataansvarlig anvender en opportunistisk TLS 1.2-kryptering (kryptering på transportlaget, der kun virker, hvis modtagerens server understøtter det), til fremsendelse af fortrolige oplysninger over internettet.

Datatilsynet anbefaler generelt – dataansvarlige der behandler e-mail med følsomme og/eller fortrolige oplysninger – til at sætte deres mailserver op til, at der gennemtvinges TLS (Forced TLS), som minimum i version 1.2.

Det er dog efter tilsynets opfattelse – ikke i sig selv – i strid med databeskyttelsesforordningens artikel 32 at anvende en opportunistisk TLS, hvis den dataansvarlige ud fra en risikovurdering – korrekt – har vurderet, at en sådan opsætning udgør en passende sikkerhedsforanstaltning.

I klagesagen havde Lowell Danmark A/S foretaget en risikovurdering og blandt andet lagt vægt på, at det generelt kun er et fåtal af deres modtagere, der benytter sig af e-mailklientversioner eller tjenesteudbydere, hvor en e-mail vil blive sendt ukrypteret, og at Lowell Danmarks A/S konkret vurderer dette for de enkelte modtagere.

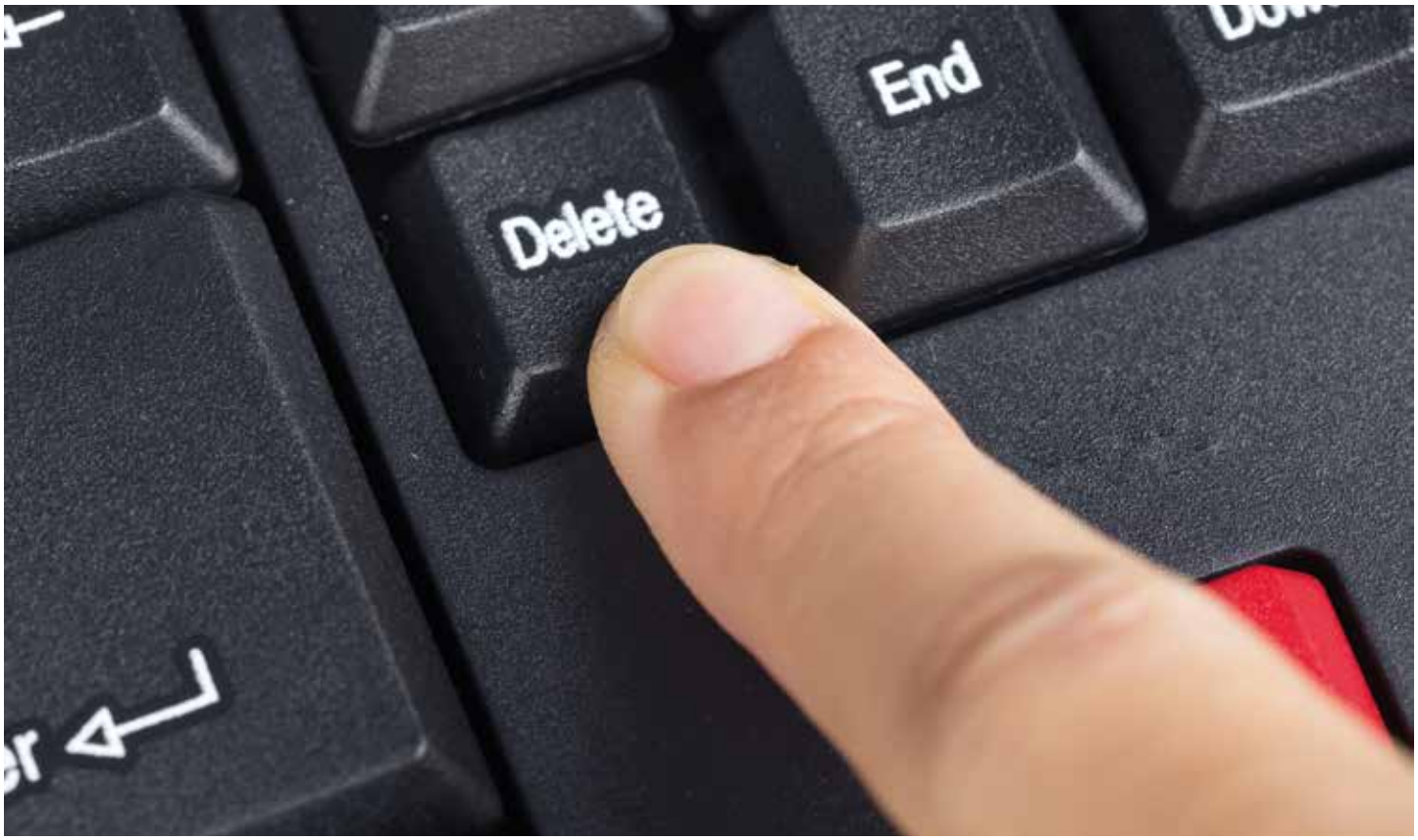
Datatilsynet fandt i den pågældende sag ikke grundlag for at tilsidesætte Lowell Danmark A/S' risikovurdering. Ved fremsendelsen af de pågældende e-mails blev der anvendt opportunistisk TLS 1.2 kryptering med en anerkendt algoritme, borgerens e-mailklient understøttede denne krypteringsform, og fremsendelsen af de pågældende e-mails havde været krypteret på transportlaget.

Datatilsynet fandt, at Lowell Danmark A/S' behandling af oplysninger var sket i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 1.

I egen drift-sagen fandt Datatilsynet, at der var grundlag for at udtale kritik af, at Lowell Danmark A/S' behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 5, stk. 2, jf. artikel 5, stk. 1, litra f, jf. artikel 32, stk. 1 og 2.

Forskellen fra den førnævnte afgørelse var, at Lowell Danmark A/S i denne sag, ikke havde kunnet verificere om modtagerdomænet kunne modtage TLS, og uanset denne manglende verifikation afsendte e-mailen med opportunistisk indstillet TLS 1.2. Lowell Danmark A/S kunne yderligere ikke godtgøre, om e-mailen rent faktisk var modtaget krypteret.

Sammenfattende gælder det, at anvendelsen af opportunistisk TLS-kryptering, kræver en verifikation af modtagerdomænet, og at behandlingen/fremsendelsen sker i henhold til en foretaget – retvisende risikovurdering, der inddrager de konkrete risici for den registreredes rettigheder, der er ved fremsendelsen.



Tilladelser mv.

Visse behandlinger kræver, at den dataansvarlige inden iværksættelsen af behandlingen indhenter Datatilsynets tilladelse.

Efter databeskyttelseslovens § 26, stk. 1, skal Datatilsynets forudgående tilladelse indhentes, når behandlingen af personoplysninger for en privat dataansvarlig foretages:

- med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret (advarselsregister),
- med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed (kreditoplysningsbureau), eller
- udelukkende med henblik på at føre retsinformationssystemer.

Datatilsynets forudgående tilladelse skal endvidere indhentes af private dataansvarlige til foretagelse af visse særlige behandlinger af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, som er nødvendige af hensyn til væsentlige samfundsinteresser, jf. databeskyttelseslovens § 7, stk. 4. Der er tale om behandlinger, som tidligere var omfattet af persondatalovens § 7, stk. 7.

Herudover skal Datatilsynets forudgående tilladelse efter databeskyttelseslovens § 10, stk. 3, indhentes i forbindelse med visse videregivelser af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2 (behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, og artikel 10, hvor behandling sker alene med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning).

På Datatilsynets hjemmeside findes flere oplysninger om de områder, hvor Datatilsynets tilladelse skal indhentes, ligesom blanketter til indgivelse af ansøgninger om tilladelse er tilgængelige på hjemmesiden. Endvidere offentliggøres der på hjemmesiden løbende et udvalg af konkrete tilladelser og afslag på tilladelse.

Nedenfor omtales enkelte konkrete tilladelsessager, som Datatilsynet har behandlet i 2019, og de sagsområder, hvor Datatilsynet har udformet (nye) standardvilkår for tilsynets tilladelser. Endelig omtales de generelle vilkår, som Datatilsynet har fastsat med hjemmel i databeskyttelseslovens § 10, stk. 4, for videregivelse af oplysninger omfattet af lovens § 10, stk. 1 og 2.

Behandling af biometriske data ved brug af automatisk ansigtsgenkendelse

Datatilsynet behandlede i 2019 en sag, hvor Brøndbyernes I.F. Fodbold A/S rettede henvendelse til tilsynet med en ansøgning om tilladelse til behandling af følsomme personoplysninger. Brøndbyernes I.F. Fodbold ønskede at etablere adgangskontrol ved behandling af biometriske data i forbindelse med automatisk ansigtsgenkendelse, for at karantænedømte personer på Brøndby IF's interne karantæneliste, ikke skulle få adgang til kampe på Brøndby Stadion.

