Datatilsynet

Årsberetning

2020

DATATILSYNET

Datatilsynet

Årsberetning

2020

DATATILSYNET

Indhold

Til Folketinget

Datatilsynet har i 2020 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.

Datatilsynet har samlet set en særdeles omfattende og alsidig opgaveportefølje. Tilsynets vejledningsopgaver retter sig mod meget forskelligartede aktører: Folketinget, borgerne, private organisationer og virksomheder samt statslige, regionale og kommunale myndigheder. Datatilsynet arbejder imidlertid målrettet på at sikre, at alle kender og overholder reglerne for behandling af personoplysninger, og at borgerne kender og kan bruge deres rettigheder.

Hver dag håndterer Datatilsynet mange telefoniske og skriftlige forespørgsler, ligesom tilsynet løbende træffer afgørelser i konkrete sager, der kan tjene som vejledning for andre. Datatilsynet offentliggør endvidere hvert år forskellige former for vejledende tekster og skabeloner mv. I 2020 har Datatilsynet offentliggjort tre nationale vejledninger om databeskyttelsesreglerne, som supplerer de 24 nationale vejledninger, der er offentliggjort i perioden fra 2017 til 2019.

Datatilsynet har i 2020 ydermere offentliggjort en række hjemmesidetekster om behandling af personoplysninger i forbindelse med håndteringen af Covid-19, ligesom tilsynet tog initiativ til at udarbejde en skabelon og seks gode råd til manuel registrering af restaurantgæster med henblik på smitteopsporing, da restauranterne efter sommerferien 2020 blev opfordret af sundhedsmyndighederne til at foretage en sådan registrering.

Herudover har Datatilsynet i 2020 udarbejdet yderligere fem episoder til tilsynets podcast om databeskyttelsesforordningen, der er særligt relevant for SMV-segmentet. Podcasten, som nu består af i alt 20 episoder, er imidlertid også blevet taget rigtig godt imod af andre typer af dataansvarlige bl.a. kommunerne og af særligt interesserede borgere.

Datatilsynet yder også en aktiv indsats på vejledningsområdet i europæiske sammenhænge. Tilsynet har i 2020 – i regi af Det Europæiske Databeskyttelsesråd – bidraget til udarbejdelsen af fire nye fælleseuropæiske vejledninger mv. om forordningen.

Sammen med en række praktisk anvendelige skabeloner – f.eks. til opfyldelse af oplysningspligten – kan alle de nævnte vejledninger findes på Datatilsynets hjemmeside.

Nyt strategisk grundlag

For yderligere at styrke Datatilsynets vejledningsindsats har tilsynet i efteråret 2020 taget en række organisatoriske tiltag. Pr. 1. oktober 2020 er der oprettet en ny enhed i sekretariatet ved navn "VIS – Vejledning og Informationssikkerhed", som har et særligt fokus på at give mere konkret vejledning til virksomheder, myndigheder og borgere. Endvidere har Datatilsynet ansat to nye kommunikationsmedarbejdere, der sammen med tilsynets første kommunikationsmedarbejder – der blev ansat i 2018 – bl.a. skal understøtte Datatilsynets jurister og it-sikkerhedskonsulenter i at omsætte svært juridisk og teknisk stof og formidle det, så indholdet bliver modtagerorienteret og forståeligt for den brede målgruppe af borgere, virksomheder og myndigheder mv.

Datatilsynet har herudover i 2020 nedsat to kontaktudvalg: ét for erhvervslivet og ét for regionerne og kommunerne. Udvalgene er nedsat med det formål at skabe en platform for vidensdeling og drøftelse af databeskyttelsesretlige problemstillinger.

Der er tale om de første initiativer, Datatilsynet tager i forlængelse af, at tilsynet i 2020 har lanceret et helt nyt strategiske grundlag, som bygger på en omfattende interessentanalyse, der har kortlagt behovet og efterspørgslen bl.a. på mere konkret rådgivning og vejledning. Datatilsynet har i 2020 også offentliggjort en ny strategi for en data- og risikobaseret indsats, der fremadrettet skal styrke tilsynets eget arbejde med at anvende data og sikre et øget fokus på en risikobaseret tilgang til myndighedsudøvelsen.

Samarbejde med Rigsadvokaten og Rigspolitiet

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 fra en sags begyndelse til dens afgørelse ved domstolene - herunder bevissikring, retssikkerhedslov og udformning af et anklageskrift. Datatilsynet har derfor i 2020 fortsat det samarbejde med Rigsadvokaten og Rigspolitiet, der blev indledt i 2019, og som har til formål at tilrettelægge den samlede håndtering af straffesager vedrørende overtrædelse af databeskyttelsesreglerne på tværs af myndighederne.

Større sagskomplekser og internationale opgaver

Året har også i vidt omfang været præget af arbejdet med større sagskomplekser og opgaver af international karakter. Datatilsynet har i 2020 behandlet flere større og ganske principielle sager om behandling af personoplysninger hos såvel offentlige myndigheder som private virksomheder. Endvidere har Datatilsynet i 2020 bl.a. deltaget aktivt i udformningen af Det Europæiske Databeskyttelsesråds bidrag til EU-Kommissionens evalueringsrapport om databeskyttelsesforordningen og rådets håndtering af den første konkrete klagesag i forbindelse med den såkaldte "One Stop Shop-mekanisme". Her skulle Det Europæiske Databeskyttelsesråd træffe en endelig bindende afgørelse som følge af, at de europæiske tilsynsmyndigheder, der var involveret i klagesagen, som berørte tilsynsmyndigheder, ikke kunne blive enige om den ledende tilsynsmyndigheds udkast til en afgørelse.

Endvidere afsagde EU-Domstolen i juli 2020 dom i Schrems II-sagen, som vedrører brugen af EU-Kommissionens standardkontrakter og "Privacy Shield". Datatilsynet har efter dommens afsigelse - ligeledes i regi af Det Europæiske Databeskyttelsesråd - brugt mange ressourcer på at analysere og udarbejde vejledende tekster om de nærmere konsekvenser af dommen.

Adfærdskodekser

Efter databeskyttelsesforordningen er det muligt for sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige og databehandlere, f.eks. en brancheorganisation eller brancheforening, at udarbejde såkaldte adfærdskodekser. Der er tale om et sæt af retningslinjer, der specificerer reglerne i databeskyttelsesforordningen for en given branche eksempelvis ved at fastlægge en procedure for, hvordan man overholder oplysningspligten og andre af de registreredes rettigheder i behandlingsprocesser, der er typiske for den pågældende branche.

Et adfærdskodeks - som regulerer, hvordan private virksomheder mv. håndterer personoplysninger - skal have et akkrediteret kontrolorgan. Kontrolorganets opgave er bl.a. at sikre, at de dataansvarlige og databehandlere, der er tilsluttet kodeksen, overholder kodeksens retningslinjer. For at blive akkrediteret af Datatilsynet skal kontrolorganet opfylde en række krav, som er fastsat i databeskyttelsesforordningen. Datatilsynet er ifølge forordningen forpligtet til at uddybe disse krav og forelægge dem for Det Europæiske Databeskyttelsesråd. Datatilsynet har i november 2020 i overensstemmelse hermed offentliggjort de danske akkrediteringskrav.

Ny underside målrettet børn og unge

I december 2020 lancerede Datatilsynet en ny underside til tilsynets hjemmeside målrettet børn og unge. Materialet på siden handler især om brug af sociale medier og deling af billeder på nettet. Formålet med siden er at oplyse om rettighederne på området og samtidig invitere børn og unge til at tage kritisk stilling, når andre behandler oplysninger om dem. Indsatsen er første led i en række formidlingsindsatser målrettet børn og unge.

Valby, april 2021

Kristian Korfits Nielsen

Formand, Datarådet

Cristina Angela Gulisano

Direktør, Datatilsynet

Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2020 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 2020, 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 henvise til sin hjemmeside for yderligere oplysninger. Årsberetningen sendes endvidere til EU-Kommissionen og Det Europæiske Databeskyttelsesråd, ligesom den offentliggøres på Datatilsynets hjemmeside.

Om Datatilsynet

Datatilsynet er den centrale uafhængige myndighed, der fører tilsyn med, at reglerne om databeskyttelse bliver overholdt. Tilsynet med domstolenes behandling af personoplysninger ligger dog hos Domstolsstyrelsen.

Datatilsynets opgaver

Tilsynet med databeskyttelsesområdet indebærer et stort antal forskelligartede opgaver. Datatilsynet har i 2020 bl.a. haft følgende opgaver:

- Information, rådgivning og vejledning.
- Behandling af klagesager.
- Behandling af anmeldelser af brud på persondatasikkerheden.
- Sager på Datatilsynets eget initiativ, herunder tilsyn med offentlige myndigheder og private dataansvarlige mv.
- Udtalelser om lovforslag og udkast til bekendtgørelser og cirkulærer mv.
- Bidrag til besvarelse af spørgsmål fra Folketinget.
- Deltagelse i internationalt samarbejde med andre datatilsynsmyndigheder i EU – i regi af Det Europæiske Databeskyttelsesråd (EDPB).
- Deltagelse i arbejdsgrupper og udvalg.
- Oplæg på konferencer og 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 brugen af disse systemer.

I 2020 har Datatilsynet lanceret et helt nyt strategisk grundlag, der bl.a. bygger på en interessentanalyse, som tilsynet har fået foretaget i foråret 2020. Datatilsynets vision er nu at sikre en ansvarlig anvendelse af borgernes data i et digitaliseret samfund. Det er samtidig Datatilsynets mission at være en åben myndighed, der arbejder lydhørt, differentieret og synligt, og som løser sine opgaver gennem anvendelig vejledning og information, tilgængelige afgørelser og målrettede tilsyn, ligesom Datatilsynet sætter aftryk på national lovgivning og europæisk samarbejde.

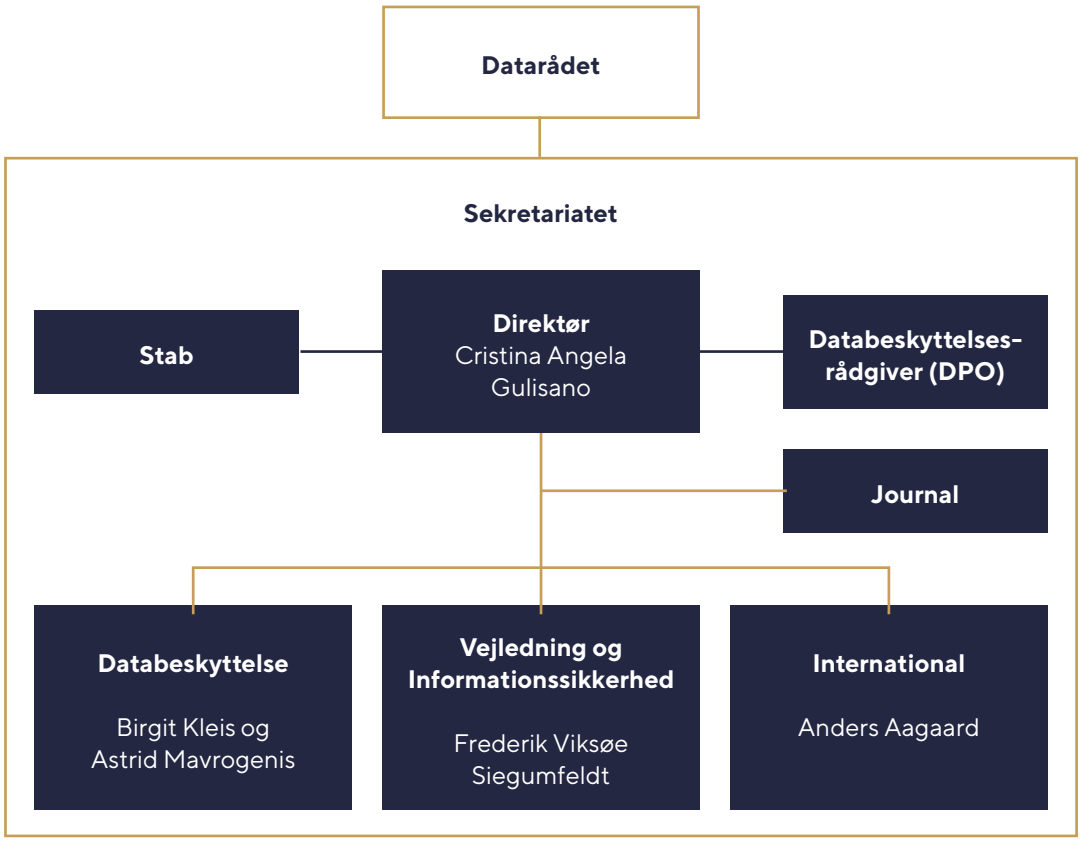
Som følge af det nye strategisk grundlag i 2020, er der sket organisatoriske ændringer i den måde, Datatilsynet er organiseret og løser sine opgaver på. Blandt de væsentligste ændringer kan nævnes, at ansvaret for den udadvendte tilsynsopgave er flyttet fra én enhed ud i hele organisationen, mens en ny enhed har fået et særligt fokus på at give mere konkret vejledning til virksomheder, myndigheder og borgere mv.

Organisationsændringen trådte i kraft den 1. oktober 2020.

Datatilsynets organisation

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

Datatilsynets afgørelser er endelige og kan ikke indbringes for en anden administrativ myndighed. Dog kan afgørelser 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 kontrol af Folketingets Ombudsmand.



Datarådet

I forbindelse med overgangen til et nyt retsgrundlag blev der efter den 25. maj 2018 nedsat et nyt Datatråd. Justitsministeren nedsætter rådet, der består af en formand, der skal være højesteretsdommer eller landsdommer, og syv andre medlemmer.

Erhvervsministeren og ministeren for offentlig innovation (nu finansministeren) udnævner hvert et af de syv andre medlemmer. Datarådet udnævnes for fire år, og der kan ske genudpegning to gange. Udpegelsen sker på baggrund af medlemmernes faglige kvalifikationer.