Efter databeskyttelsesforordningens artikel 9, stk. 1, gælder et generelt forbud mod behandling af følsomme oplysninger, herunder behandling af biometriske data med det formål entydigt at identificere en fysisk person. Forbuddet gælder efter bestemmelsens stk. 2, imidlertid ikke hvis et af de i litra a-j nævnte forhold gør sig gældende.

Efter databeskyttelsesforordningens artikel 9, stk. 2, litra g, og databeskyttelseslovens § 7, stk. 4, kan forbuddet mod behandling af følsomme oplysninger fraviges. Efter bestemmelsen i § 7, stk. 4, skal Datatilsynet give tilladelse hertil, hvis behandlingen ikke foretages for en offentlig myndighed. Datatilsynet har mulighed for at fastsætte vilkår i forbindelse med en sådan tilladelse.

Sagen blev forelagt for Datarådet, bl.a. fordi Datatilsynet ikke tidligere havde taget stilling til behandling af biometriske data med henblik på entydig identifikation efter databeskyttelsesforordningen og databeskyttelseslovens regler, idet sådanne oplysninger – modsat efter de tidligere gældende regler – er følsomme oplysninger.

Datatilsynet vurderede, at betingelserne var opfyldt og gav tilladelse til Brøndbyernes I.F. Fodbold til behandling af biometriske data i medfør af databeskyttelseslovens § 7, stk. 4, i forbindelse med adgangskontrol ved brug af automatisk ansigtsgenkendelse. Tilladelsen blev givet på følgende vilkår:

1. Tilladelsen gælder ved afvikling af fodboldlandskampe, fodboldkampe, herunder træningskampe med deltagelse af hold fra Superligaen, 1. og 2. division samt ved fodboldkampe i UEFA-regi på Brøndby Stadion.
2. Meddelelse af karantæne skal ske på et sagligt og proportionalt grundlag i forhold til overtrædelse af ordensreglementet for Brøndby IF og Superligaen.
3. Personoplysninger, der behandles som led i ansigtsgenkendelsessystemet, der ikke resulterer i et match med oplysninger fra Brøndby IF's interne karantæneliste, må ikke lagres.
4. Personoplysninger, der behandles som led i ansigtsgenkendelsessystemet, der resulterer i et match med oplysninger fra Brøndby IF's interne karantæneliste, skal slettes umiddelbart efter enhver kamp på Brøndby Stadion.
5. Brøndby IF skal iagttage oplysningspligten ved indsamling af personoplysninger. Brøndby IF skal desuden ved skiltning eller på anden tydelig måde give oplysning om, at der foretages adgangskontrol, herunder behandling af biometriske data ved brug af et automatisk ansigtsgenkendelsessystem.
6. Personoplysninger, der behandles som led i ansigtsgenkendelsessystemet skal transporteres til og opbevares krypteret på serveren med ajourførte og bredt anerkendte krypteringsalgoritmer.
7. Overvågningskameraerne skal installeres på et separat VLAN og må ikke være eksponeret mod internettet.
8. Brøndby IF skal føre adgangskontrol med ansigtsgenkendelsessystemet, herunder
   - autorisation af medarbejdere til betjening af ansigtsgenkendelsessoftwaren og logning af manuelle opslag i systemet,
   - anvendelse af to-faktor-godkendelse i log-in processen.
9. Eventuelle ændringer i de forhold, der er omfattet af ansøgningen, skal meddeles Datatilsynet.

Ovenstående vilkår er supplerende og præciserende i forhold til reglerne i databeskyttelsesforordningens og databeskyttelsesloven, hvorfor de databeskyttelsesretlige regler finder anvendelse i det omfang, at der er tale om forhold, der ikke er reguleret i vilkårene.

Bekendtgørelse om videregivelse af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2

Datatilsynet har den 18. december 2019 fastsat bekendtgørelse nr. 1509 om videregivelse af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2, samt i den forbindelse offentliggjort en supplerende vejledning. Bekendtgørelsen og vejledningen er udarbejdet efter beslutning i Datarådet

og finder anvendelse fra den 1. januar 2020 for enhver videregivelse af personoplysninger, der forud for videregivelsen har været behandlet efter reglerne i databeskyttelseslovens § 10. Bekendtgørelsen og vejledningen kan findes via Retsinformation og/eller Datatilsynets hjemmeside.

Bekendtgørelsen har til formål at sikre beskyttelsen af personoplysninger, der har været behandlet i statistisk eller videnskabeligt øjemed efter databeskyttelseslovens § 10, stk. 1 og 2, når oplysningerne skal videregives til en ny dataansvarlig i de tilfælde, hvor videregivelsen ikke er omfattet af de i § 10, stk. 3, nævnte krav om tilladelse.

Bekendtgørelsen er overordnet opdelt i vilkår for behandling af personoplysninger hos henholdsvis den afgivende og den modtagende dataansvarlige. Endvidere finder databeskyttelsesforordningen og databeskyttelseslovens regler under alle omstændigheder anvendelse, i det omfang forholdet ikke er reguleret særskilt i bekendtgørelsen.

I de tilfælde, hvor videregivelsen kræver Datatilsynets forudgående tilladelse efter databeskyttelseslovens § 10, stk. 3, vil der til Datatilsynets tilladelse til den konkrete tilladelse være knyttet specifikke vilkår, der træder i stedet for kravene i bekendtgørelsen.

Videregivelse efter databeskyttelseslovens § 10, stk. 3

Der skal efter databeskyttelseslovens § 10, stk. 3, indhentes forudgående tilladelse fra Datatilsynet til videregivelse af personoplysninger, der har været behandlet med henblik på statistiske eller videnskabelige undersøgelser efter § 10, stk. 1 og 2, i følgende tre tilfælde:

- når videregivelsen sker til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde, herunder til EØS-lande
- når videregivelsen vedrører biologisk materiale, for eksempel blod- eller vævsprøver
- når videregivelsen sker med henblik på offentliggørelse i anerkendte videnskabelige tidsskrifter eller lignende.

Datatilsynet har udarbejdet en blanket til anmodninger om tilladelse til videregivelse, der indeholder en vejledende tekst om, hvad ansøgere især skal være opmærksomme på. Blanketten kan findes via Datatilsynets hjemmeside.

Ved enhver anmodning om tilladelse vurderer Datatilsynet, om der er forhold, der taler imod at give tilladelse til videregivelse, herunder antallet af registrerede og mængden af personoplysninger om den enkelte registrerede.

Videregivelse til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde

Tilladelseskravet i databeskyttelseslovens § 10, stk. 3, nr. 1, omfatter videregivelse til dataansvarlige, der er etableret uden for EU (også kaldet tredjelande), herunder i EØS-lande (Island, Liechtenstein og Norge), samt til internationale organisationer.

Datatilsynet vil sædvanligvis meddele tilladelse til en overførsel til sikre tredjelande eller internationale organisationer efter databeskyttelsesforordningens artikel 45 og til EØS-lande, da en overførsel hertil i andre tilfælde (dvs. uden for § 10, stk. 3) vil kunne ske uden yderligere foranstaltninger.

I andre tilfælde skal den afgivende dataansvarlige sikre, at der foreligger et overførselsgrundlag efter databeskyttelsesforordningens artikel 46, 47 eller 49. Datatilsynet modtager hovedsaglig anmodninger, hvor EU-Kommissionens standardkontrakter er anført som overførselsgrundlag.

Videregivelse der vedrører biologisk materiale

Kravet om tilladelse i databeskyttelseslovens § 10, stk. 3, nr. 2, omfatter videregivelse af fysisk biologisk materiale, der kan anvendes – eventuelt ved yderligere bearbejdning – til at identificere enkeltpersoner.

Datatilsynets tilladelse skal således ikke indhentes til videregivelse af såkaldt "tørre data", også selv om sådanne data netop er udledt fra biologisk materiale.

Bortset fra, at videregivelsen har et fysisk aspekt, og at der ikke er tale om elektroniske oplysninger, adskiller videregivelsessituationen sig ikke betydeligt i forhold til anden tilsvarende videregivelse af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2. Størstedelen af disse anmodninger imødekommes derfor uden videre med en tilladelse.

Videregivelse med henblik på offentliggørelse i anerkendte videnskabelige tidsskrifter eller lignende

Databeskyttelseslovens § 10, stk. 3, nr. 3, om videregivelse med henblik på offentliggørelse i et anerkendt videnskabeligt tidsskrift eller lignende omfatter enhver videregivelse, hvor det bagvedliggende formål er en publicering af en videnskabelig artikel.

Følgende situationer er omfattet:

- en videnskabelig artikel, der ønskes publiceret i et anerkendt tidsskrift eller lignende, indeholder pseudonymiserede personoplysninger.
- personoplysninger, der indgår i en statistisk eller videnskabelig undersøgelse, ønskes videregivet til et anerkendt tidsskrift eller lignende med henblik på udførelse af en fagfællebedømmelse.
- personoplysninger, der indgår i en statistisk eller videnskabelig undersøgelse, ønskes videregivet til andre dataansvarlige end selve det anerkendte tidsskrift – f.eks. til et selvstændigt datarepositorium eller en database.

Datatilsynets vurdering af anmodninger om tilladelse til videregivelse vil navnlig tage sigte på det tidsskrift, som ansøgeren ønsker at publicere en artikel i, eller på den database, som personoplysningerne ønskes tilgængeliggjort i.

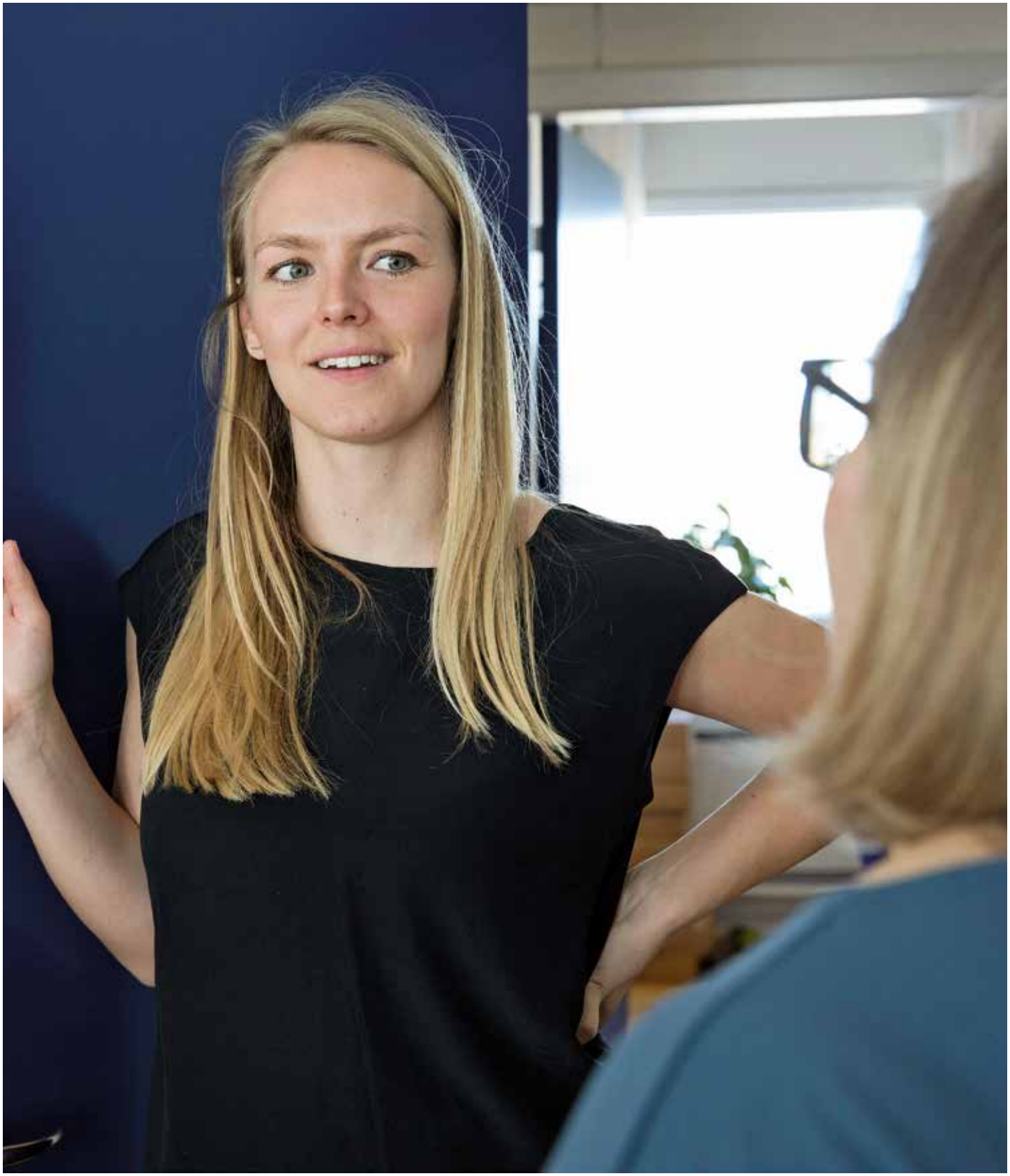
Datatilsynet modtager jævnligt anmodninger, som tilsynet ikke er i stand til at behandle, fordi anmodningen er indgivet på et tidspunkt, hvor ansøgeren alene har et ønske om publicering uden at have vished om, hvilket tidsskrift eller lignende, der ønskes videregivet til.

Når der foreligger oplysning om, hvilket tidsskrift der er tale om, har Datatilsynet især fokus på, om tidsskriftet er optaget på den seneste version af BFI-listen for serier på Uddannelses- og Forskningsministeriets hjemmeside.

Datatilsynet offentliggør løbende meddelte tilladelser og afslag på tilladelse efter databeskyttelseslovens § 10, stk. 3, på Datatilsynets hjemmeside.

Nye standardvilkår for kreditoplysningsbureauer

Privates behandling af oplysninger med henblik på (erhvervsmæssig) videregivelse af oplysninger til bedømmelse af en persons eller en virksomheds økonomiske soliditet og kreditværdighed – i daglig tale omtalt kreditoplysningsbureauer – kræver, som det var tilfældet efter reglerne i den tidligere gældende persondatalov, Datatilsynets tilladelse, inden behandlingen iværksættes.



I forlængelse af overgangen til databeskyttelsesforordningen og databeskyttelsesloven har Datatilsynet med udgangspunkt i de vilkår, som blev stillet i henhold til persondataloven, opdateret vilkårene for kreditoplysningsbureauer. De nye vilkår er tilgængelige på Datatilsynets hjemmeside, hvor der også findes en vejledning, som nærmere beskriver, hvornår der er tale om kreditoplysningsbureauvirksomhed, og hvordan ansøgningsprocessen foregår. Vejledningen indeholder også en gennemgang af de enkelte vilkår.

Tilladelse til behandling af personoplysninger, som er opnået i henhold til reglerne i den tidligere gældende persondatalov, gælder, indtil den erstattes af en ny tilladelse efter databeskyttelsesloven.

Datatilsynet vil kontakte kreditoplysningsbureauer, som har fået tilsynets tilladelse efter de tidligere gældende regler, med henblik på udstedelse af en ny tilladelse på de opdaterede vilkår.

Nye standardvilkår for advarselsregistre og spærrelister

Databeskyttelsesloven indeholder et krav om, at private dataansvarlige, som ønsker at føre et såkaldt advarselsregister eller en spærreliste, skal indhente tilladelse fra Datatilsynet, inden behandling af oplysninger om registrerede påbegyndes.

Ved advarselsregistervirksomhed forstås en dataansvarlig, som behandler oplysninger med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret. En spærreliste er en særlig form for advarselsregister, der specifikt angår spærring af betalingskort og andre betalingsinstrumenter og har til formål at undgå bl.a. misbrug af et stjålet eller på anden vis bortkommet betalingskort.

Kravet om indhentelse af Datatilsynets forudgående tilladelse til behandling af oplysninger i forbindelse med førelse af et advarselsregister eller en spærreliste fulgte også af den tidligere gældende persondatalov. Kravet gælder alene for private dataansvarlige, og skyldes det forhold, at behandlinger på dette område kan medføre meget alvorlige skadevirkninger for de involverede.

Datatilsynet har i forbindelse med overgangen til de nye databeskyttelsesregler opdateret vilkårene for privates behandling af oplysninger i forbindelse med førelse af advarselsregistre og spærrelister. Vilkårene præciserer og supplerer reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

De nye vilkår er tilgængelige via Datatilsynets hjemmeside, hvor der også findes vejledninger til vilkårene, som nærmere beskriver, hvornår der er tale om henholdsvis et advarselsregister og en spærreliste, og hvordan ansøgningsprocessen foregår. Vejledningerne indeholder også en gennemgang af de enkelte vilkår.

En tilladelse meddelt i henhold til reglerne i den tidligere gældende persondatalov gælder, indtil den erstattes af en ny tilladelse efter databeskyttelsesloven.