Datarådets forretningsorden, der fastsættes af rådet selv, blev vedtaget på Datarådets første møde den 20. december 2018.

Datarådets medlemmer (pr. 31. december 2020)

Formand
Formand, højesteretsdommer, Kristian Korfits Nielsen.

Medlemmer
Næstformand, professor, dr.jur., Henrik Udsen.
Advokat, Pia Kirstine Voldmester.
Formand for Rådet for Digital Sikkerhed, Henning Mortensen.
Fhv. sundhedsdirektør, Svend Hartling.
Advokat, Martin von Haller Grønbæk.
Vicedirektør i Forbrugerrådet Tænk, Mette Raun Fjordside.
Juridisk chef i KL, Pernille Christensen.

Sekretariatet

Sekretariatet beskæftiger 60 medarbejdere og består af jurister, it-sikkerhedskonsulenter, kontorpersonale og studenter m.fl., der varetager Datatilsynets daglige drift under ledelse af direktør, cand. jur., Cristina Angela Gulisano.

De bevillingsmæssige forhold mv. fremgår af Datatilsynets økonomiske årsrapport for 2020, der kan findes på Datatilsynets hjemmeside under "Årsberetninger og årsrapporter".

Sekretariatets medarbejdere (pr. 31. december 2020)

(Oversigten viser antallet af medarbejdere og ikke antallet af årsværk. Der kan derfor være afvigelser i forhold til den økonomiske årsrapport for 2020)

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. Anders Aagaard
Chefkonsulent, cand.jur. Karina Kok Sanderhoff
Chefkonsulent, cand.jur. Katrine Valbjørn Trebbien
Chefkonsulent, cand.jur. Mia Staal Klintrup
Chefkonsulent, cand.jur. Susanne Richter
Specialkonsulent, cand.jur. Eva Volfing
Specialkonsulent, cand.jur. Sarah Hersom Kublitz
Stabsmedarbejder, cand.soc. Anne Bech
Kommunikationskonsulent, cand. mag. Anders Due
It-sikkerhedskonsulent, cand. jur. Allan Frank
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 Mette-Maj Aner Leilund
Kontorfuldmægtig Pernille Jensen
Kontorfunktionær Anette Sørensen
Kontorfunktionær Lisbeth Søndberg Liljekrans (vikar)
Kontorfunktionær Camilla Knutsdotter Hallingby
Kommunikationsfuldmægtig, cand.mag. Natascha Helverskov Jørgensen
Kommunikationsfuldmægtig, cand.public. Johan Engstrøm
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. Caroline Rasmussen
Fuldmægtig, cand.jur. Cecilie Spendrup Slagslunde
Fuldmægtig, cand.jur. Charlotte Nørtoft Poulsen
Fuldmægtig, cand.jur. Ditte Malene Kieler Koefoed
Fuldmægtig, cand.jur. Kasper Viftrup
Fuldmægtig, cand.jur. Kasper Folmar
Fuldmægtig, cand.jur. Kenni Elm Olsen
Fuldmægtig, cand.jur. Lea Bruun
Fuldmægtig, cand.jur. Lise Fredskov
Fuldmægtig, cand.jur. Line Sørensen
Fuldmægtig, cand.jur. Mads Nordstrøm Kjær
Fuldmægtig, cand.jur. Marie Raahauge Christiansen
Fuldmægtig, cand.jur. Nikolaj Niss Rohde
Fuldmægtig, cand.jur. Pernille Ørum Walther
Fuldmægtig, cand.jur. Rasmus Arslev
Fuldmægtig, cand.jur. Ramus Martens
Fuldmægtig, cand.jur. Sara Koch Jørgensen
Fuldmægtig, cand.jur. Sara Thorning Hansen
Fuldmægtig, cand.jur. Sofie Eberhard Bendtz (Orlov)
Fuldmægtig, cand.jur. Susanne Dige Nielsen
Fuldmægtig, cand.jur. Victoria Lenchler-Huebertz
Fuldmægtig, cand.jur. Zenia Dinesen
Stud.jur. Amalie Pilgaard Stubdrup
Stud.jur. Pernille Elisabeth Jensen

Datatilsynets nye strategisk grundlag

I 2020 har Datatilsynet lanceret et helt nyt strategisk grundlag med ny vision, mission og værdigrundlag. Det nye strategiske grundlag sætter retningen for tilsynets arbejde i de kommende år og omfatter blandt andet et styrket fokus på mere konkret vejledning og en række ændringer i den måde, Datatilsynet er organiseret og løser sine opgaver på.

Datatilsynets vision er nu at sikre en "ansvarlig anvendelse af borgernes data i et digitaliseret samfund". Det er samtidig tilsynets mission at være en åben myndighed, der arbejder lydhørt, differentieret og synligt, og som løser sine opgaver gennem anvendelig vejledning og information, tilgængelige afgørelser og målrettede tilsyn, ligesom Datatilsynet sætter aftryk på national lovgivning og det europæiske samarbejde.

Strategi med afsæt i interessenternes input

Det nye strategiske grundlag er blevet til på baggrund af input fra de aktører, der særligt har en interesse i Datatilsynets arbejde. Der er således blevet udarbejdet en interessentanalyse, hvor en række myndigheder, brancheorganisationer og interesseorganisationer er blevet hørt om deres oplevelse af og fremtidige ønsker til Datatilsynets arbejdsfokus.

Med det afsæt har en gruppe af medarbejdere og ledere fra Datatilsynet udarbejdet det nye strategiske grundlag gennem foråret og sommeren med ikrafttrædelse pr. 1. oktober 2020.

Med Datatilsynets nye strategiske grundlag har vi et stærkere fundament for at fortsætte den bevægelse, vi har været i gang med de seneste år, hvor vi har forsøgt at være mere åbne og konkrete end tidligere. Samtidig skruer vi op for vores vejledningsindsats, så vi i endnu højere grad kan hjælpe virksomheder og myndigheder på rette vej"

- Datatilsynets direktør, Cristina Angela Gulisano.

Strategisk grundlag

Vision, mission og værdigrundlag udgør det strategiske fundament for Datatilsynets arbejde.

Vision

Datatilsynets vision sætter den overordnede retning for vores arbejde. Visionen er det mål, vi gennem vores myndighedsudøvelse arbejder hen imod:

Ansvarlig anvendelse af borgernes data i et digitaliseret samfund.

Mission

Datatilsynets mission sætter rammen for tilsynets myndighedsudøvelse, herunder hvordan vi som tilsyn løfter vores kerneopgaver:

- Vi er en åben myndighed, der løfter vores opgaver i uafhængighed.
- Vi arbejder lydhørt, differentieret og synligt.
- Vi løser vores opgaver gennem anvendelig vejledning og information, tilgængelige afgørelser og målrettede tilsyn.
- Vi sætter aftryk på national lovgivning og europæisk samarbejde.

Værdigrundlag

Værdigrundlaget beskriver de væsentligste værdier, som understøtter Datatilsynets myndighedsudøvelse og arbejde både nu og fremadrettet:

Høj faglighed: Alle samfundets aktører kan være sikre på, at Datatilsynets afgørelser foretages med afsæt i en dyb faglighed: dette fremhæves også som en af Datatilsynets styrker af dets interessenter.

Udsyn: Datatilsynet skal i endnu højere grad åbne sig mod og interagere med omverdenen for at have fingeren på pulsen i forhold til tendenserne i samfundet, den teknologiske udvikling og interessenternes behov.

Integritet: Datatilsynet er en myndighed, der løser sine opgaver - herunder træffer afgørelser og udfærdiger vejledninger i uafhængighed.

Mod: Datatilsynet skal turde træffe beslutninger - også i vanskelige sager. Datatilsynet skal være tydelig i sine udmeldinger for på den måde at være retningsgivende og bidrage til forståelsen af databeskyttelsesreglerne.

Proaktivitet: Proaktivitet skal kendetegne Datatilsynets opgaveløsning og den måde, tilsynet møder omverdenen på.

En mere data- og risikobaserede tilgang

I forlængelse af Datatilsynets nye strategiske grundlag er der udarbejdet en strategi for at styrke den data- og risikobaserede indsats i tilsynet: "Tilsyn med effekt: Datatilsynets data- og risikobaserede tilgang 2020-2023". Den datadrevne tilgang skal bidrage til, at tilsynets ressourcer anvendes mest optimalt.

Den samfundsmæssige udvikling mod et mere digitaliseret samfund giver private og offentlige aktører nye muligheder for at udnytte personoplysninger i et hidtil uset omfang. Denne øgede anvendelse af oplysninger er ikke nødvendigvis dårlig. Det sætter dog databeskyttelsen under pres og stiller stadig større krav til, at Datatilsynet målretter sin indsats på områder, hvor behovet for vejledning eller kontrol er størst. For at imødekomme disse krav har tilsynet udarbejdet en ny strategi for en data- og risikobaseret indsats, der fremadrettet skal styrke tilsynets eget arbejde med at anvende data og sikre et øget fokus på en risikobaseret tilgang til myndighedsudøvelsen.

Datatilsynet råder i dag over væsentlige datakilder fra det løbende arbejde i tilsynet – fx klagesager i tilsynets journalsystem og et stort antal anmeldte brud på persondatasikkerheden. Disse data kan potentielt danne et solidt grundlag for databaserede og risikobaserede aktiviteter. De tilgængelige datakilder (og de understøttende it-systemer) er imidlertid præget af, at de i høj grad er blevet tilvejebragt og anvendt med det formål for øje, at de skal kunne understøtte konkret sagsbehandling i enkeltsager – og kun i mindre grad danne grundlag for eksempelvis tværgående analyser.

For at kunne målrette vores vejlednings- og kontrolaktiviteter har vi behov for at kunne bruge de samme data på en ny og mere systematiseret måde. Det stiller krav til den måde, som vi indsamler og registrerer data på. Målet er, at allerede tilgængelige data i langt højere grad skal kunne give os en dokumenteret indsigt i forhold om dataansvarlige, om udvalgte brancher, om hyppige klagetemaer, om databeskyttelsesretlige udfordringer, om risikoprofiler, om udviklingstendenser etc.

Strategiske udfordringer

Hvordan sikrer vi en høj kvalitet af vores data?

Indsats # 1

Evaluering af datakvaliteten og registrering af metadata

Indsats # 2

Systematiseret indsamling af data

Hvordan sikrer vi adgang til relevante datakilder?

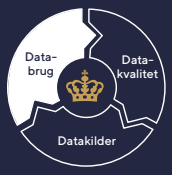
Indsats # 3

Forsøg med nyt tilsynskoncept (ny intern datakilde)

Indsats # 4

Adgang til eksterne datakilder

Hvordan bliver vi gode til at bruge data?



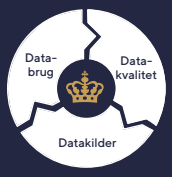
Indsats # 5

Klare kriterier for udvælgelse af kontrolområder

Indsats # 6

Flere databaserede beslutninger

Hvordan dokumenterer og evaluerer vi indsatsen?



Indsats # 7

Dokumenterede processer, beslutninger og resultater

Indsats # 8

Forsøg med effektmåling

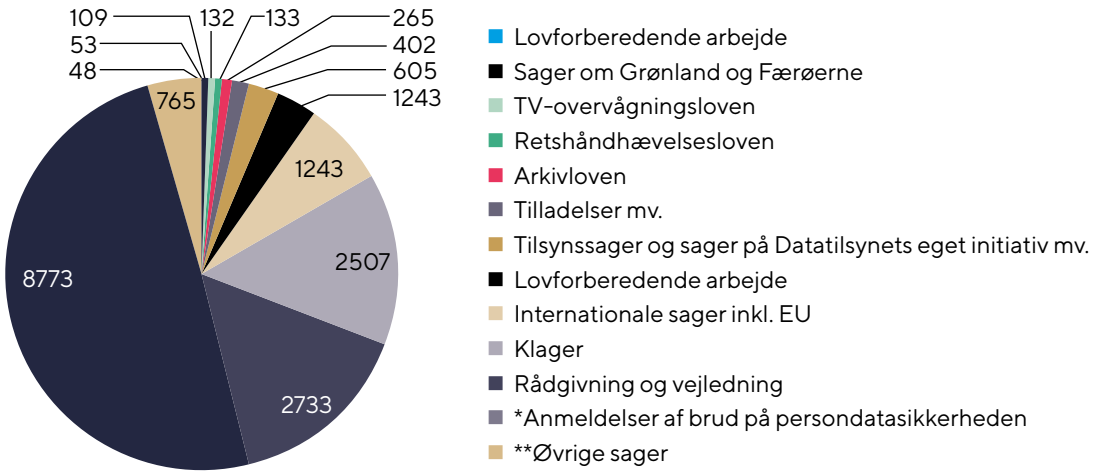
Året i tal

I det følgende afsnit findes oplysninger om antallet af nye sager, som er oprettet i Datatilsynets journalsystem i 2020. En del af Datatilsynets sagsbehandling er 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 **17.768** nye sager i 2020.

Fordelingen af oprettede sager 2020	
Lovforberedende arbejde	605
Rådgivning og vejledning	2.733
Klager	2.507
Sager på Datatilsynets eget initiativ	402
Tilladelser mv.	265
Internationale sager inkl. EU	1.243
Anmeldelser af brud på persondatasikkerheden*	8.773
Retshåndhævelsesloven	132
TV-overvågningsloven	109
Lov om massemediers informationsdatabaser	48
Arkivloven	133
Sager om Grønland og Færøerne	53
Øvrige sager**	765
Sager i alt	17.768

Oprettede sager i 2020



Bemærkninger:

Der er ikke fuld overensstemmelse mellem tallene i Datatilsynets økonomiske årsrapport 2020, som sendes til Folketingets Finansudvalg, Rigsrevisionen og Finansministeriet, og nærværende tal, eftersom statistikken er trukket på forskellige tidspunkter. Der kan derfor optræde mindre afvigelser, hvor nogle sager eksempelvis er omjournaliseret eller konstateret fejloprettet.