Datatilsynet vil kontakte de dataansvarlige, som har fået tilsynets tilladelse efter de tidligere gældende regler, med henblik på udstedelse af en ny tilladelse på de opdaterede vilkår.

Nye vilkår for førelse af retsinformationssystemer

Efter databeskyttelseslovens § 9 kan oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, og artikel 10 behandles, hvis dette alene sker med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig for førelsen af systemerne.

Med et retsinformationssystem menes navnlig et system, der er til rådighed for en bredere kreds af abonnenter for at sikre en ensartet retsanvendelse.

Hvis personoplysninger behandles efter lovens § 9, stk. 1, må disse oplysninger ikke senere behandles i andet øjemed. Det samme gælder behandling af andre personoplysninger, hvis behandlingen alene foretages med henblik på at føre retsinformationssystemer.

I henhold til databeskyttelseslovens § 26, stk. 1, nr. 3, skal en privat dataansvarlig forinden iværksættelse af en behandling indhente Datatilsynets tilladelse, når behandlingen udelukkende finder sted med henblik på at føre retsinformationssystemer. Efter lovens § 26, stk. 4, kan tilsynet i forbindelse med meddelelse af en tilladelse efter stk. 1 fastsætte vilkår for udførelsen af behandlingerne. Endvidere følger det af lovens § 9, stk. 3, at tilsynet kan meddele nærmere vilkår for de behandlinger, der nævnes i stk. 1. Det samme gør sig gældende for de oplysninger, der er nævnt i forordningens artikel 6, som alene behandles i forbindelse med førelsen af retsinformationssystemer. De nye vilkår er tilgængelige via Datatilsynets hjemmeside.

Datatilsynet har med udgangspunkt i de vilkår, som blev stillet i henhold til persondataloven, opdateret vilkårene for førelse af retsinformationssystemer.

Vilkårene er supplerende i forhold til reglerne i databeskyttelsesforordningen og databeskyttelsesloven, og i et vist omfang er de udtryk for en præcisering af lovens regler. Det er reglerne i databeskyttelsesforordningen og databeskyttelsesloven, som finder anvendelse, i det omfang der er tale om forhold, som ikke er reguleret i vilkårene.

En tilladelse, som er meddelt i henhold til reglerne i den nu ophævede persondatalov, gælder, indtil den erstattes af en ny tilladelse efter databeskyttelsesloven.

Internationalt samarbejde

Med databeskyttelsesforordningen har det internationale samarbejde fået en helt ny betydning. Databeskyttelsesområdet er således med forordningen i langt højere omfang reguleret på EU-plan, hvilket bl.a. kommer til udtryk gennem etableringen af et formaliseret samarbejde tilsynsmyndighederne imellem.

Dette afspejler sig i Datatilsynets daglige arbejde i forhold til både udarbejdelse af generel vejledning og behandling af konkrete sager og tilsyn. Det er derfor af afgørende betydning, at Datatilsynet prioriterer det internationale arbejde og i den forbindelse får gjort danske synspunkter gældende.

Datatilsynets mål for det internationale arbejde er at være en aktiv og respekteret medspiller, der via dialog og konstruktivt samarbejde sikrer dansk indflydelse på de beslutninger, der træffes, såvel på det generelle plan i form af vejledninger og udtalelser mv. som på det konkrete plan i forhold til afgørelser i konkrete sager. Et pejlemærke i den forbindelse er den velkendte danske pragmatiske tilgang, idet der er hensyn at tage til såvel de registrerede som virksomheder og myndigheder.

For at kunne leve op til denne målsætning, er det internationale arbejde nødt til at være en integreret del af det daglige arbejde i hele tilsynet, og Datatilsynets strategi for det internationale arbejde, som blev færdiggjort i 2019, skal være med til at sikre dette, ligesom strategien skal sikre, at tilsynet kan deltage aktivt og kvalificeret såvel på arbejdsgruppeniveau som på de månedlige møder i Det Europæiske Databeskyttelsesråd og på den måde få gjort danske synspunkter gældende i rette tid og på rette sted. Med henblik på at sikre dette har tilsynet i løbet af 2019 bl.a. fastlagt processer, der skal sikre den interne koordinering og stillingtagen til dansk holdning fra opstarten af arbejdet med f.eks. en ny vejledning til dennes endelige vedtagelse på et møde i rådet.

Datatilsynet har i øvrigt yderligere intensiveret sin deltagelse i det internationale samarbejde i 2019 og deltager nu som udgangspunkt i alle arbejdsgrupper under Det Europæiske Databeskyttelsesråd, ligesom tilsynet også aktivt involverer sig i arbejdet med udarbejdelse af vejledninger mv., både som ledende tilsyn på udvalgte dokumenter og som medforfatter på andre.

Det Europæiske Databeskyttelsesråd (EDPB)

Det Europæiske Databeskyttelsesråd er et uafhængigt EU-organ, som skal sikre en ensartet anvendelse af databeskyttelsesforordningen og retshåndhævelsesdirektivet i hele EU. På engelsk hedder rådet European Data Protection Board (EDPB). Rådets medlemmer består af repræsentanter for medlemsstaternes tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). EU-Kommissionen kan deltage i rådets aktiviteter og møder, men har ikke stemmeret. Danmark er repræsenteret ved Datatilsynets direktør.

Med henblik på at sikre en ensartet anvendelse af reglerne om persondatabeskyttelse kan Det Europæiske Databeskyttelsesråd bl.a.:

- give generel vejledning for at præcisere lovgivningen (udkast til vejledninger sendes ofte i offentlig høring)
- fremme samarbejdet og en effektiv udveksling af oplysninger og bedste praksis mellem nationale tilsynsmyndigheder

- komme med udtalelser om ethvert spørgsmål om den generelle anvendelse af databeskyttelsesforordningen eller ethvert spørgsmål, der har indvirkning i mere end én medlemsstat samt udtalelser om visse afgørelser, der træffes af medlemsstaters tilsynsmyndigheder, og som har grænseoverskridende virkninger
- træffe bindende afgørelser omkring fortolkningen af reglerne, f.eks. hvor tilsynsmyndigheder har forskellige opfattelser af, hvordan en konkret sag skal afgøres, eller hvis en national myndighed ikke følger rådets udtalelse om et udkast til afgørelse
- rådgive EU-Kommissionen om ethvert spørgsmål om beskyttelse af personoplysninger i EU

Det Europæiske Databeskyttelsesråds opgaver fremgår af databeskyttelsesforordningens artikel 70.

Det Europæiske Databeskyttelsesråd har sin egen forretningsorden, som indeholder de vigtigste regler for rådets drift, herunder organisering, samarbejdet mellem medlemmer og arbejdsmetoder. Rådet bistås af et sekretariat, som udfører sine opgaver efter instruks fra formanden. Sekretariat ligger i Bruxelles, hvor rådets møder også afholdes.

Det Europæiske Databeskyttelsesråd holder møder af 2 dages varighed en gang om måneden. Rådet afholdt i 2019 11 møder. Datatilsynet deltager i møderne. Hvor afstemning er nødvendig, træffer rådet afgørelse med simpelt flertal blandt sine medlemmer, medmindre andet følger af databeskyttelsesforordningen.

I 2019 var der fortsat fokus på udarbejdelse af vejledninger, men i tillæg hertil behandlede rådet også de første sager i den såkaldte sammenhængsmekanisme, som skal være med til at sikre en ensartet anvendelse af reglerne i de enkelte lande.

Af særlig dansk interesse kan nævnes, at Datatilsynet i 2019 offentliggjorde standardbestemmelser til brug for indgåelse af en databehandleraftale. Forud herfor havde tilsynet, som databeskyttelsesforordningen foreskriver, indhentet en udtalelse fra EDPB vedrørende aftalens overensstemmelse med kravene i forordningen.

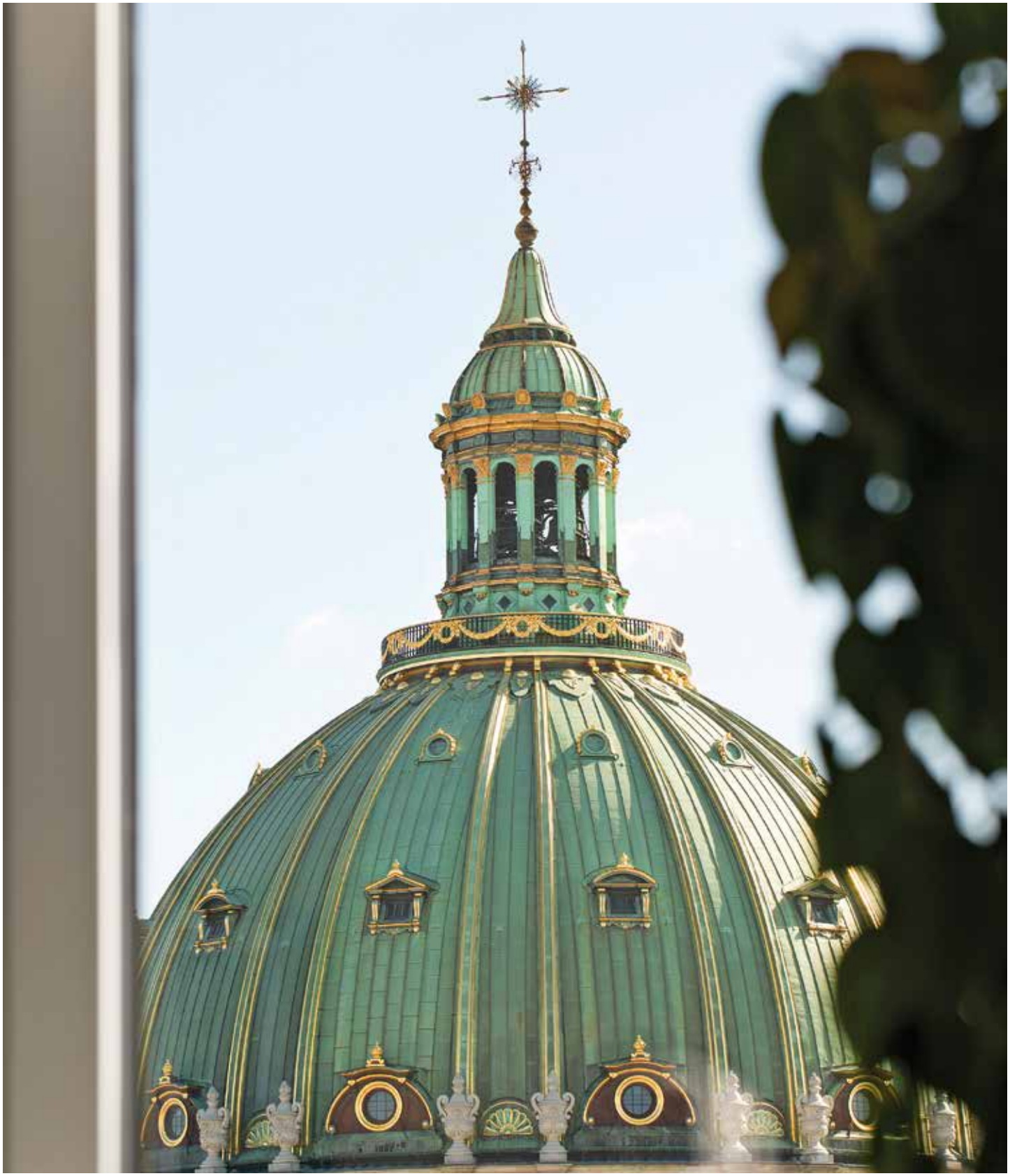
Tidligere på året havde EDPB også afgivet en udtalelse vedrørende Datatilsynets udkast til liste over situationer, hvor det er obligatorisk at udarbejde konsekvensanalyser, som Datatilsynet havde indsendt.

Endelig blev også den første danske grænseoverskridende klagesag afgjort i den såkaldte One-Stop-Shop mekanisme.

Som nævnt ovenfor i afsnittet om det internationale samarbejde er Datatilsynet aktivt involveret i rådets arbejde bl.a. gennem deltagelse i flere ekspertarbejdsgrupper under rådet og i forberedelsen af vejledninger og afgørelser.

Arbejdet med forberedelsen af vejledninger, udtalelser, afgørelser mv., som Databeskyttelsesrådet skal træffe beslutninger om, forestås primært af pt. 12 ekspertarbejdsgrupper, som mødes med 1-2 måneders intervaller, og som imellem de fysiske møder udveksler skriftlige bemærkninger og afholder telefonmøder.

Det Europæiske Databeskyttelsesråd har sin egen hjemmeside, www.edpb.europa.eu, ligesom det har sin egen Twitter-profil, @EU_EDPB, og egen LinkedIn profil, European Data Protection Board, hvor det er muligt at følge rådets arbejde. På Datatilsynets hjemmeside bliver der også løbende offentliggjort vejledninger mv. fra Det Europæiske Databeskyttelsesråd.



Særlige internationale tilsynsforpligtelser

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. Datatilsynet foretog i slutningen af 2018 et tilsyn med Rigspolitiets behandling af personoplysninger i Schengen-informationssystemet. Tilsynet forventes afsluttet i første halvår 2020.

Som led i tilsynet med behandling af personoplysninger i SIS II deltager Datatilsynet endvidere i Koordinationsgruppen for tilsynet med anden generation af Schengen-informationssystemet (SIS II SCG). Gruppen, der består af repræsentanter for Den Europæiske Tilsynsførende for Databeskyttelse, de nationale datatilsyn i EU-medlemslandene og de nationale datatilsyn i Island, Norge, Liechtenstein og Schweiz, har i 2019 afholdt to møder.

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.

Told-informationssystemet (CIS)

Toldinformationssystemet (CIS) 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. Datatilsynet fører således tilsyn med behandlingen af informationer i den danske del af det fælleseuropæiske toldinformationssystem.

Datatilsynet deltager endvidere på EU-niveau i Den Fælles Tilsynsmyndighed for Toldinformationssystemet (JSA Customs) og Koordinationsgruppen for tilsynet med Toldinformationssystemet (CIS SCG). Der har i 2019 været afholdt to møder i Koordinationsgruppen for tilsynet med Toldinformationssystemet.

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

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 endvidere i Koordinationsgruppen for tilsynet med Eurodac (Eurodac SCG). Koordinationsgruppen består af repræsentanter for Den Europæiske Tilsynsførende for Databeskyttelse, de nationale datatilsyn i EU-medlemslandene og de nationale datatilsyn i Island, Norge, Liechtenstein og Schweiz.

I 2019 har der været afholdt to møder, hvor gruppen bl.a. har haft besøg af repræsentanter for EU-Kommissionen og eu-LISA med henblik på orienteringer om den seneste udvikling på området og drøftelser af de aktuelle databeskyttelsesretlige problemstillinger, herunder EU-Kommissionens forslag til en ny Eurodac-forordning. Herudover har gruppen bl.a. drøftet følgende emner:

- EU-Kommissionens to forslag til forordninger, som skal give det nye European Travel Information and Authorisation System (ETIAS) adgang til andre EU systemer.
- Udøvelsen af de registreredes rettigheder, herunder et samarbejde med Fundamental Rights Agency (FRA) om et nyt værktøj til at oplyse de registrerede om deres rettigheder.

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. Datatilsynet foretog i slutningen af 2018 et tilsyn med behandlingen af personoplysninger i Visum-informationssystemet. Tilsynet forventes afsluttet i første halvår 2020.

Som led i tilsynet med behandling af personoplysninger i VIS deltager Datatilsynet endvidere i Koordinationsgruppen for tilsynet med Visum-informationssystemet (VIS SCG). Gruppen består af repræsentanter for Den Europæiske Tilsynsførende for Databeskyttelse, de nationale datatilsyn i EU-medlemslandene og de nationale datatilsyn i Island, Norge, Liechtenstein og Schweiz. I 2019 har der været afholdt to møder, hvor koordinationsgruppen bl.a. har haft besøg af repræsentanter for EU-Kommissionen og eu-LISA, som har orienteret gruppen om den seneste udvikling på området, herunder EU-Kommissionens forslag til en ny VIS-forordning. Der har herudover bl.a. været drøftet følgende emner:

- EU-Kommissionens to forslag til forordninger, som skal give det nye European Travel Information and Authorisation System (ETIAS) adgang til andre EU-informationssystemer.
- Databeskyttelsesretlig træning af personale hos myndigheder, der har adgang til VIS.

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 er et informationssystem oprettet af EU-Kommissionen, som overordnet har til formål at lette europæiske myndigheders grænseoverskridende samarbejde og sagsbehandling i henhold til en given EU-retsakt.

Datatilsynet er udpeget som tilsynsmyndighed i relation til behandlingen af personoplysninger i den danske del af systemet. På EU-niveau deltager Datatilsynet endvidere i Koordinationsgruppen for tilsynet med Indre Markeds-informationssystemet (IMI SCG). Der har i 2019 været afholdt et enkelt møde i gruppen.

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

Eurojust

Eurojust 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 (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).