*Anmeldelser af brud på persondatasikkerheden efter retshåndhævelsesloven er ikke medtaget i antallet af anmeldelser af brud på persondatasikkerheden, men fremgår af sagsgruppen "Retshåndshævelsesloven".

**Øvrige sager dækker over sager vedrørende Datatilsynets egen administration og aktindsigtsanmodninger mv.

Lovforberedende arbejde
(Høringer, folketingspørgsmål mv.)

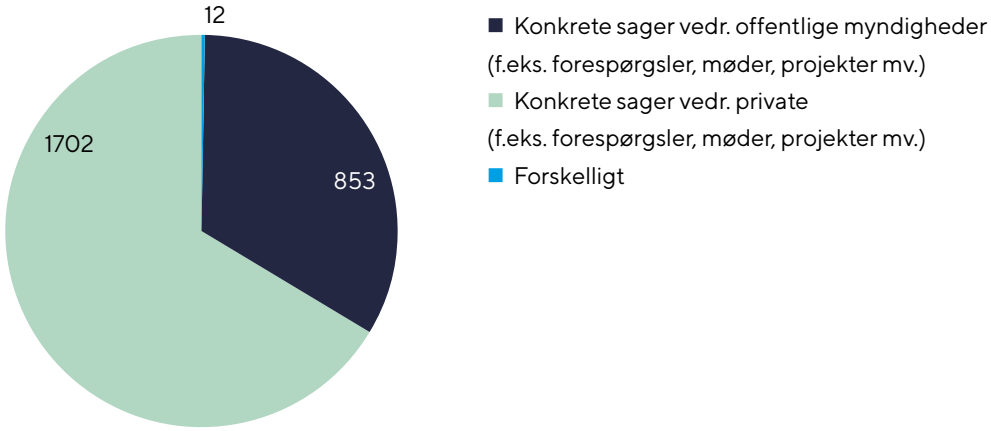
Fordelingen af sager vedrørende lovforberedende arbejde	
Høringer over bekendtgørelser, cirkulærer, vejledninger, anordninger mv.	351
Høringer over betænkninger, lovforslag, EU-retsakter, konventioner mv.	206
Folketingsspørgsmål, private lovforslag, folketingsbeslutninger, høringer mv.	40
Forskelligt	9
Sager i alt	606

Sager vedrørende lovforberedende arbejde

Rådgivning og vejledning
(Forespørgsler, møder, projekter mv.)

Fordeling af sager vedr. rådgivning og vejledning	
Konkrete sager vedr. private (f.eks. forespørgsler, møder, projekter mv.)	1702
Konkrete sager vedr. offentlige myndigheder (f.eks. forespørgsler, møder, projekter mv.)	853
Forskelligt	12
I alt	2567

Fordeling af sager vedr. rådgivning og vejledning

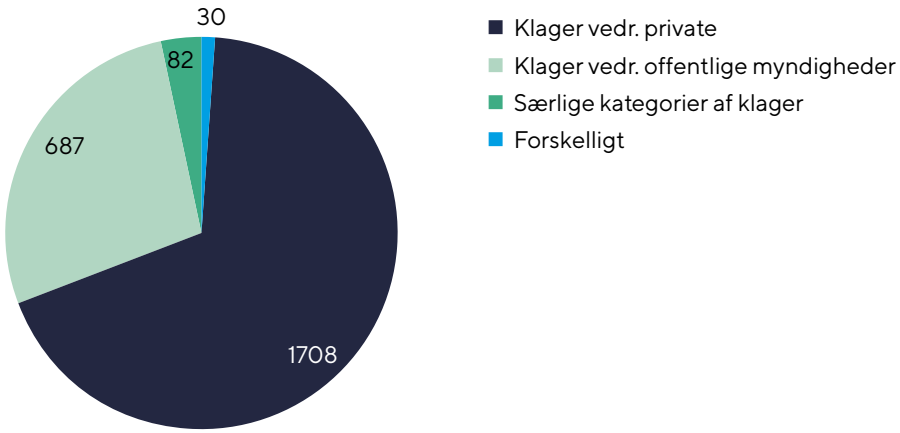


Tilsyn

Klager

Fordeling af klagesager	
Klager vedr. private	1708
Klager vedr. offentlige myndigheder	687
Særlige kategorier af klager *	82
Forskelligt	30
I alt	2507

Klagesager

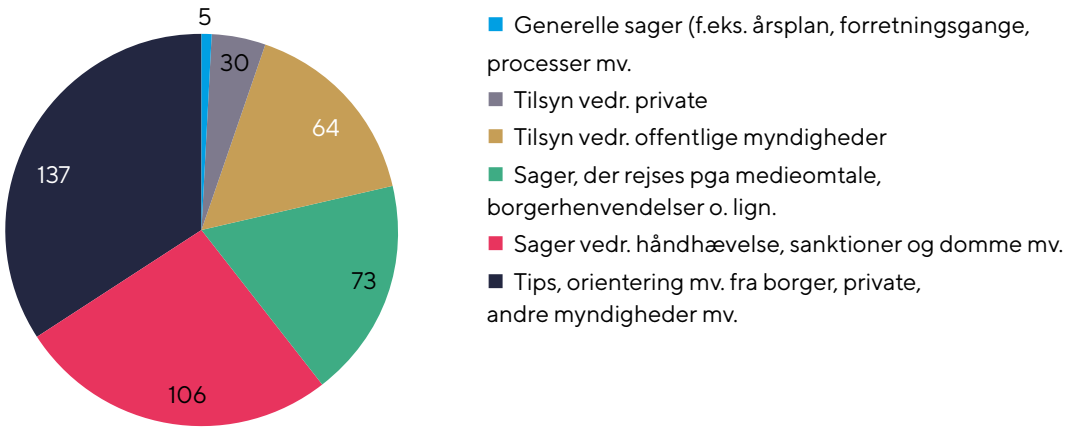


*Klager over kreditoplysningsbureauer

Sager på Datatilsynets eget initiativ

Fordeling af sager på eget initiativ	
Tilsyn vedr. private	18
Tilsyn vedr. offentlige myndigheder	64
Sager, der rejses pga. medieomtale, borgerhenvendelse o.lign.	73
Sager vedr. håndhævelse, sanktioner og domme mv.	106
Tips, orientering mv. fra borgere, private, andre myndigheder mv.	137
Generelle sager (f.eks. årsplan, forretningsgange, processer mv.)	4
I alt	402

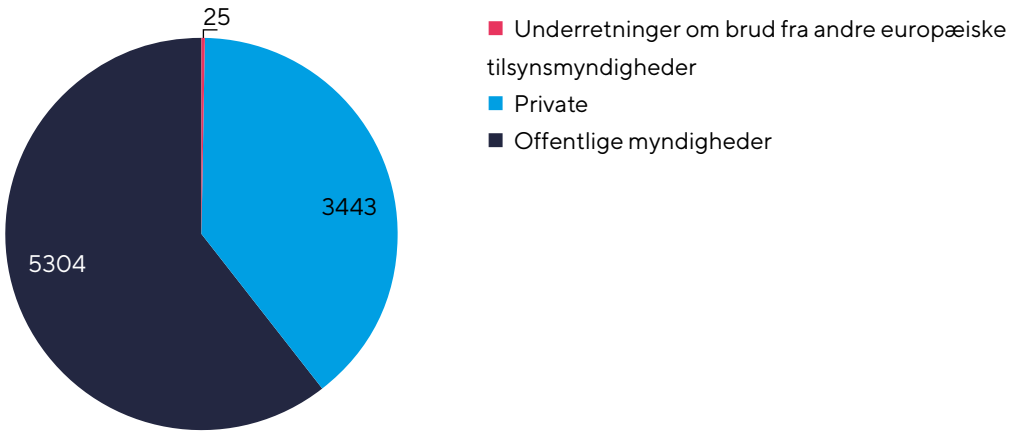
Sager på Datatilsynets eget initiativ



Anmeldelser af brud på persondatasikkerheden

Fordelingen af anmeldelser af brud på persondatasikkerheden	
Anmeldelser af brud på persondatasikkerheden:	
Offentlige myndigheder	5304
Private	3443
Underretninger om brud fra andre europæiske tilsynsmyndigheder	25
Sager i alt	8772

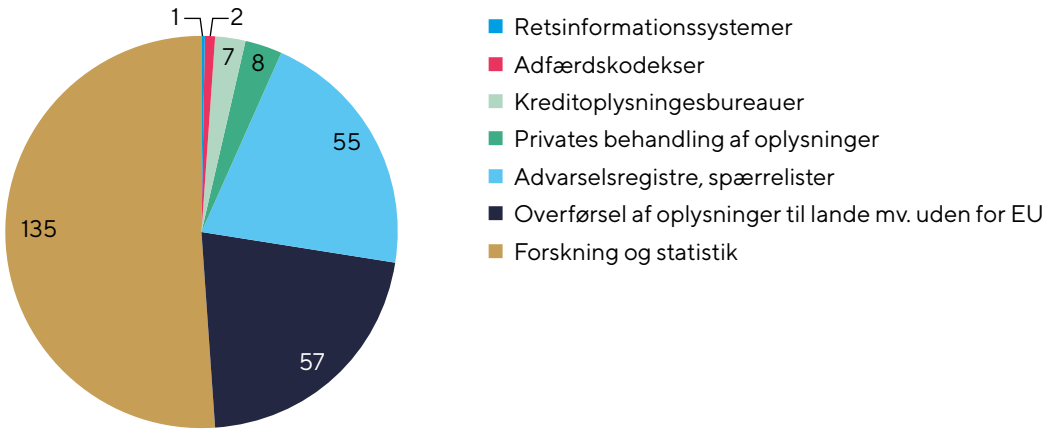
Fordelingen af anmeldelser af brud på persondatasikkerheden



Tilladelser mv.

Tilladelser	
Forskning og statistik	135
Overførsel af oplysninger til lande mv. uden for EU	57
Advarselsregistre, spærreliste	55
Privates behandling af oplysninger	8
Kreditoplysningsbureauer	7
Adfærdskodekser	2
Retsinformationssystemer	1
I alt	265

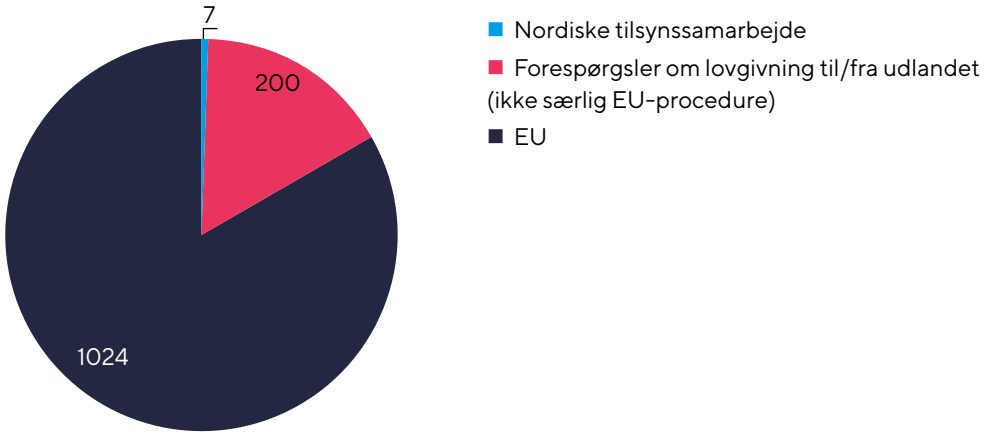
Tilladelser mv.



Internationale sager

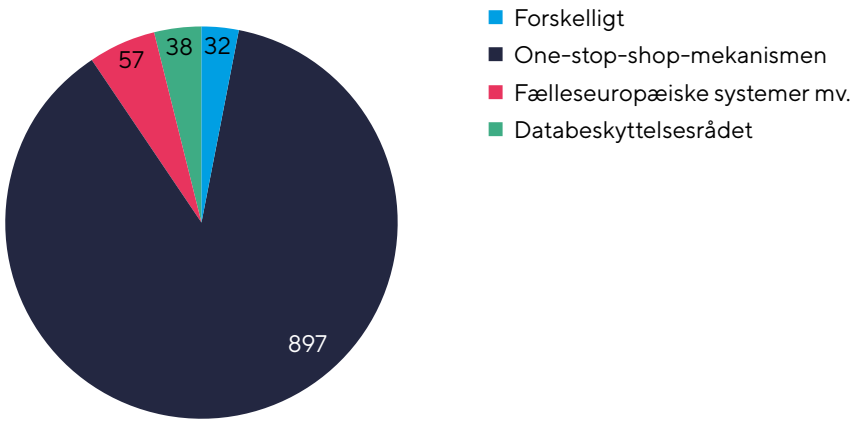
Fordelingen af internationale sager	
Forespørgsler om lovgivning til/fra udlandet (ikke særlig EU-procedure)	200
Nordiske tilsynssamarbejde	7
EU	1024
I alt	1231

Fordelingen af internationale sager



Fordelingen af EU sager	
Forskelligt	32
Databeskyttelsesrådet	38
Fælleseuropæiske systemer mv.	57
One-stop-shop mekanismen	897
I alt	1024

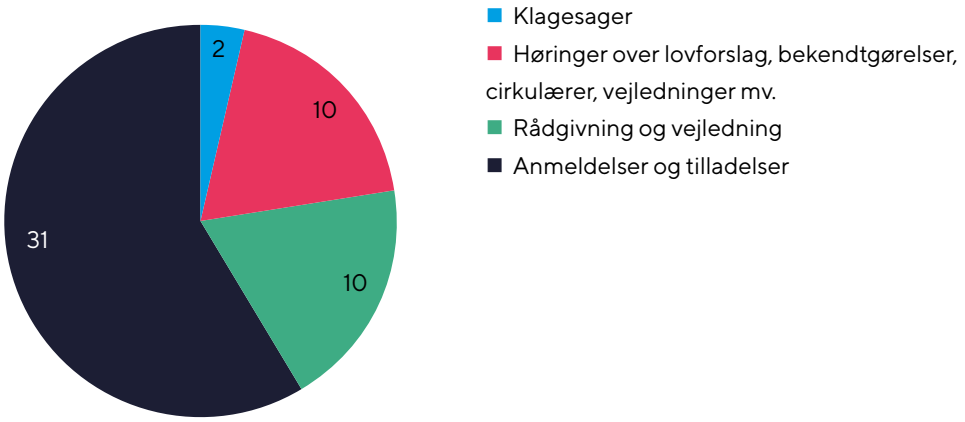
Fordelingen af EU-sager



Sager om Grønland og Færøerne

Fordeling af sager om Grønland og Færøerne	
Anmeldelser og tilladelser	31
Rådgivning og vejledning	10
Høringer over lovforslag, bekendtgørelser, cirkulærer, vejledninger mv.	10
Klagesager	31
I alt	53

Fordelingen af sager om Grønland og Færøerne



Rådgivning og vejledning

For at sikre en høj beskyttelse af danskernes personoplysninger er det afgørende, at myndigheder og private virksomheder mv. kender og overholder reglerne for behandling af personoplysninger, mens borgerne forstår deres rettigheder og det at gøre brug af dem. Datatilsynet gør dette muligt gennem synlig rådgivning og vejledning, dialog og kontrol. Det er Datatilsynets opgave at rådgive om registrering, videregivelse og anden behandling af personoplysninger samt føre tilsyn med, at myndigheder, virksomheder og andre dataansvarlige overholder reglerne for databeskyttelse.