Datatilsynet var repræsenteret i den Fælles Kontrolinstans (JSB) – en uafhængig kontrolinstans oprettet i medfør af artikel 23 i Eurojust-afgørelsen, som kollektivt overvågede de af Eurojusts aktiviteter, der indebar behandling af personoplysninger. Der har årligt – herunder i 2019 – været afholdt ét møde i den fælles kontrolinstans.

Ved forordning af 14. november 2018 (Europa-Parlamentets og Rådets forordning (EU) 2018/1727) er Rådets afgørelse om oprettelse af Eurojust med virkning fra den 12. december 2019 ophævet, og Eurojust er nu oprettet ved forordningen.

Den Fælles Kontrolinstans (JSB) eksisterer herefter ikke længere, og kontrollen med Eurojusts behandling af personoplysninger foretages nu af Den Europæiske Tilsynsførende for Databeskyttelse (EDPS).

Europarådet

Europarådet blev oprettet i 1949 og danner i dag rammen om et samarbejde mellem 47 lande, herunder de 27 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.

I 2019 deltog Datatilsynet i Europarådets konvention 108-arbejdsgruppemøde i Strasbourg. På mødet drøftedes bl.a. en fremtidig standard for global databeskyttelse. Herudover deltog arbejdsgruppen i den såkaldte Octopus-konference, hvor en tillægsprotokol til Budapest-konventionen om IT-kriminalitet blev drøftet.

Berlin-gruppen

International Working Group on Data Protection in Technology, også bare kaldet Berlin-gruppen, har i 2019 afholdt to møder. I april mødtes gruppen i Bledt, og i oktober afholdtes gruppens møde i Bruxelles.

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

Berlin-gruppens fokus på privatliv og sikkerhed har i 2019 ført til vedtagelsen af tre Working Papers. Det ene omkring risici ved børns brug af "Smart Devices", typisk netværksforbundet legetøj. Det andet om beskyttelsen af børns brug af on-line services. Det tredje om forbundne biler.

Dokumentet om "Smart Devices" omhandler også det såkaldte "internet of things" IOT. Særligt her opkobling på internettet af diverse artikler, aktivitetsmålere og legetøj, alt målrettet mod børn og unge. Der er i dokumentet fokus på den betydelige informationsindsamling hos den enkelte og det faktum, at enhederne typisk ikke har nogen – eller kun ringe – sikkerhed. Gruppens mål har været at få lavet beskrivelser og oplæg til standarder, der giver brugere af sådant udstyr mulighed for dels at vide hvordan og hvor oplysninger indsamles og lagres, dels at sikre at enhederne kan opdateres således, at sikkerheden ikke kompromitteres.

Dokumentet om forbundne biler, de såkaldte "connected cars", konsoliderer 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" bliver behandlet. Udviklingen går mere og mere imod biler med fast opkobling og brug af internetbaserede apps. Dokumentet beskriver de implikationer teknologien har for såvel privatliv som databeskyttelse, og hvordan brugen kan ske transparent og under brugerens kontrol.

I årets løb har Berlin-gruppen også fortsat arbejdet med aktuelle emner, som indeholder problemstillinger med hensyn til databeskyttelse og beskyttelse af privatliv, eksempelvis dataportabillitet, blockchain, webtracking, smart dust, quantum computing, 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, da tilsynene har mange fælles interesser og synspunkter. De nordiske tilsyn er derfor i jævnlig kontakt om såvel konkrete som generelle emner og drøfter også emner af fælles interesse i forbindelse med deltagelse i møder i Det Europæiske Databeskyttelsesråd og dets ekspertarbejdsgrupper.

I tillæg hertil afholder tilsynene en gang om året et fællesnordisk samarbejdsmøde med deltagelse af såvel ledelse, som sagsbehandlere og it-eksperter samt et mindre opfølgningsmøde senere på året.

Det nordiske samarbejdsmøde blev i 2019 afholdt i Stockholm, hvor man med en erklæring fulgte op på den København-erklæring, som tilsynene vedtog i 2018, da Datatilsynet var vært for mødet. Stockholm-erklæringen lægger især vægt på at fortsætte det tætte nordiske samarbejde på databeskyttelsesområdet – både i EU-sammenhænge og landene imellem.

Den europæiske konference

Den Europæiske Konference for datatilsynsmyndigheder, også kaldet Forårskonferencen, afholdes en gang årligt. Konferencen, der kun er for europæiske datatilsyn, blev i 2019 afholdt i Georgien. Datatilsynet deltog ikke i konferencen i 2019.

Den internationale konference

Den Internationale Konference for Databeskyttelsesmyndigheder er en årlig konference med deltagere fra hele verden. Konferencen består dels af en lukket del forbeholdt ledere af de forskellige datatilsyn, som er medlem af konferencen, og en åben del tilgængelig for alle.

Konferencen, der hidtil har været kendt under navnet International Conference of Data Protection and Privacy Commissioners (ICDPPC), besluttede på 2019-konferencen at skifte navn til Global Privacy Assembly (GPA). Fremadrettet kan forsamlingens arbejde, herunder de resolutioner, der vedtages på de årlige konferencer, følges via hjemmesiden www.globalprivacyassembly.org.

I 2019 vedtog man på konferencen, der blev afholdt i Tirana, Albanien, bl.a. resolutioner om et effektivt samarbejde på tværs af grænser, om voldeligt og ekstremistisk indhold på sociale medier, om betydningen af menneskelige fejl i relation til sikkerhedsbrud og om samarbejdet mellem databeskyttelses-, forbruger- og konkurrenceretsmyndigheder med henblik på at sikre en høj standard for databeskyttelse i den digitale økonomi. Datatilsynet var ikke repræsenteret på årets konference.

I regi af GPA er der nedsat forskellige arbejdsgrupper, herunder den såkaldte Berlin-gruppe, som Datatilsynet deltager i. Datatilsynet følger endvidere arbejdet i "Ethics and Data Protection in Artificial Intelligence" og "Digital Citizens and Consumers" arbejdsgrupperne.

Grønland og Færøerne

Efter anmodning fra Grønlands Selvstyre blev en særlig udgave af den tidligere gældende persondatalov ved kongelig anordning pr. 1. december 2016 sat i kraft for Grønland. Loven afløste de hidtil gældende registerlove fra 1978.

Persondataloven er endvidere med virkning fra den 1. juli 2017 sat i kraft for rigsmyndighedernes behandling af oplysninger på Færøerne. For den behandling af personoplysninger på Færøerne, der foretages af færøske myndigheder og af private virksomheder, organisationer mv. gælder den færøske persondatalov. Tilsynsmyndighed i forhold til denne lov er det færøske datatilsyn Dátueftirlitið.

Datatilsynet har i 2019 kun modtaget få konkrete henvendelser om behandling af personoplysninger i Grønland eller ved rigsmyndighederne på Færøerne og har ikke behandlet mere principielle sager herom.

Datatilsynet modtog i 2019 imidlertid 104 anmeldelser om behandling af personoplysninger fra grønlandske myndigheder og 19 anmeldelser fra grønlandske virksomheder mv. Formålet med anmeldelsesordningen er at give Datatilsynet mulighed for at kunne kontrollere visse behandlinger af personoplysninger. Anmeldelsesordningen har endvidere til formål at gøre det muligt for offentligheden at gøre sig bekendt med behandlingerne.

På Datatilsynets hjemmeside findes fortegnelser over igangværende behandlinger, som myndigheder og virksomheder mv. i Grønland har anmeldt til tilsynet, og som tilsynet har færdigbehandlet.

2.del: Retshåndhævelsesloven

Retshåndhævelsesloven (lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger med senere ændringer) gælder for politiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og for anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, når behandlingen foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Datatilsynet fører tilsyn med enhver behandling omfattet af loven med undtagelse af behandling af oplysninger, der foretages for domstolene. Tilsynet med domstolene foretages af henholdsvis Domstolsstyrelsen og retterne i overensstemmelse med retshåndhævelseslovens regler.

I 2019 har Datatilsynet bl.a. behandlet klagesager og anmeldelser fra de retshåndhævende myndigheder om brud på persondatasikkerheden.

Anmeldelse af brud på persondatasikkerheden

Datatilsynet modtog den 12. juli 2019 en anmeldelse fra Rigspolitiets Center for Databeskyttelse om et brud på persondatasikkerheden hos Sydsjællands og Lolland-Falsters Politi.

Sikkerhedsbruddet bestod i, at en privatperson var kommet i besiddelse af en anmeldelsesrapport fra en straffesag fra Sydsjællands og Lolland-Falsters Politi. Bruddet skete efter det oplyste ved, at en medarbejder i politikredsen – som led i sit arbejde – havde taget anmeldelsesrapporten med hjem, hvorefter en person, som havde adgang til medarbejderens hjem, var kommet i besiddelse af anmeldelsesrapporten og havde optaget billeder af denne.

Anmeldelsesrapporten indeholdt oplysninger om to registrerede, herunder oplysninger om deres personnummer og helbredsforhold samt oplysninger om strafbare forhold.

Sydsjællands og Lolland-Falsters Politi blev bekendt med bruddet, da privatpersonen den 15. august 2018 rettede henvendelse til Københavns Vestegns Politi og oplyste at være i besiddelse af rapporten. Politikredsen var imidlertid ikke opmærksom på, at hændelsen skulle anses for et brud på persondatasikkerheden, og at der skulle ske anmeldelse af bruddet til Datatilsynet uden unødig forsinkelse.

Sydsjællands og Lolland-Falsters Politi underrettede de berørte registrerede om bruddet henholdsvis den 24. juli og 3. september 2019. Idet Rigspolitiets Center for Databeskyttelse imidlertid vurderede, at disse underretninger var mangelfulde, underrettede politikredsen de registrerede på ny den 13. september 2019.

Efter en samlet vurdering af sagen fandt Datatilsynet, at Sydsjællands og Lolland-Falsters Politi ved utilsigtet at have givet adgang til personoplysninger, herunder oplysninger om personnummer, strafbare forhold og oplysninger om helbred, til uvedkommende ikke havde levet op til kravet om at gennemføre passende sikkerhedsforanstaltninger, jf. retshåndhævelseslovens § 27, stk. 1. Ved vurderingen heraf lagde Datatilsynet vægt på det oplyste om, at medarbejderen havde taget anmeldelsesrapporten med hjem, og at uvedkommende i den forbindelse havde fået adgang til oplysningerne.

Datatilsynet fandt endvidere, at Sydsjællands og Lolland-Falsters Politi ikke havde levet op til kravet om at anmelde brud på persondatasikkerheden til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet, jf. retshåndhævelseslovens § 28, stk. 1.

Endelig fandt Datatilsynet, at Sydsjællands og Lolland-Falsters Politi ikke havde underrettet de berørte registrerede uden unødig forsinkelse, jf. retshåndhævelseslovens § 29, stk. 1. Datatilsynet lagde i den forbindelse vægt på, at Sydsjællands og Lolland-Falsters Politi havde været bekendt med de berørte registreredes identitet allerede ved bruddets konstatering den 15. august 2018, og at der skete delvis underretning af de registrerede om bruddet henholdsvis den 24. juli 2019 og den 3. september 2019 og derefter fuldstændig underretning den 13. september 2019.

Samlet set fandt Datatilsynet, at der var grundlag for at udtale alvorlig kritik af, at Sydsjællands og Lolland-Falsters Politis behandling af personoplysninger ikke var sket i overensstemmelse med retshåndhævelses-lovens §§ 27, stk. 1, 28, stk. 1, og 29, stk. 1.

Klage over manglende indsigt

Datatilsynet traf den 18. november 2019 afgørelse i en sag, hvor en borger klagede over, at Københavns Politi ikke i tilstrækkelig grad havde besvaret borgerens anmodning om indsigt i de oplysninger, politikredsen behandlede om borgeren og dennes søn.

Efter retshåndhævelseslovens § 15, stk. 1, har en registreret som udgangspunkt ret til at få den dataansvarlige retshåndhævende myndigheds bekræftelse på, om der behandles oplysninger om vedkommende.

Retshåndhævelseslovens § 16, stk. 1, er en undtagelse til dette udgangspunkt, hvorefter retten til indsigt kan udsættes, begrænses eller nægtes, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for hensynet til de offentlige interesser, der er nævnt i retshåndhævelseslovens § 14, stk. 1 – herunder hensynet til at undgå at skade forebyggelsen, afsløringen, efterforskningen eller retsforfølgningen af strafbare handlinger eller fuldbyrdelsen af strafferetlige sanktioner.

Retshåndhævelseslovens § 16, stk. 3, giver endvidere den dataansvarlige retshåndhævende myndighed mulighed for i stedet at give meddelelse til den registrerede om, at det ikke kan oplyses, om der behandles oplysninger om den pågældende af hensyn til de samme formål, som er nævnt i lovens § 16, stk. 1.

Retshåndhævelseslovens § 16, stk. 4, fastsætter endvidere, at justitsministeren fastsætter nærmere regler om, hvilke kategorier af behandling der er omfattet af stk. 1, herunder om undtagelser fra retten til at få oplysninger efter § 15, for så vidt hensynene i stk. 1, må antages at medføre, at begæringer om indsigt i almindelighed må nægtes. Der er endnu ikke fastsat nærmere regler efter § 16, stk. 4, af relevans for den pågældende sag.

Det fremgik af sagen, at Københavns Politi havde meddelt borgeren indsigt i personoplysninger, som kredsen behandlede om borgeren efter retshåndhævelsesloven i tre sager om hastighedsovertrædelser. I besvarelsen til borgeren havde politikredsen endvidere oplyst, at kredsen – af hensyn til politiets efterforskning og forfølgelse af strafbare handlinger – hverken kunne be- eller afkræfte, om kredsen i øvrigt behandlede oplysninger om borgeren og dennes søn.

I sagen oplyste Københavns Politi, at det er politikredsens udgangspunkt – at uanset om kredsen behandler oplysninger om personen, der anmoder om indsigt, eller ej – at kredsen hverken be- eller afkræfter, om der i forbindelse med verserende sager behandles oplysninger omfattet af retshåndhævelsesloven, medmindre det konkret vurderes, at der bør gives oplysning herom, f.eks. hvis den pågældende person formodes at være bekendt med kredsens behandling af oplysninger, fordi vedkommende er blevet afhørt. Politikredsen havde i den konkrete sag ikke fundet grundlag for at afvige udgangspunktet om hverken at be- eller afkræfte, om der behandles oplysninger omfattet af retshåndhævelsesloven.

Datatilsynet fandt, at Københavns Politi ikke var berettigede til at afvise at meddele borgeren indsigt med henvisning til retshåndhævelseslovens § 16, stk. 3, idet politikredsen ikke have foretaget en konkret vurdering og angivet konkrete omstændigheder for, hvorfor det i borgerens specifikke situation var nødvendigt at fravige udgangspunktet om retten til indsigt.

Datatilsynet udtalte i den forbindelse, at det er tilsynets vurdering, at det ikke generelt og som hovedregel kan undlades at give indsigt og alene meddelelse efter § 16, stk. 3, i samtlige anmodninger om indsigt. Meddelelsen efter § 16, stk. 3, kan således alene gives på grundlag af en konkret vurdering af omstændighederne i den enkelte sag. Datatilsynet understregede i den forbindelse, at det er den dataansvarliges ansvar at besvare indsigtsanmodninger, herunder at imødekomme disse i videst muligt omfang. Datatilsynet bemærkede endvidere, at det er en væsentlig forringelse af de registreredes ret-

tigheder at undlade at meddele indsigt, når der ikke er et – i sagen – konkret begrundet behov herfor. Datatilsynet indskærpede derfor over for Københavns Politi, at kredsen fremover alene kunne undlade at meddele de registrerede indsigt, når der er konkrete omstændigheder i forhold til sagen, som gør, at udgangspunktet om at meddele indsigt efter retshåndhævelseslovens § 15, stk. 1, bør fraviges.

Datatilsynet udtalte på den baggrund alvorlig kritik af, at Københavns Politi ikke havde overholdt retshåndhævelseslovens § 15, stk. 1.

Det fremgik i øvrigt af sagen, at Københavns Politi først besvarede klagers anmodning om indsigt to måneder og otte dage efter anmodningen. Datatilsynet fandt, at politikredsen herved ikke havde levet op til retshåndhævelseslovens § 18, stk. 2. Efter denne bestemmelse skal den dataansvarlige snarest og på skrift besvare anmodninger om indsigt efter retshåndhævelsesloven. Er anmodningen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil samt om, hvornår anmodningen forventes besvaret. Datatilsynet udtalte på denne baggrund kritik af, at politikredsens behandling af personoplysninger ikke havde været i overensstemmelse med retshåndhævelseslovens § 18, stk. 2.

Databekymringspostkassen

Sammen med initiativet om nedsættelse af Dataetisk Råd foreslog den tidligere regering i 2018 oprettelsen af en særlig mailboks hos Datatilsynet, hvor borgere kan indsende deres databekymringer. De indsendte databekymringer skal være med til at understøtte Dataetisk Råd i dets opgaver.

Datatilsynet har i samarbejde med Dataetisk Råds sekretariatet på baggrund af ovenstående lanceret en databekymringspostkasse, hvor borgerne kan henvende sig via e-mail med deres databekymringer. Databekymringspostkassen blev af Datatilsynet officielt oprettet og lanceret den 4. juli 2019. Datatilsynet har siden lanceringen af postkassen og indtil udgangen af 2019 i alt modtaget 58 databekymringer.