Datatilsynets forpligtelse til at yde en serviceorienteret og anvendelig rådgivning er imidlertid ikke kun en del af tilsynets vision og mission. Det følger også direkte af databeskyttelsesforordningen og bliver bl.a. sikret gennem de mange telefoniske og skriftlige forespørgsler om reglerne, som Datatilsynet

håndterer hver eneste dag. Tilsynet holder også mange møder med interesse- og brancheorganisationer samt enkeltstående dataansvarlige og databehandlere efter behov.

Datatilsynet har i 2020 offentliggjort tre nationale vejledninger om databeskyttelsesreglerne, som supplerer de 24 nationale vejledninger, som tilsynet har offentliggjort fra 2017 til 2019. Datatilsynet yder også en aktiv indsats på vejledningsområdet i europæiske sammenhænge og har i regi af Det Europæiske Databeskyttelsesråd bidraget til udarbejdelsen af fire nye fælleseuropæiske vejledninger om databeskyttelsesforordningen. Alle de nævnte vejledninger og skabeloner kan findes på Datatilsynets hjemmeside. I 2020 har tilsynet udarbejdet yderligere fem episoder til podcasten om databeskyttelsesforordningen "Datatilsynets podcast – bliv klogere på GDPR".

I lyset af Covid-19 pandemien har Datatilsynet offentliggjort en række vejledningstekster om behandling af personoplysninger i forbindelse med håndteringen af Covid-19, hvor tilsynet tog initiativ til at udarbejde en skabelon og seks gode råd til manuel registrering af restaurantgæster med henblik på smitteopsporing, da restauranterne efter sommerferien 2020 blev opfordret af sundhedsmyndighederne til at foretage en sådan registrering.

Datatilsynet prioriterer endvidere som myndighed at deltage med indlæg på konferencer, seminarer mv. for at informere om databeskyttelsesreglerne og tilsynets praksis, men også for, at tilsynet selv kan opnå større intern viden om, hvilke udfordringer de registrerede, andre offentlige myndigheder og den private sektor oplever inden for databeskyttelsesområdet. Covid-19 har i den forbindelse sat sine naturlige begrænsninger for Datatilsynets muligheder for deltagelse samt omfanget af relevante arrangementer.

Mere konkret vejledning

Der er i Datatilsynet i disse år en meget stor opmærksomhed på, hvordan vi formulerer os som myndighed. Øvelsen er at finde en passende balance, hvor formidlingen både er korrekt og til at forstå – forenklet uden at være forsimplet. Datatilsynet har i 2020 ansat to nye kommunikationsmedarbejdere, der sammen med tilsynets første kommunikationsmedarbejder - der blev ansat i 2018 - bl.a. skal understøtte Datatilsynets jurister og it-sikkerhedskonsulenter i at omsætte komplekst, juridisk stof og formidle det, så indholdet bliver modtagerorienteret og forståeligt for den brede målgruppe af borgere, virksomheder og myndigheder mv.

Datatilsynets podcast – "Bliv klogere på GDPR"

I løbet af 2020 udgav Datatilsynet yderligere fem nye podcastepisoder, som formidler forskellige emner og problemstillinger inden for databeskyttelsesforordningen. Siden september 2019 har Datatilsynet produceret i alt 20 tilgængelige episoder med over 51.000 afspilninger i perioden 31. december 2019 til 31. december 2020, hvilket samlet set udgør 71.000 afspilninger siden lanceringen.

Podcastepisoderne tager fat på et afgrænset emne og udfolder sig som en dialog mellem to af Datatilsynets medarbejdere. Formidlingen foregår i en uformel tone, hvor de juridiske problemstillinger forklares i øjenhøjde med konkrete og virkelighedsnære eksempler. Podcasten er et supplement til den mere traditionelle, skriftlige vejledning, som Datatilsynet ellers stiller til rådighed på datatilsynet.dk. Podcasten er med andre ord tænkt som et alternativ til de andre informationskanaler, der især skal gøre mindre dataansvarlige opmærksomme på reglerne og opfordre dem til at søge nærmere vejledning og hjælp efter behov.

Emnerne til de fem episoder produceret i 2020 bygger bl.a. på input fra Datatilsynets mange følgere på LinkedIn og behandler temaer som:

"#16 Behandling af oplysninger om besøgende på hjemmesider"

"#17 Dataansvarlige og databehandlere"

"#18 Kreditoplysninger og spærrelister"

"#19 Børn og unge - deling af billeder"

"#20 Fælles dataansvar - når der er mere end én dataansvarlig"

Datatilsynets podcast er tilgængelig på alle gængse streamingtjenester.

Etablering af kontaktudvalg

Datatilsynet har i 2020 nedsat et kontaktudvalg for erhvervslivet og et andet målrettet regioner og kommuner. Initiativet er et led i opfølgningen på Datatilsynets nye strategiske grundlag, men også GDPR-anbefaling nr. 1 fra Erhvervslivets EU- og Regelforum.

For at sikre en ansvarlig anvendelse af danskernes personoplysninger er det afgørende, at der er en kontinuerlig dialog mellem Datatilsynet og Datatilsynets interessenter for bl.a. at sikre klarhed og forståelse for de databeskyttelsesretlige regler. Datatilsynet har derfor et ønske om at samarbejde med interessentlandskabet i endnu højere grad end tidligere og have fingeren på pulsen i forhold til udfordringer og behov, tendenser i samfundet og den generelle teknologiske udvikling.

Formålet med kontaktudvalgene er at skabe en platform for vidensdeling og drøftelse af databeskyttelsesretlige problemstillinger, der bidrager til at sikre beskyttelsen af personoplysninger. Kontaktudvalgene fungerer som et supplement til Datatilsynets øvrige interessentinddragelse. I de to kontaktudvalg er der en fast dialog mellem Datatilsynet og udvalgsmedlemmerne to gange om året, som skal

sikre vidensdeling og konkret vejledning. Samtidig sikrer de faste kontaktudvalgsmøder, at Datatilsynet får løbende indsigt i, hvilke konkrete problemstillinger der rører sig i samfundet, og hvor der er behov for afklaring og vejledning.

Læs mere om kontaktudvalgene på Datatilsynets hjemmeside på undersiden "Kontaktudvalg".

Flere afgørelser på hjemmesiden

I lyset af Datatilsynets nye strategiske grundlag og GDPR-anbefaling nr. 2 fra Erhvervslivets EU- og Regelforum, blev der i 2020 igangsat en udvikling mod at få publiceret flere afgørelser på Datatilsynets hjemmeside og LinkedIn. Initiativet skal sikre, at interessentlandskabet får et øget fokus på de mange afgørelser, der i årets løb bliver behandlet og afsluttet i Datatilsynet.

Covid-19 vejledning

Datatilsynet offentliggjorde i 2020 en række tekster med gode råd til, hvordan situationen med Covid-19 håndteres set fra et databeskyttelsesretligt perspektiv.

Datatilsynet offentliggjorde i marts 2020 bl.a. en række råd til, hvordan arbejdsgivere kan tage de nødvendige forholdsregler uden samtidig at overtræde databeskyttelsesreglerne, når arbejdsgivere anser det for nødvendigt at behandle oplysninger om, at en ansat er smittet med Covid-19.

Efter at Datatilsynet var blevet opmærksom på flere private initiativer, der skulle bidrage til kortlægningen af udbredelsen af Covid-19 i Danmark på baggrund af indsamling af helbredsoplysninger, udarbejdede tilsynet en række gode råd til, hvad man skal være særlig opmærksom på, inden man deler sine oplysninger.

I april 2020 offentliggjorde Datatilsynet endvidere en tekst med de grundlæggende hensyn til databeskyttelse, som man bør have for øje, når man udvikler en app, idet den nuværende app til sporing af eventuelle kontakter til smittede med Covid-19 på daværende tidspunkt var under udvikling.

I juni 2020 udgav Datatilsynet endvidere en række gode råd til uddannelsesinstitutioner, som overvejer at livestreame skoleafslutninger og studenterarrangementer som følge af den manglende mulighed for at mødes i større forsamlinger.

Efter at sundhedsmyndighederne havde opfordret restauranter, caféer o.lign. til at registrere oplysninger om deres gæster med henblik på smitteopsporing, offentliggjorde Datatilsynet i september 2020 en skabelon, som restauratørerne kan tage udgangspunkt i, hvis de ønsker at bidrage til smitteopsporingen og samtidig være sikre på at overholde databeskyttelsesreglerne.

Datatilsynet har også bidraget aktivt til udarbejdelsen af internationale vejledninger – i regi af Det Europæiske Databeskyttelsesråd (EDPB) – i forbindelse med håndteringen af Covid-19.

Læs mere om EDPB vejledningerne på side 40 i årsberetningen.

Ny vejledning om behandling af oplysninger om hjemmesidebesøgende

I februar 2020 udgav Datatilsynet en ny vejledning, der har til formål at hjælpe de dataansvarlige med at behandle personoplysninger om hjemmesidebesøgende i overensstemmelse med de databeskyttelsesretlige regler.

Vejledningen tager udgangspunkt i, at samtykke ofte vil udgøre det retlige grundlag for behandlingen. For at et sådant samtykke kan anses for at være gyldigt, skal det opfylde en række krav. Blandt andet skal et samtykke være udtryk for et aktivt tilvalg fra den besøgende om, at vedkommendes oplysninger må behandles. Derudover skal det være klart for den besøgende, hvad oplysningerne bruges til, herunder hvilke formål den dataansvarlige har med behandlingen.

Der stilles endvidere krav om, at den besøgende skal have lige så let ved at give samtykke til behandlingen, som det er at afvise hjemmesidens behandling af oplysninger. Det er i den forbindelse vigtigt, at den besøgende får mulighed for at foretage et granuleret valg, således at den besøgende ikke tvinges til at give ét samtykke til samtlige af den dataansvarliges behandlingsformål, men i stedet får mulighed for at vælge imellem de enkelte formål.

Derudover er det vigtigt, at den dataansvarlige kan dokumentere, hvad en besøgende har samtykket til, og hvordan samtykket er indhentet.

Ny vejledning om optagelse af telefonsamtaler

Datatilsynet offentliggjorde i november 2020 en ny vejledning om optagelse af telefonsamtaler, som indeholder råd om, hvordan virksomheder overholder databeskyttelsesreglerne, hvis man ønsker at optage telefonsamtaler med sine interessenter f.eks. kunder mv.

Der kan være forskellige årsager til, at dataansvarlige ønsker at optage ind- og udgående telefonsamtaler, som den dataansvarlige har med sine interessenter. Det kan være, at den dataansvarlige har et ønske om at dokumentere, hvad der er sket og sagt under samtalen – herunder eventuelt indgåede aftaler, eller et ønske om at uddanne/træne sine medarbejdere.

Uanset hvad formålet med at optage en telefonsamtale er, skal en sådan optagelse altid ske i overensstemmelse med databeskyttelsesreglerne.

Datatilsynets vejledning fokuserer på de mest almindeligt forekommende databeskyttelsesretlige problemstillinger, som man skal være opmærksom på, hvis man ønsker at optage telefonsamtaler.

Vejledningen forklarer særligt, hvordan man som dataansvarlig sikrer sig et passende behandlingsgrundlag (hjemmel) til at optage samtalen, herunder hvornår der skal/ikke skal indhentes samtykke fra den, der optages. Endvidere kommer teksten ind på, hvor længe man kan opbevare optagelser af telefonsamtaler samt spørgsmålet om de registreredes rettigheder. Vejledningen kommer også med konkrete eksempler på, hvordan man i forskellige situationer kan iagttage sin oplysningspligt.

Opdatering af vejledning om fortegnelse

Datatilsynet offentliggjorde i februar 2018 en vejledning om fortegnelse i samarbejde med Justitsministeriet. Vejledningen var myndighedernes bud på, hvad en fortegnelse skulle indeholde for at leve op til kravene i databeskyttelsesforordningens artikel 30.

Datatilsynet opdaterede vejledningen om fortegnelse i sommeren 2020. Vejledningen blev opdateret på baggrund af de erfaringer, som tilsynet har gjort sig, efter at databeskyttelsesforordningen siden den 25. maj 2018 har fundet anvendelse.

Selve forpligtelsen til at føre en fortegnelse fremgår af databeskyttelsesforordningens artikel 30. Denne bestemmelse fastlægger, at den dataansvarlige og dennes eventuelle repræsentant skal føre en fortegnelse over behandlingsaktiviteter under deres ansvar. Herudover skal databehandlere og deres eventuelle repræsentanter føre fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Bestemmelsen angiver en række specifikke oplysninger, som en fortegnelse skal indeholde for henholdsvis den dataansvarlige og databehandleren.

Kravet om at føre en fortegnelse skal ses som en forlængelse af databeskyttelsesforordningens øgede fokus på ansvarlighed. Ansvarlighedstanken indebærer for det første, at den dataansvarlige, og i visse tilfælde databehandleren, har ansvaret for, at forordningens regler efterleves. For det andet skal den dataansvarlige også kunne påvise, at de behandlinger, denne har ansvaret for, lever op til forordningens regler.

Datatilsynet foretog ved opdateringen af vejledningen en række præciseringer i forhold til de oplysninger, som en fortegnelse skal indeholde.

Som led i opdateringen af vejledningen blev det således præciseret, at en fortegnelse over behandlingsaktiviteter - henset til formålene med fortegnelseskravet - efter Datatilsynets vurdering bør indeholde en tydelig kobling mellem kategorierne af personoplysninger og de enkelte kategorier af registrerede. Hvis der bliver eller vil blive videregivet personoplysninger i forbindelse med en behandlingsaktivitet, skal fortegnelsen også indeholde information om, hvilke kategorier af personoplysninger, der bliver eller vil blive videregivet til den pågældende modtager. I tilknytning hertil skal det også fremgå, hvilke kategorier af registrerede de pågældende oplysninger vedrører.

Dette er efter Datatilsynets opfattelse oplysninger, som dataansvarlige/databehandlere – i henhold til ansvarlighedstanken – bør have viden om og dokumentation for, bl.a. til brug for udarbejdelse af risikovurderinger og implementering af passende tekniske og organisatoriske sikkerhedsforanstaltninger mv.

Opdatering af vejledning om databeskyttelse i ansættelsesforhold

Datatilsynet har opdateret vejledningen om databeskyttelse i ansættelsesforhold blandt andet på baggrund af drøftelser med repræsentanter for arbejdsmarkedets parter om tillidsrepræsentanters brug af arbejdsgivers it-udstyr. Den opdaterede vejledning er endvidere tilrettet i overensstemmelse med tilsynets ændrede praksis om forståelsen af databeskyttelsesforordningens artikel 6 og 9. Datatilsynet har herudover foretaget justeringer i en række afsnit om f.eks. rettigheder for stillingsansøgere og ansatte og om kontrol af medarbejdere på baggrund af konkrete sager, som tilsynet har behandlet siden vejledningens første udgivelse i 2018.

Ny revisionserklæring

I 2019 lancerede FSR - danske revisorer og Datatilsynet sammen en revisorerklæring, som skulle hjælpe dataansvarlige med at påse, at deres databehandlere lever op til kravene i databeskyttelsesforordningen mv.

I 2020 har FSR - danske revisorer - og Datatilsynet offentliggjort yderligere en revisionserklæring, som har fået navnet "Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med [Dataansvarlig]".

Den nye erklæring er en "light version" i forhold til den tidligere erklæring, og den kan således være med til at sikre, at brugen af revisorerklæringer står mål med behovet i den konkrete situation.

Når man som dataansvarlig benytter sig af databehandlere, skal man indgå en databehandleraftale, men man skal også efterfølgende kontrollere behandlingen af personoplysninger hos databehandleren. En af måderne, man kan gøre dette på, er ved at bruge en revisorerklæring.

Erklæringen skal give den dataansvarlige sikkerhed for, at en databehandler, som behandler persondata for den dataansvarlige, har styr på procedurer og regler vedrørende beskyttelsen af personoplysninger.

Den nye erklæring - som er lanceret i 2020 - er særligt målrettet organisationer, hvor behandlingen af personoplysninger ikke er meget kompleks, hvor behandlingen er mindre risikofyldt, eller hvor organisationen i forvejen fører et omfattende tilsyn med databehandleren. Det er ikke som sådan nødvendigt at benytte revisorerklæringer for at efterleve databeskyttelsesforordningen mv., men sådanne erklæringer kan være en god måde at sikre, at de relevante områder bliver belyst, og man får foretaget en uvildig kontrol af sikkerhedsniveauet.

Krav til akkreditering af kontrolorganer for adfærdskodekser

Datatilsynet offentliggjorde i november 2020 sine akkrediteringskrav til kontrolorganer for adfærdskodekser på tilsynets hjemmeside på både dansk og engelsk. Forud for offentliggørelsen havde tilsynet forelagt kravene for Det Europæiske Databeskyttelsesråd (EDPB) i maj 2020, og dernæst gennemgået en revideringsproces som endte med, at EDPB vedtog en udtalelse om kravene i november 2020.

En databeskyttelsesretlig adfærdskodeks er et sæt af retningslinjer, der specificerer reglerne i databeskyttelsesforordningen for en given branche og kan være et godt værktøj for mindre og mellemstore dataansvarlige og databehandlere til at efterleve reglerne for databeskyttelse.

En adfærdskodeks, som regulerer, hvordan private virksomheder mv. håndterer personoplysninger, skal imidlertid have et akkrediteret kontrolorgan. Kontrolorganets opgave er blandt andet at sikre, at de dataansvarlige og databehandlere, som er tilsluttet kodeksen, overholder kodeksens retningslinjer.

For at blive akkrediteret af Datatilsynet skal kontrolorganet opfylde en række krav, som er fastsat i databeskyttelsesforordningen. Reglerne om akkrediterede kontrolorganer finder ikke anvendelse for behandling, der foretages af offentlige myndigheder og organer.

Kontrolorganet kan enten være eksternt eller internt for kodeksejeren. Databeskyttelsesforordningens artikel 41, stk. 2, fastsætter en række krav, som det indstillede kontrolorgan skal opfylde for at opnå akkreditering. Datatilsynets offentliggjorte retningslinjer skal hjælpe til fortolkning og forståelse af kravene til at opnå akkreditering.

Ny underside om databeskyttelse målrettet børn og unge

Onlineaktivitet er en integreret del af de fleste børn og unges hverdag. Samtidig er det en gruppe, der typisk er mindre bevidste om de risici, der kan gøre sig gældende, når andre behandler oplysninger om dem, ligesom de ofte ikke kender til deres rettigheder på området. Bl.a. på baggrund af dette foreskriver reglerne for databeskyttelse, at børn og unge bør nyde en særlig beskyttelse af deres personoplysninger. Derfor finder Datatilsynet også, at det er en vigtig opgave at gøre en særlig indsats for at oplyse og vejlede børn og unge om deres rettigheder.

I december 2020 lancerede Datatilsynet derfor en ny underside på tilsynet hjemmeside, som henvender sig specielt til børn og unge.

Materialet på siden handler især om brug af sociale medier og deling af billeder på nettet. På siden kan man bl.a. finde videoer, podcast, en quiz og korte tekster om deling af billeder, rettigheder mv. Formålet med siden er dels at oplyse om rettighederne på området, dels at invitere børnene og de unge til at tage kritisk stilling, når andre behandler oplysninger om dem.

Initiativet er blevet taget godt imod – bl.a. er podcasten om deling af billeder blevet afspillet mere end 1.600 gange, og undersiden på vores hjemmeside har haft mere end 4.000 besøgende i løbet af de første to måneder. Endvidere har flere, bl.a. følgere på Datatilsynets LinkedIn-side, efterspurgt mere materiale om databeskyttelse målrettet børn og unge.

Datatilsynet planlægger at følge op på det nye materiale med flere oplysningskampagner rettet mod børn og unge.

Nye fælleseuropæiske vejledninger

Det Europæiske Databeskyttelsesråd (EDPB) har i 2020 vedtaget en række vejledninger mv. om aktuelle databeskyttelsesretlige emner:

Vejledninger om databeskyttelsesretlige spørgsmål vedrørende Covid-19

EDPB vedtog i april 2020 en vejledning om behandling af oplysninger i videnskabelig øjemed og til brug for forskning i relation til Covid-19. Vejledningen har til formål at skabe en fælles forståelse af, på hvilke betingelser og med hvilken hjemmel der kan forskes i Covid-19. Herudover behandler vejledningen spørgsmål om, hvordan de generelle principper for behandling af personoplysninger og den registreredes rettigheder skal iagttages.

EDPB vedtog endvidere i april 2020 en vejledning om behandling af lokationsdata og kontaktopsporingsværktøjer i forbindelse med Covid-19.

Vejledningen fastlægger rammerne for de kriterier, der skal inddrages for at vurdere nødvendigheden og proportionaliteten ved behandling af lokationsoplysninger og kontakter mellem fysiske personers medbragte digitale udstyr til brug for smitteopsporing og sygdomsforebyggelse. Vejledningen indeholder i den forbindelse en række anbefalinger om designet af værktøjer til smittesporing på mobilt udstyr, herunder særligt de funktionelle krav der bør tilgodeses.

Opdatering af vejledning om samtykke

EDPB vedtog i maj 2020 en opdatering af rådets vejledning om samtykke i henhold til databeskyttelsesforordningen.

Der blev kun foretaget mindre ændringer af vejledningen, som havde til formål at præcisere reglerne om gyldigheden af et samtykke i forhold til forskellige tekniske samtykkeløsninger.

Det fremgår nu udtrykkeligt af vejledningen, at et samtykke ikke kan anses for at være givet frivilligt, hvis adgangen til tjenester og funktioner er betinget af en brugers samtykke til, at oplysninger lagres, eller at der opnås adgang til oplysninger, der allerede er lagret i brugerens terminaludstyr (såkaldte cookie walls).

Det fremgår endvidere, at det forhold, at en bruger scroller eller swiper gennem et websted ikke kan anses for tilstrækkeligt til at fastslå, at brugeren dermed har givet samtykke til behandling af sine personoplysninger.

Anbefalinger om europæiske væsentlige garantier for overvågnings-foranstaltninger

EDPB vedtog i november 2020 anbefalinger om europæiske væsentlige garantier for overvågnings-foranstaltninger. Datatilsynet har deltaget aktivt i udarbejdelsen af anbefalingerne.

Anbefalingerne beskriver de garantier, som skal respekteres for at sikre, at indgreb i de registreredes rettigheder ikke går ud over, hvad der er nødvendigt i et demokratisk samfund, når der sker overførsel af personoplysninger til et tredjeland. Garantierne er udledt af retspraksis fra EU-Domstolen, herunder den såkaldte Schrems-II-afgørelse, og af Den Europæiske Menneskerettighedsdomstols retspraksis.

Målet med anbefalingerne er at tilvejebringe en liste over elementer, der skal undersøges, når der overføres personoplysninger til et tredjeland. Garantierne udgør derfor en del af den vurdering, der skal foretages for at afgøre, om et tredjeland yder et beskyttelsesniveau, der i det væsentlige svarer til det, som er garanteret i EU.

Vejledning om samspillet mellem databeskyttelsesforordningen og betalingstjenestedirektivet

EDPB vedtog i december 2020 en vejledning om samspillet mellem reglerne i det reviderede betalingstjenestedirektiv (PSD2) og reglerne i databeskyttelsesforordningen.

Formålet er at give yderligere vejledning om væsentlige databeskyttelsesaspekter inden for anvendelsesområdet af PSD2, herunder samspillet mellem de to regelsæt. Vejledningen adresserer bl.a. de to regelsæts samtykkekrav, behandlingen af oplysninger om tredjeparter (silent par ties), behandlingen af følsomme personoplysninger og de grundlæggende principper for behandling af personoplysninger, herunder dataminimering, gennemsigtighed, ansvarlighed og sikkerhed.

Vejledning om overførsel af personoplysninger til offentlige myndigheder mv. i tredjelande

EDPB vedtog i december 2020 en vejledning om overførsel af personoplysninger fra offentlige myndigheder mv. i EU- eller EØS-lande til offentlige myndigheder mv. uden for EU/EØS.

I databeskyttelsesforordningens artikel 46, stk. 2, litra a, og 46, stk. 3, litra b, er der fastsat særlige retsgrundlag for denne form for overførsel af personoplysninger til tredjelande. Vejledningen fastsætter bl.a., hvilke garantier der skal tilvejebringes, når disse særlige retsgrundlag anvendes.

Det bemærkes, at offentlige myndigheder mv. i EU- og EØS-lande ikke er tvunget til at anvende disse særlige retsgrundlag, idet de også kan gøre brug af de generelle retsgrundlag for overførsel til tredjelande, som i øvrigt er fastsat i databeskyttelsesforordningens artikel 46.

Høringer over lovforslag mv.

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

Datatilsynet registrerede **606** sager i 2020 vedrørende høringer over lovforslag mv.

Datatilsynet forholder sig i sine udtalelser til de eventuelle databeskyttelsesretlige problemstillinger i de foreliggende lovforslag. Datatilsynet anser udtalelserne for at være et væsentligt bidrag til lovgivningsprocessen, eftersom tilsynet besidder en ekspertviden om databeskyttelse og udøver sin funktioner i fuld uafhængighed. Datatilsynet prioriterer derfor denne opgave højt.

Lovforslag om ændring af straffeloven (Initiativer mod fremmedkrigere og andre terrordømte)

I starten af 2020 anmodede Justitsministeriet om Datatilsynets eventuelle bemærkninger til udkast til lovforslag om ændring af straffeloven (Initiativer mod fremmedkrigere og andre terrordømte).

Formålet med forslaget var at forebygge nye terrorhandlinger ved at sikre, at terrordømte ikke skulle fastholdes eller falde tilbage i radikaliserede miljøer samt minimere mulighederne for, at de ville kunne påvirke radikaliseringsudsatte personer i en negativ retning. Lovforslaget indeholdt bl.a. et forslag om, at terrordømte ved dom kunne gives et kontaktforbud, dvs. et forbud mod at søge kontakt med personer, der er dømt for en eller flere terrorrelaterede lovovertrædelser. Det blev endvidere foreslået, at politiet skulle kunne føre tilsyn med sådanne personers overholdelse af forbuddene. Politiet ville i den forbindelse have mulighed for at videregive personoplysninger til den dømte om de personer, som den dømte ikke måtte kontakte. I bemærkningerne til udkast til lovforslag var der lagt op til, at den dømte ville være dataansvarlig for behandlingen af disse personoplysninger med den konsekvens, at den dømtes behandling skulle ske i overensstemmelse med de grundlæggende principper i databeskyttel sesforordningens artikel 5.

For så vidt angår de personoplysninger, som den dømte ville modtage fra politiet, var det Datatilsynets vurdering, at behandlingen skulle anses som en behandling, der blev foretaget af en fysisk person som led i rent personlige aktiviteter, og derfor faldt uden for databeskyttelsesforordningens anvendelsesområde. Datatilsynet bemærkede dog, at den dømtes behandling af personoplysninger efter omstændighederne ville kunne få karakter af andet end ren personlig aktivitet, f.eks. hvis den dømte videregav eller offentliggjorde oplysningerne.

På baggrund af Datatilsynets første høringssvar fremsendte Justitsministeriet fem nye afsnit til tilsynet, som ministeriet på baggrund af tilsynets høringssvar ville tilføje til bemærkningerne til udkastet til lovforslag. I de nye afsnit anførte Justitsministeriet bl.a., at den dømtes behandling af personoplysninger ville være at anse som en behandling, der blev foretaget af en fysisk person som led i rent personlige aktiviteter i overensstemmelse med Datatilsynets vurdering.

Lovforslag om ændring af lov om social pension og forskellige andre love (Indførelse af ret til Tidlig Pension)

Styrelsen for Arbejdsmarked og Rekruttering anmodede i november 2020 Datatilsynet om eventuelle bemærkninger til forslag til lov om ændring af lov om social pension og forskellige andre love (Indførelse af ret til Tidlig Pension).

Med loven indføres tidlig pension for personer, der har tre år eller mindre til folkepensionsalderen, og som har haft en langvarig tilknytning til arbejdsmarkedet.

Lovforslaget indebar bl.a., at Udbetaling Danmark – for at kunne tage stilling til borgerens ret til tidlig pension – får mulighed for bl.a. via Danmarks Statistik at indsamle personoplysninger, som er indsamlet til statistisk brug samt historiske oplysninger, der er overført til bevaring i Rigsarkivet.

For så vidt angår Udbetaling Danmarks indsamling af personoplysninger fra Rigsarkivet lagde Datatilsynet til grund, at denne indsamling (og Rigsarkivets videregivelse af personoplysningerne) vil ske inden for rammerne af gældende arkivlovgivning.

Datatilsynet bemærkede om Udbetaling Danmarks indsamling af personoplysninger fra bl.a. Danmarks Statistik, at viderebehandling af personoplysninger, der er eller bliver behandlet med henblik på arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske

formål, til andre formål end disse, som altovervejende hovedregel må betragtes som uforeneligt med det formål, hvortil de oprindeligt er behandlet, hvilket som udgangspunkt vil være i strid med databeskyttelsesforordningens regler om formålsbegrænsning. Dette medfører bl.a., at personoplysninger, som behandles alene med henblik på at udføre statistiske eller videnskabelige undersøgelser, som altovervejende hovedregel ikke må anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer.

Databeskyttelsesforordningen er imidlertid ikke til hinder for viderebehandling af personoplysninger, hvis behandlingen er hjemlet i national ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til et af de mål, som udtømmende er angivet i databeskyttelsesforordningen.

Af lovforslagets bemærkninger fremgik, at lovforslaget var en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til andre vigtige målsætninger i forbindelse med beskyttelse af generelle samfundsinteresser.

Datatilsynet bemærkede i den forbindelse, at hvad der udgør generelle samfundsinteresser som omhandlet i databeskyttelsesforordningen i sidste ende er en politisk beslutning.

Datatilsynet fandt imidlertid anledning til at påpege, at lovgivningen i Danmark hjemler en vid adgang til at gennemføre omfattende statistiske og videnskabelige undersøgelser, herunder med hjemmel i lov om Danmarks Statistik. Denne vide adgang til at gennemføre statistiske og videnskabelige undersøgelser hviler på en forudsætning om, at det sker på en ansvarlig måde, herunder at behandlingen er underlagt fornødne garantier for registreredes rettigheder og frihedsrettigheder. En af disse "fornødne garantier" er, at personoplysninger, der bliver behandlet med henblik på udførelse af statistiske og videnskabelige undersøgelser, ikke senere anvendes til andre formål, herunder til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer.

Datatilsynet understregede derfor, at det er vigtigt at holde sig for øje, at hver gang der ved lovgivningsmæssige foranstaltninger sker en fravigelse af denne garanti, bliver det efter Datatilsynets opfattelse mere og mere vanskeligt inden for rammerne af databeskyttelsesforordningen at opretholde det oprindelige lovgrundlag, der hjemler behandling af personoplysninger til brug for udførelsen af statistiske og videnskabelige undersøgelser.

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 i 2020 indgivet 11 politianmeldelser med indstilling om bøde efter databeskyttelsesforordningen. Heraf udsprang den ene af et tilsyn, som Datatilsynet havde opstartet i 2018. Herudover har Datatilsynet anmeldt et mindre antal sager til politiet med henblik på ydereligere efterforskning af sagen.

Det er derfor væsentligt, at Datatilsynets medarbejdere har et godt kendskab til de mange forhold, som det er vigtigt at være opmærksom 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 sammen med Rigspolitiet (herunder Nationalt Cyber Crime Center, NC3) og Rigsadvokaten.

Datatilsynet har ligeledes bidraget til udarbejdelsen af Rigsadvokatmeddelelsens afsnit om håndtering af sådanne sager og aftalt løbende opfølgninger med såvel Rigspolitiet som Rigsadvokaten. Herudover er der i Datatilsynet 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

Datatilsynet træffer i klagesager afgørelse om, hvornår den dataansvarliges 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, og om klagen hører under tilsynets kompetence, og hvorvidt 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 klage anses for uforholdsmæssig, inddrages Datatilsynets opgaver og forpligtelser. Også 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 også 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.

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), hvori Datatilsynet vil skulle behandle klagesagen i samarbejde med andre europæiske datatilsyn.

Der vil i den forbindelse blive udpeget en ledende tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 56, stk. 1, og det er denne tilsynsmyndighed, som vil stå for selve behandlingen af klagesagen. Den ledende tilsynsmyndighed er tilsynsmyndigheden for den dataansvarliges hovedvirksomhed eller eneste etablering i Unionen. Det 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 og andre datatilsyn, der er berørte af den pågældende grænseoverskridende behandling, vil via IMI-systemet have mulighed for at kommentere på og komme med indsigelser mod den ledende tilsynsmyndigheds afgørelse i sagen.

Nedenfor ses eksempler på klagesager, som Datatilsynet i 2020 traf afgørelse i.

Behandling af personoplysninger om en persons besøg på en hjemmeside

Datatilsynet traf i februar 2020 afgørelse i en sag vedrørende Danmarks Meteorologiske Institut (DMI)'s behandling af personoplysninger om en persons besøg på instituttets hjemmeside i forbindelse med visning af bannerannoncer på hjemmesiden.

Efter at sagen havde været forelagt Datarådet, udtalte Datatilsynet, at hverken DMI's tidligere eller nuværende løsning til indhentning af samtykke til behandling af personoplysninger om de besøgende på dmi.dk opfyldte databeskyttelsesforordningens krav til den registreredes samtykke i artikel 4, nr. 11, og det grundlæggende princip om lovlighed, rimelighed og gennemsigtighed i artikel 5, stk. 1, litra a.

Endvidere fandt Datatilsynet, at DMI's behandling af personoplysninger om klager ved indsamling og videregivelse til Google var i strid med databeskyttelsesforordningens artikel 6, idet ingen af de i artikel 6, stk. 1, nævnte forhold gjorde sig gældende.

Tilsynet lagde bl.a. vægt på, at indsamling af personoplysninger til forskellige formål på baggrund af ét samlet samtykke ikke gav de besøgende et tilstrækkeligt frit valg i forhold til at kunne identificere og til- og fravælge, hvilke formål de besøgende reelt ønskede at give samtykke til. Tilsynet lagde i tilknytning hertil også vægt på, at samtykket ikke var tilstrækkeligt informeret, idet der manglede informationer om de andre dataansvarlige - herunder Google – der blev indsamlet personoplysninger i samarbejde med og videregivet personoplysninger til.

Datatilsynet lagde endvidere vægt på, at DMI's samtykkeløsning ikke gav den besøgende mulighed for at afslå behandling af personoplysninger ved det indledende besøg på dmi.dk. Det krævede, at den besøgende valgte funktionen "Vis detaljer" for derefter at vælge "Opdater samtykke". En sådan "et-klik-væk" fremgangsmåde er efter Datatilsynets opfattelse ikke gennemsigtig og derfor i strid med det grundlæggende princip i databeskyttelsesforordningen.

På den baggrund fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at DMI's behandling af personoplysninger om de besøgende på dmi.dk, herunder klager, ikke var sket i overensstemmelse med databeskyttelsesforordningen.

Behandling af personoplysninger i rent private sammenhænge

Behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter, er ikke omfattet af databeskyttelsesreglerne.

Ved vurderingen af, om en privatpersons offentliggørelse af personoplysninger på internettet kan anses for at være sket i rent private sammenhænge – og dermed falder uden for databeskyttelsesreglernes anvendelsesområde – skal der foretages en konkret helhedsvurdering af offentliggørelsen, herunder om aktiviteten kan anses for at være legitim, ligesom der også kan lægges vægt på, om der er tale om en aktivitet, der anses for sædvanlig i den konkrete sammenhæng. I den forbindelse kan bl.a. inddrages karakteren af de offentliggjorte oplysninger, konteksten, hvori oplysningerne er offentliggjort, og formålet med offentliggørelsen. Det kan også indgå i vurderingen, om behandlingen er uden forbindelse med erhvervsmæssig eller kommerciel aktivitet.

Datatilsynet har i 2020 truffet en række konkrete afgørelser, som illustrerer, hvornår behandling af personoplysninger sker i rent personlig eller familiemæssig sammenhæng. Datatilsynet har bl.a. i to konkrete sager fundet, at offentliggørelse af personoplysninger på henholdsvis en hjemmeside og på YouTube i de konkrete tilfælde måtte anses for at være sket i rent private sammenhænge. Omvendt fandt Datatilsynet i en anden sag, at et opslag på en persons Facebook-profil ikke var sket i en rent privat sammenhæng, da opslagene havde nær tilknytning til personens enkeltmandsvirksomhed.

I en af de sager, som Datatilsynet har behandlet i 2020, havde en borger klaget over offentliggørelse på en hjemmeside af korrespondance mellem ham og ejeren af hjemmesiden, som bl.a. indeholdt oplysninger om klagerens navn og hans betragtninger om en kendt forfatters forfatterskab.

Efter en samlet vurdering, og efter at sagen havde været forelagt Datarådet, konkluderede Datatilsynet, at databeskyttelsesforordningen ikke fandt anvendelse i sagen, da offentliggørelsen af oplysninger om klageren måtte anses for en behandling foretaget af en fysisk person som led i rent personlige eller familiemæssige aktiviteter. Datatilsynet lagde vægt på, at offentliggørelsen var sket i relation til en debat om den kendte forfatters forfatterskab, og at hjemmesiden havde karakter af en blog, hvor ejeren bl.a. fremkom med egne holdninger om forskellige emner og efter det oplyste indsamlede og formidlede viden om fagområder, hvilket efter Datatilsynets vurdering måtte anses for sædvanlige og legitime aktiviteter. Datatilsynet lagde endvidere vægt på karakteren af de omhandlende oplysninger, herunder at der var tale om ikke-følsomme oplysninger, som efter Datatilsynets opfattelse var af harmløs karakter. Herudover lagde Datatilsynet vægt på, at en del af den offentliggjorte korrespondance indeholdt meningstilkendegivelser, og at offentliggørelsen i øvrigt ikke skete med henblik på at skabe en økonomisk fortjeneste.

Offentliggørelse af gamle klubblade - Jyllinge Sejlklub

Datatilsynet traf afgørelse i en sag, hvor en borger klagede til tilsynet over, at foreningen Jyllinge Sejlklub havde lagt tre af foreningens klubblade fra 1981 og 1982 på internettet, hvori der fremgik oplysninger om borgerens navn, adresse, alder og billede, og at foreningen havde afvist at imødekomme borgerens anmodning om sletning af de pågældende oplysninger.

Datatilsynet bemærkede i afgørelsen, at en forenings behandling af personoplysninger er omfattet af databeskyttelsesretten, og at foreninger derfor skal iagttage de databeskyttelsesretlige regler i forbindelse med behandling af personoplysninger.

Datatilsynet fastslog at det er i overensstemmelse med de databeskyttelsesretlige regler, at Jyllinge Sejlklub har offentliggjort tre af foreningens klubblade på internettet, hvori der fremgår personoplysninger om borgeren. Datatilsynet lagde vægt på oplysningernes karakter, klubbladenes alder og foreningens legitime interesse i at værne om, beskytte og informere om sin historie i en naturlig kontekst.

Efter Datatilsynets opfattelse havde Jyllinge Sejlklub handlet i overensstemmelse med de databeskyttelsesretlige regler ved ikke at imødekomme borgerens anmodning om sletning af de oplysninger om borgeren, som fremgår af klubbladene. Datatilsynet lagde i vurderingen heraf vægt på, at Jyllinge Sejlklub behandler oplysninger om borgeren på et lovligt grundlag, og at borgeren ikke har anført særlige grunde, som går forud for foreningens interesse i at behandle oplysningerne.

Utilstrækkelig sikkerhed ved levering af inkassobreve

Datatilsynet traf afgørelse i en sag, hvor en borger klagede over, at Alektum A/S den 10. og den 15. september 2019 har afleveret to breve til borgeren ved at placere dem ved borgerens hoveddør i stedet for i borgerens postkasse.

Alektum A/S har indgået en databehandleraftale med RoestNielsen ApS, hvorefter RoestNielsen ApS leverede breve til borgeren på vegne af Alektum A/S. Datatilsynet vurderede, at sagen skulle rettes mod RoestNielsen ApS som databehandler.

Datatilsynet fandt, at RoestNielsen ApS ikke havde handlet i overensstemmelse med den instruks, som RoestNielsen ApS var blevet underlagt af Alektum A/S som dataansvarlig.

Datatilsynet udtalte herefter kritik af databehandleren RoestNielsen ApS, idet virksomheden ikke levede op til kravene om et passende sikkerhedsniveau i databeskyttelsesforordningens artikel 32 i forbindelse med levering af inkassobrevene fra Alektum A/S til borgeren, idet en konsulent ansat ved RoestNielsen ApS afleverede inkassobreve til borgeren ved at placere brevene ved borgerens hoveddør.

I vurderingen lagde Datatilsynet vægt på, at konsulenten ikke afleverede brevene i borgerens postkasse - uagtet at borgeren havde en postkasse - og at kuverterne var placeret så tilgængelige, at der var en stor risiko for, at de ville gå tabt i et eventuelt uvejr, eller at uvedkommende ville kunne tilgå dem. Datatilsynet lagde endvidere vægt på, at der i brevene fremgik oplysninger om inkasso og gæld, og at eksponering af sådanne oplysninger ville kunne indebære alvorlige krænkelser for borgeren.

Forkert behandlingsgrundlag

Ved valg af behandlingsgrundlag skal en dataansvarlig altid forud for påbegyndelsen af behandling af personoplysninger gøre sig klart, hvilket behandlingsgrundlag i databeskyttelsesforordningens artikel 6, der er det mest passende. En dataansvarlig kan have flere behandlingsgrundlag til forskellige behandlingsformål vedrørende de samme personoplysninger og skal også i denne situation, inden behandlingen påbegyndes, have gjort sig klart, i hvilke situationer de forskellige behandlingsgrundlag finder anvendelse.

Hvis en behandling ønskes foretaget på grundlag af den registreredes samtykke, skal den dataansvarlige bl.a. overveje, om det reelt vil være muligt for den registrerede at trække sit samtykke tilbage, herunder hvilke konsekvenser dette i givet fald vil have, idet den behandling af oplysninger, som den dataansvarlige foretager på grundlag af samtykket, skal ophøre ved tilbagekaldelse.

På baggrund af en konkret klage udtalte Datatilsynet alvorlig kritik af, at Rejsekort & Rejseplan A/S (Rejsekort) havde behandlet klagerens oplysninger i strid med princippet om lovlighed, rimelighed og gennemsigtighed, da Rejsekort ikke burde have behandlet oplysninger om klager på baggrund af et samtykke. Samtykke var ikke det mest passende behandlingsgrundlag særligt fordi, at Rejsekort havde tilrettelagt sin behandling af personoplysninger således, at der skulle ske skift af behandlingsgrundlaget. Hvis samtykket blev trukket tilbage, ville Rejsekort fortsat behandle oplysninger om klager i medfør af forordningens artikel 6, stk. 1. Samtykke ville dermed reelt ikke kunne trækkes tilbage, og klager havde ikke den kontrol over oplysningerne, som der burde følge med et samtykke.

Da Rejsekort havde oplyst, at behandlingen af oplysninger om personer, der havde et rejsekort, var baseret på samtykke, var det Datatilsynets opfattelse, at Rejsekort skulle foretage en fornyet vurdering af behandlingsgrundlaget for behandlingen af personoplysninger om andre end klager i de tilfælde, hvor behandlingen var baseret på et samtykke.

Sager på eget initiativ

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

Oversigt over udførte tilsyn i 2020

Offentlige myndigheder:
Aarhus Universitet
ATP (Arbejdsmarkedets Tillægspension)
Børne- og Undervisningsministeriet
Esbjerg Kommune
Familieretshuset
IT-Universitetet i København
Odense Kommune
Region Hovedstaden
Region Syddanmark
Slagelse Kommune
Udlændingestyrelsen
Udviklings- og Forenklingsstyrelsen
Kolding Kommune
Nævnenes Hus

Private virksomheder:
Aleris Hamlet Hospitaler A/S
Codan Forsikring A/S
Danske Spil A/S
IDA Ingeniørforeningen i Danmark
Salling Group A/S
TDC A/S
SIF Gruppen A/S
SDC A/S
Carlsberg A/S

Tilsyn med fælleseuropæiske systemer

Offentlige myndigheder:
Ankenævnet for Bus, Tog og Metro
Arbejdstilsynet
Beredskabsstyrelsen
Civilstyrelsen
Energistyrelsen

Erhvervsstyrelsen
Finanstilsynet
Forbrugerombudsmanden
Forbruger Europa
Færdselsstyrelsen
Fødevarestyrelsen
Geodatastyrelsen
Gældsstyrelsen
Jernbanenævnet
Justitsministeriet
Konkurrence- og Forbrugerstyrelsen
Kulturministeriet
Landbrugsstyrelsen
Lægemiddelstyrelsen
Naturstyrelsen
Miljøstyrelsen
Politiets administrative center (PAC)
Psykolognævnet
Ankestyrelsen Aalborg
Radio- og tv-nævnet
Rigspolitiet
Sikkerhedsstyrelsen
Slots- og Kulturstyrelsen
Styrelsen for Dataforsyning og Effektivisering
Styrelsen for Forskning og Uddannelse
Styrelsen for International Rekruttering og Integration
Styrelsen for Patientsikkerhed
Sundheds- og Ældreministeriet
Sundhedsstyrelsen
Søfartsstyrelsen
Trafik-, Bygge- og Boligstyrelsen
Transport- og Boligministeriet
Udenrigsministeriet – Borgerservice
Udlændinge- og Integrationsministeriet

Private virksomheder:
Advokatsamfundet
Advokatsamfundet
Agro Business Park – EEN Danmark
Dansk Byggeri
Dansk Erhverv
Dansk Industri
Erhvervshus Sjælland – EEN Danmark
Forbrugerrådet Tænk
Forsikring & Pension
IDA Ingeniørforeningen i Danmark
NordDanmarks EU-kontor – EEN Danmark

Den Digitale Prøvevagt

Datatilsynet valgte i marts 2019 på baggrund af bl.a. medieomtale at undersøge programmet "Den Digitale Prøvevagt" af egen drift.

Den Digitale Prøvevagt var et monitoreringsprogram, der var under udvikling af Styrelsen for It og Læring (STIL). Det var hensigten, at programmet skulle anvendes af de gymnasiale institutioner. Programmet dokumenterede en række handlinger, som eleverne foretog på deres computer under afvikling af prøver, med henblik på at kunne opdage og forebygge snyd under prøverne.

Der var den 7. marts 2019 blevet gennemført en generalprøve af programmet. Det var frivilligt for eleverne, om de ønskede at medvirke, og dermed om de ønskede at aktivere monitoreringssystemet under prøven. Der var ca. 8.000 elever, der valgte at installere og teste Den Digitale Prøvevagt. Der blev i forbindelse med denne generalprøve behandlet personoplysninger om de elever, som frivilligt havde installeret og testet systemet.

Ved udtalelse af 6. marts 2020 fandt Datatilsynet anledning til at udtale alvorlig kritik af, at STILs behandling af personoplysninger i forbindelse med generalprøven ikke skete i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32.

STIL havde ikke forud for generalprøven foretaget en risikovurdering. I forbindelse med generalprøven samt en efterfølgende risikovurdering blev der konstateret flere sikkerhedsmæssige problematikker. Endvidere kom STIL efter gennemførslen af generalprøven frem til, at der skulle udføres en fornyet risikovurdering, og at kriterierne for, at der skulle foretages en konsekvensanalyse var opfyldt. Datatilsynet fandt, at den efterfølgende risikovurdering viste en række forhold, hvor den implementerede sikkerhed ved generalprøven var utilstrækkelig.

Da programmet på tidspunktet for Datatilsynets udtalelse ikke var færdigudviklet, fandt tilsynet, at der ikke var grundlag for at tage stilling til behandlingen af personoplysninger ved brug af dette program. Datatilsynet har efterfølgende haft et møde med STIL og Børne- og Undervisningsministeriet, hvor de databeskyttelsesretlige spørgsmål omkring monitorering af elevers computere under afholdelse af prøver og eksamener blev drøftet.

Fem tilsyn med efterlevelse af oplysningspligten

I 2020 afsluttede Datatilsynet fem planlagte skriftlige tilsyn, som tilsynet havde startet op i efteråret 2019. Tilsynene fokuserede på efterlevelse af reglerne om oplysningspligt ved brug af kontrolforanstaltninger over for medarbejdere. Datatilsynet havde udvalgt to private virksomheder (TDC A/S og SIF Gruppen A/S) og tre offentlige myndigheder (Arbejdsmarkedets Tillægspension, Kolding Kommune og Nævnenes Hus).

Det følger af databeskyttelsesforordningens artikel 13 og 14, at den dataansvarlige har pligt til at give en række informationer til den registrerede, når der behandles oplysninger om vedkommende. Dette gælder naturligvis også, når en arbejdsgiver behandler oplysninger om sine medarbejdere.

Databeskyttelsesforordningens artikel 5, stk. 1, litra a, indeholder endvidere et grundlæggende princip om, at enhver behandling af personoplysninger skal være lovlig, rimelig og gennemsigtig.

Ved arbejdsgivers behandling af personoplysninger i forbindelse med kontrolforanstaltninger over for de ansatte medfører princippet om gennemsigtighed efter Datatilsynets opfattelse, at arbejdsgiveren som udgangspunkt skal give de ansatte lettilgængelig, forudgående information om de anvendte kontrolforanstaltninger, herunder særligt om kontrolformålet.

I forbindelse med de skriftlige tilsyn har Datatilsynet påset, om virksomhederne og myndighederne har efterlevet reglerne om oplysningspligt i forbindelse med brugen af kontrolforanstaltninger over for medarbejdere, jf. forordningens artikel 13 og 14. Herudover har tilsynet generelt påset, om virksomhedernes og myndighedernes iagttagelse af oplysningspligten lever op til princippet om gennemsigtighed i forordningens artikel 5, stk. 1, litra a.

Datatilsynet endte med at udtale alvorlig kritik i tre af de fem sager. I de øvrige to sager udtalte tilsynet kritik.

Over for Kolding Kommune udtalte Datatilsynet alvorlig kritik af, at kommunen i vidt omfang havde iagttaget oplysningspligten mundtligt over for kommunens medarbejdere, hvilket ikke er i overensstemmelse med forordningens artikel 12, stk. 1, 2. pkt., som bl.a. foreskriver, at oplysningerne skal gives skriftligt. Herudover havde Kolding Kommunes efterlevelse af oplysningspligten været mangelfuld, fordi kommunen ikke havde givet medarbejderne tilstrækkelig information om formålet med behandlingen af personoplysninger, retsgrundlaget for behandlingen af personoplysninger, de berørte kate-

gorier af personoplysninger og det tidsrum, hvor oplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum.

Datatilsynet udtalte over for Arbejdsmarkedets Tillægspension alvorlig kritik af, at myndighedens efterlevelse af oplysningspligten havde været mangelfuld, fordi myndigheden ikke havde givet medarbejderne tilstrækkelig tydelig information om formålet med behandlingen af oplysningerne, retsgrundlaget for behandlingen, de berørte kategorier af personoplysninger og det tidsrum, hvor oplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier der anvendes til at fastlægge dette tidsrum. Herudover var den information, som Arbejdsmarkedets Tillægspension havde givet til sine medarbejdere, ikke blevet givet til medarbejderne i en tiltrækkelig lettilgængelig form.

I forbindelse med tilsynet over for SIF Gruppen A/S udtalte Datatilsynet alvorlig kritik af, at virksomhedens efterlevelse af oplysningspligten i forbindelse med brugen af GPS-overvågning havde været mangelfuld, fordi virksomheden ikke havde givet medarbejderne tilstrækkelig information om retsgrundlaget for behandling af personoplysninger, den registreredes rettigheder og retten til at indgive klage til Datatilsynet. Herudover havde SIF Gruppen A/S ikke underrettet medarbejderne om den behandling af personoplysninger, der finder sted i forbindelse med tv-overvågning, hvorfor det heller ikke havde været tilstrækkeligt gennemsigtigt for medarbejderne, at tv-overvågningen kunne anvendes i kontroløjemed.

For så vidt angår Nævnenes Hus udtalte Datatilsynet kritik af, at myndighedens efterlevelse af oplysningspligten i flere tilfælde havde været mangelfuld, fordi myndigheden ikke havde givet medarbejderne tilstrækkelig tydelig information om identiteten på den dataansvarlige, formålet med behandlingen af oplysningerne, retsgrundlaget for behandlingen, de berørte kategorier af personoplysninger, eventuelle modtagere eller kategorier af modtagere af oplysningerne, og det tidsrum, hvor oplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier der anvendes til at fastlægge dette tidsrum.

Over for TDC A/S udtalte Datatilsynet kritik af, at virksomhedens efterlevelse af oplysningspligten i et tilfælde havde været mangelfuld, da virksomheden ikke havde givet medarbejderne tilstrækkelig, tydelig information om formålet med behandlingen af oplysningerne. Datatilsynet fandt dog samtidig, at virksomhedens iagttagelse af oplysningspligten over for medarbejdere i forbindelse med brug af kontrolforanstaltninger generelt var sket i en tilstrækkelig gennemsigtig og lettilgængelig form.

Tilsyn om brug af personoplysninger som testdata og underdatabehandlere

I 2020 afsluttede Datatilsynet et planlagt tilsyn med SDC A/S, som tilsynet havde startet op i efteråret 2019. Tilsynet fokuserede på virksomhedens brug af oplysninger om fysiske personer i testmiljøer og virksomhedens brug af underdatabehandlere. Tilsynet blev gennemført som et skriftligt tilsyn, idet Datatilsynet efter at have gennemgået det af SDC A/S fremsendte materiale vurderede, at det ikke var nødvendigt med et egentligt fysisk tilsynsbesøg.

I forhold til brugen af personoplysninger som testdata fokuserede tilsynet særligt på, om SDC A/S havde foretaget den fornødne vurdering af risikoen for de registreredes rettigheder i testmiljøer, hvor testmiljøet var forskelligt fra de systemer i drift, hvor virksomheden som databehandler behandlede oplysninger på vegne af de dataansvarlige. På baggrund af de modtagne oplysninger valgte Datatilsynet at fokusere på ét it-system.

Det følger af databeskyttelsesreglerne, at dataansvarlige og databehandlere skal sørge for – på baggrund af en vurdering af risikoen for de pågældende personers rettigheder – at etablere passende sik-

kerhedsforanstaltninger. Det er i den forbindelse Datatilsynets opfattelse, at en sådan risikovurdering som minimum bør tage stilling til:

- Hvilke relevante trusler der er mod fortroligheden, tilgængeligheden og integriteten af de oplysninger, der behandles om de pågældende personer,
- for hver trussel vurdere sandsynligheden for, at den enkelte trussel er reel for den pågældende behandlingsaktivitet, og
- for hver trussel vurdere de mulige konsekvenser for personerne.

På baggrund af sandsynligheden og konsekvensen for den enkelte trussel kan risikoen vurderes, herunder med hensynstagen til de eventuelle eksisterende foranstaltninger der måtte være truffet.

Efter en gennemgang af det materiale, som SDC A/S havde sendt til Datatilsynet, vurderede tilsynet, at virksomhedens risikovurdering ikke indeholdt de ovenfor nævnte elementer. Samlet set fandt Datatilsynet, at SDC A/S i forhold til den konkrete behandling ikke havde foretaget en risikobaseret tilgang til behandlingssikkerheden. Datatilsynet fandt på den baggrund anledning til at udtale kritik.

For så vidt angår SDC A/S' brug af underdatabehandlere fokuserede tilsynet navnlig på, om virksomheden havde pålagt sine underdatabehandlere de samme forpligtelser, som virksomheden selv, som databehandler, var blevet pålagt i databehandleraftalerne med to udvalgte dataansvarlige.

I forbindelse med tilsynet gennemgik Datatilsynet derfor en kopi af SDC A/S' databehandleraftaler med de to udvalgte kunder og en kopi af SDC A/S' aftaler med tre specifikke underdatabehandlere, som SDC A/S gør brug af i forbindelse med den behandling af personoplysninger, som virksomheden foretager på vegne af de to dataansvarlige kunder.

Databeskyttelsesforordningen fastsætter en række specifikke krav til indholdet af en databehandleraftale. Aftalen skal bl.a. indeholde oplysninger om de pligter, som databehandleren har i forhold til at varetage den pågældende opgave for den dataansvarlige, ligesom det skal fremgå af aftalen, om databehandleren må gøre brug af underdatabehandlere i forbindelse med opgaven.

Efter en gennemgang af aftalerne fandt Datatilsynet, at SDC A/S havde pålagt sine underdatabehandlere de samme forpligtelser, som virksomheden selv er blevet pålagt i databehandleraftalerne med to udvalgte dataansvarlige, hvilket var i overensstemmelse med reglerne.

Tilsyn med Carlsberg Danmark A/S

I 2020 afsluttede Datatilsynet et skriftligt tilsyn med Carlsberg Danmark A/S, som tilsynet havde startet op i sommeren 2019. Tilsynet fokuserede på Carlsbergs opbevaring og sletning af personoplysninger om ansøgere indsamlet i forbindelse med rekruttering til ansættelse, hvor ansøgeren ikke blev ansat.

Carlsberg oplyste under tilsynssagen, at virksomheden behandler oplysninger om ansøgere, som ikke er blevet ansat, til to formål:

Oplysningerne bliver opbevaret for at sikre dokumentation for korrekt rekrutteringsforløb. Disse oplysninger bliver opbevaret på baggrund af virksomhedens legitime interesse. Herudover opbevarer Carlsberg oplysninger om ansøgere med henblik på at oplyse om fremtidige jobmuligheder i virksomheden. Disse oplysninger bliver opbevaret på baggrund af ansøgerens samtykke.

Datatilsynet fandt, at Carlsberg i begge tilfælde havde lovligt grundlag til behandlingen i databeskyttelsesforordningens artikel 6.

Med hensyn til Carlsbergs opbevaring og sletning af oplysninger om ansøgere, der ikke blev ansat, fremgik det af tilsynet, at Carlsberg opbevarer oplysninger i op til seks måneder efter endt rekrutteringsforløb. Oplysningerne gemmes i Carlsbergs rekrutteringssystem, hvor der sker automatisk sletning af oplysninger, der er seks måneder gamle, den første i hver måned. Herudover har ansøgere mulighed for selv at slette deres ansøgerprofil inden for perioden på seks måneder.

Datatilsynet fandt, at Carlsbergs behandling også i denne henseende var i overensstemmelse med reglerne.

Tik Tok

Datatilsynet indledte i juni 2020 en undersøgelse af videoappen TikTok med det formål at vurdere, om tjenesten lever op til reglerne for databeskyttelse.

TikTok er meget populært blandt især børn, som ifølge databeskyttelsesforordningen har krav på en særlig beskyttelse af deres oplysninger. Derfor så Datatilsynet på omfanget og grundlaget for den behandling af personoplysninger, der sker i appen. Endvidere dækkede undersøgelsen en række sikkerhedsmæssige aspekter af TikTok.

TikTok oplyste tidligt i afklaringen af sagen, at de ville etablere sig i Europa med hovedsæde i Irland, og i december 2020 oplyste det irske datatilsyn, at TikTok er hovedetableret i Irland. Datatilsynet i Danmark besluttede derfor – i overensstemmelse med reglerne i forordningen – at overdrage sagen til det irske datatilsyn.

I hele forløbet har der været et tæt samarbejde med andre europæiske tilsynsmyndigheder, som har haft lignende undersøgelser rettet mod TikTok. I samarbejde med de øvrige myndigheder bliver de danske undersøgelser overdraget til Irland. Datatilsynet i Irland kan fortsætte på det fundament, som er tilvejebragt af de øvrige europæiske tilsyn. Datatilsynet vil følge sagen tæt og søge indflydelse på en endelig afgørelse over for TikTok.

Anmeldelse af brud på persondata-sikkerheden

Opgørelse af brud på persondatasikkerheden i 2020

Datatilsynet modtager stadigvæk en stor mængde anmeldelser om brud på persondatasikkerheden. I 2020 blev der anmeldt næsten 9000 af disse brud. I de uger der blev modtaget flest, var tallet op i mod 300 på én uge.

Som et led i en ny strategi for en mere data- og risikobaseret indsats har Datatilsynet lavet en mere dynamisk opgørelse over anmeldelserne på tilsynets hjemmeside. Denne datakilde skal også understøtte det strategiske arbejde med et tilsynskoncept, der inkluderer empiri om, hvor risikoen for de registrerede opstår ved behandlingerne. Statistikken skal fungere som et værktøj, der bidrager til at opfylde et af tilsynets mål om at basere udvælgelsen af kontrolområder på tilgængelige datakilder og derved føre tilsyn, hvor effekten er størst.

Det er meningen, at statistikken skal komme månedligt og kunne tilgås på tilsynets hjemmeside. De nye statistikker udbygger og erstatter de tidligere kvartalvise opgørelser.

Tallene viser meget den samme tendens som de første opgørelser, Datatilsynet lavede i det første år efter 25. maj 2018. Det er de dataansvarlige, der har flest kontakter med de registrerede, der har de fleste brud.

De typetilfælde, der indberettes, er stadig overvejende af typen, hvor oplysninger til en person sendes forkert til en anden, men visse typer af cyberkriminalitet har også udviklet sig, f.eks. Ransomwareangreb, hvor eksponering af personoplysninger bliver benyttet som et pressionsmiddel for betaling.

Brugen af personoplysninger i udvikling og misvisende risikovurdering

Datatilsynet har i 2020 udtalt kritik af, at en databehandler i forbindelse med overtagelsen af et udviklings- og testmiljø fra en anden leverandør (før forordningen fandt anvendelse) ikke havde gennemført passende sikkerhedsforanstaltninger.

Da databehandleren erhvervede it-løsningen (i forbindelse med et virksomhedsopkøb) blev det ikke påset, i hvilket omfang en test- og udviklingsserver indeholdt oplysninger om fysiske personer. Serveren var til brug for udviklingsopgaver opkoblet mod netværk udenfor databehandlerens kontrol (inter nettet), og den 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 - indeholdte personhenførbare informationer fra flere dataansvarlige.

Datatilsynet fandt, at bruddet kunne have været undgået, hvis der havde været indført helt almindelige, tekniske sikkerhedsforanstaltninger (bl.a. firewallregler), 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).

Denne sag fik Datatilsynet til at komme med følgende konkrete udmelding om brugen produktionsdata i test- og udviklingsmiljøer, som også er at finde på tilsynets hjemmeside:

Generelt om testmiljøer og produktionsdata

Generelt set skal Datatilsynet indskærpe, at der også i forbindelse med udvikling og test udvises den fornødne opmærksomhed, hvis der sker behandling af oplysninger om fysiske personer. Der er konstateret flere tilfælde, hvor udviklere enten på egen hånd, i samarbejde med forretningen eller som aftalt led i udviklingen benytter produktionsdata for at sikre kvaliteten af løsningen.

Dette er der ikke nødvendigvis noget forkert i, så længe der foreligger en vurdering af risikoen for de registreredes rettigheder, og der i overensstemmelse med denne er etableret en passende sikkerhed inden behandlingen påbegyndes, og at der i alle de tilfælde, hvor risikoen for den registrerede måtte være høj, er foretaget en konsekvensanalyse.

Lidt forenklet sagt gælder det, at hvis man ønsker at bruge produktionsdata, skal der som udgangspunkt være den samme sikkerhed på ens udviklings- og testmiljø som det, der er vurderet som passen de i driftssetuppet.

Databehandlers behandling af oplysninger uden for instruks

Datatilsynet har i 2020 behandlet flere sager, hvor databehandlere har anvendt en ikke godkendt underleverandør. Tilsynet har i disse sager udtalt alvorlig kritik af, at databehandlerens brug af underleverandøren ikke var i overensstemmelse med reglerne og den indgåede databehandleraftale.

Kommune

Datatilsynet udtalte alvorlig kritik i en sag, hvor en kommune anmeldte et brud på persondatasikkerheden, da en databehandler havde overført personoplysninger til en ikke godkendt leverandør.

Leverandøren, som databehandleren overførte personoplysninger til, behandlede oplysningerne i usikre tredjelande. Databehandlerens overførsel af data til leverandøren var i strid med databeskyttelsesforordningen, hvor databehandlere ikke må gøre brug af databehandlere uden forudgående godkendelse fra den dataansvarlige.

Ved sin udtalelse af graden af kritik lagde Datatilsynet vægt på, at der var tale om oplysninger vedrørende et højt antal registrerede, at oplysningerne omfattede personnummer, og at der var sket uhjemlet overførsel af personoplysninger til usikre tredjelande.

Forsikringsselskab

I en lignende sag havde et forsikringsselskab benyttet en databehandler, der var indrømmet ret til brug af underdatabehandlere, disse skulle dog anmeldes til den dataansvarlige efter databeskyttelsesforordningens artikel 28, stk. 2, 2. pkt., hvilket ikke skete.

Datatilsynet udtalte alvorlig kritik af databehandleren for ikke at have foretaget den fornødne underretning og for ikke at have haft behandlingshjemmel til den viderebehandling, der blev foretaget i de yderligere led i kæden af underdatabehandlere.

Datatilsynet fandt endvidere, at der skulle være dokumentation for, at alle underdatabehandlere, som databehandleren benytter, er godkendt af den dataansvarlige – enten ved specifik eller generel godkendelse jf. databeskyttelsesforordningens artikel 28, stk. 2.

Brud på persondatasikkerheden som skulle have været anmeldt

På baggrund af en klage fra en registreret udtalte Datatilsynet i 2020 kritik af, at en kommune ikke havde identificeret og anmeldt et brud på persondatasikkerheden jf. databeskyttelsesforordningens artikel 4, nr. 12 og 33. Endvidere havde kommunen ikke underrettet den registrerede jf. databeskyttelsesforordningens artikel 34, og efter en gennemgang af sagsforløbet blev det lagt til grund, at kommunen ikke havde haft de fornødne procedurer til verifikation af den rette modtager til e-post i sager, der omhandlede påtænkt opsigelse, hvilket var en overtrædelse af databeskyttelsesforordningens artikel 32.

Kommunen fik ved en fejl sendt en "sindet skrivelse" vedrørende opsigelse af en medarbejder til den pågældende medarbejders kollega. Skrivelsen indeholdt et udkast til opsigelsen og oplysninger om medarbejderens helbredsmæssige forhold og fagforeningsforhold.

Datatilsynet udtalte, at det normalt er korrekt, at risikoen for den registrerede er ubetydelig ved fejlagtig fremsendelse internt i en organisation, hvor de ansatte er underlagt tavshedspligt. Dette er dog ikke tilfældet i en sag som denne, hvor den pågældende medarbejders påtænkte opsigelse, på grund af de beskrevne helbredsmæssige forhold, blev sendt til en kollega. Bruddet skulle derfor have været anmeldt til Datatilsynet.

I det konkrete tilfælde vurderede Datatilsynet, at risikoen for den registreredes rettigheder ved det skete brud havde været høj, hvorfor kommunen skulle have foretaget underretning i medfør af databeskyttelsesforordningens artikel 34.

På baggrund af kommunens forklaring om, at der ikke var særlige organisatoriske forholdsregler for behandlingen af opsigelsessager, udtalte tilsynet, at det normalt ville være passende sikkerhed jf. databeskyttelsesforordningens artikel 32 at have sådanne foranstaltninger, da intern fejlsending i denne type sager kunne have betydelige konsekvenser for en registreret.

Generelt er de dataansvarlige rigtig gode til at anmelde de brud på persondatasikkerheden efter databeskyttelsesforordningens artikel 33. Vurderingen af risikoen for den registreredes rettigheder i forbindelse med et brud giver dog i visse filfælde – som i denne sag – anledning til fejlskøn.