Størstedelen af de indkomne databekymringer omhandler sundhedssektoren. Der er flere af data-bekymringerne, der vedrører samkørslen af personoplysninger i forskellige systemer samt opbevaringen af helbredsoplysninger og andre personoplysninger i både fysiske og elektroniske journaler. Når størstedelen af de indkomne databekymringer omhandler sundhedssektoren kan dette hænge sammen med, at der er tale om en sektor, hvor der behandles mange følsomme og fortrolige personoplysninger, og at borgerne er mere opmærksomme på behandlingen af disse personoplysninger.

Et andet tema, som mange af de indkomne databekymringer omhandler, er brugen af personoplysninger. Der ses således at være en generel bekymring blandt borgere om, at deres personoplysninger vil blive benyttet til andre formål, end oplysningerne er indsamlet til. Det kan også være en bekymring om videregivelse til andre parter, som borgeren ikke er oplyst om. Endvidere er en del borgere opmærksomme på, hvilke personoplysninger de videregiver, når de f.eks. skal foretage et køb online eller benytte en app. Dette kan ses som et øget fokus på værdien af personoplysninger. Bekymringen om opbevaringen af personoplysninger hænger for borgerne sammen med brugen af personoplysninger. Der ses en bekymring for, at ens personoplysninger ikke forbliver i "sikre hænder", men derimod misbruges. Flere borgere omtaler derudover bekymringen for manglende sletning af personoplysninger.

En del databekymringer efterspørger en højere grad af gennemsigtighed ved offentlige myndigheders brug og indsamling af personoplysninger. Når de offentlige myndigheder behandler personoplysninger forventer borgerne, at behandlingen sker sikkert og i overensstemmelse med indsamlingsgrundlaget. Det forventes også, at behandlingen sker fortroligt og af de rette mennesker. Databekymringerne vedrørende offentlige myndigheder fokuserer – som nævnt ovenfor – på sundhedssektoren, men børn- og ungeområdet er også i fokus. Der er f.eks. modtaget en bekymring for manglende anonymisering af børns trivselsundersøgelser og efterfølgende manglende sletning af disse oplysninger. Der er flere bekymringer, som omhandler sletning af personoplysninger. Dette bliver efterspurgt både hos offentlige myndigheder og private virksomheder. Der er hos borgere særligt fokus på personoplysninger, som er tilgængelige på internettet

Når det gælder eventuelle samarbejder mellem offentlige myndigheder og private virksomheder, er borgere bekymret for, at personoplysninger senere vil blive benyttet ulovligt af den private virksomhed, f.eks. i forbindelse med markedsføring. Der er også databekymringer om, hvilke oplysninger de private virksomheder er i besiddelse af.

Afslutningsvis kan det oplyses, at også emner som kunstig intelligens, sager nævnt i medierne og generel mistillid til brugen af personoplysninger kort blev berørt i enkelte modtagne databekymringer.

Bilag 1: Oversigt over lovgivning mv.

Love, bekendtgørelser og vejledninger

Databeskyttelsesforordningen

- Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

Databeskyttelsesloven

- Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Retshåndhævelsesdirektivet

- Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA.

Retshåndhævelsesloven

- Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger. Loven er senest ændret ved lov nr. 506 af 23. maj 2018 om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger.

Tv-overvågningsloven

- Lovbekendtgørelse nr. 1190 af 11. oktober 2007 om tv-overvågning. Loven er senest ændret ved lov nr. 506 af 23. maj 2018 om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger.

Relevante bekendtgørelser

- Bekendtgørelse nr. 1287 af 25. november 2010 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for Den Europæiske Union og Schengen-samarbejdet.
- Bekendtgørelse nr. 881 af 4. juli 2014 med senere ændringer om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret).
- Bekendtgørelse nr. 1080 af 20. september 2017 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG).
- Bekendtgørelse nr. 1079 af 20. september 2017 om behandling af personoplysninger i Politiets Efterforskningsstøttedatabase (PED).
- Bekendtgørelse nr. 1078 af 20. september 2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser.
- Bekendtgørelse nr. 1134 af 13. oktober 2017 om underretning ved udgang og løsladelse mv. samt ved medvirken i tv- eller radioprogrammer eller portrætinterview.
- Bekendtgørelse nr. 594 af 29. maj 2018 om behandling af personoplysninger i forbindelse med Forsvarets internationale operative virke.
- Bekendtgørelse nr. 1757 af 27. december 2018 om PNR-enhedens behandling af PNR-oplysninger i en overgangsperiode.

- Bekendtgørelse nr. 454 af 1. januar 2019 om forretningsorden for Datarådet.
- Bekendtgørelse nr. 1509 af 18. december 2019 om videregivelse af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2.

Relevante forarbejder mv.
- Justitsministeriets betænkning nr. 1565 om databeskyttelsesforordningen (2016/679) - og de retlige rammer for dansk lovgivning.
- Lovforslag nr. L 68 af 25. oktober 2017 om lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).
- Retsudvalgets betænkning af den 9. maj 2018 over Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

De nævnte love, bekendtgørelser og forarbejder kan findes på enten Retsinformations hjemmeside og/eller via Datatilsynets hjemmeside under punktet "Lovgivning".

Danske vejledninger
- Vejledning af september 2017 om samtykke (opdateret i september 2019)
- Vejledning af september 2017 om overførsel af personoplysninger til tredjelande (opdateret i juni 2019)
- Vejledning af oktober 2017 om databeskyttelsesforordningen (generel informationspjece)
- Vejledning af november 2017 om dataansvarlige og databehandlere
- Vejledning af december 2017 om databeskyttelsesrådgivere
- Vejledning af januar 2018 om fortegnelse
- Vejledning af januar 2018 om adfærdskodekser og certificeringsordninger (opdateret i december 2018)
- Vejledning af februar 2018 om håndtering af brud på persondatasikkerheden
- Vejledning af marts 2018 om konsekvensanalyse
- Vejledning af juni 2018 om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger
- Vejledning af juli 2018 om de registreredes rettigheder
- Vejledning af november 2018 om databeskyttelse og ansættelsesforhold
- Vejledning af oktober 2019 om kreditoplysningsbureauer
- Vejledning af november 2019 om advarselsregistre
- Vejledning af november 2019 om spærrelister

Vejledninger fra Det Europæiske Databeskyttelsesråd
- Adfærdskodekser (EDPB guideline 1/2019)
- Akkreditering (EDPB-guideline 4/2018)
- Art. 6(1)(b) som behandlingshjemmel ved udbud af online tjenester (EDPB guideline 2/2019)
- Administrative bøder i henhold til databeskyttelsesforordningen (wp253)
- Anmeldelse af brud på persondatasikkerheden (wp250)
- Automatiske individuelle afgørelser og profilering (wp251)
- Bindende virksomhedsregler (BCR), elementer og principper, der skal være indeholdt (wp256)
- Bindende virksomhedsregler (BCR) for databehandlere, elementer og principper, der skal være indeholdt (wp257)
- Bindende virksomhedsregler (BCR) for dataansvarlige, standardansøgning til brug for godkendelse af (wp264)

- Bindende virksomhedsregler (BCR) for databehandlere, standardansøgning til brug for godkendelse af (wp265)
- Bindende virksomhedsregler (BCR) for dataansvarlige og databehandlere, samarbejdsproceduren ved godkendelse af (wp263)
- Certificering (EDPB guideline 1/2018)
- Dataportabilitet, retten til (wp242)
- Databeskyttelsesrådgivere, DPO'ere (wp243)
- Fortegnelsen, undtagelser fra kravet om fortegnelse i artikel 30, stk. 5 (tilkendegivelse af 19/4 2018)
- Gennemsigtighed og oplysningsforpligtelser (wp260)
- Konsekvensanalyser vedrørende databeskyttelse, DPIA (wp248)
- Ledende tilsynsmyndighed (wp244)
- Samtykke (wp259)
- Territorialt anvendelsesområde for databeskyttelsesforordningen (Guideline 3/2018)
- Tredjelandsoverførsler, tilstrækkeligt databeskyttelsesniveau (wp254)
- Tredjelandsoverførsler, undtagelser i særlige situationer (EDPB guideline 2/2018) Guidelines 1/2019
- Videoovervågning (under opdatering efter endt offentlig høring)

De nævnte vejledninger er offentliggjort under punkterne "Vejledninger" og "EDPB-vejledninger", hvor der også løbende vil blive offentliggjort nye vejledninger.

Årsberetning

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Foto: Datatilsynet

ISBN nr. 978-87-999222-4-6

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk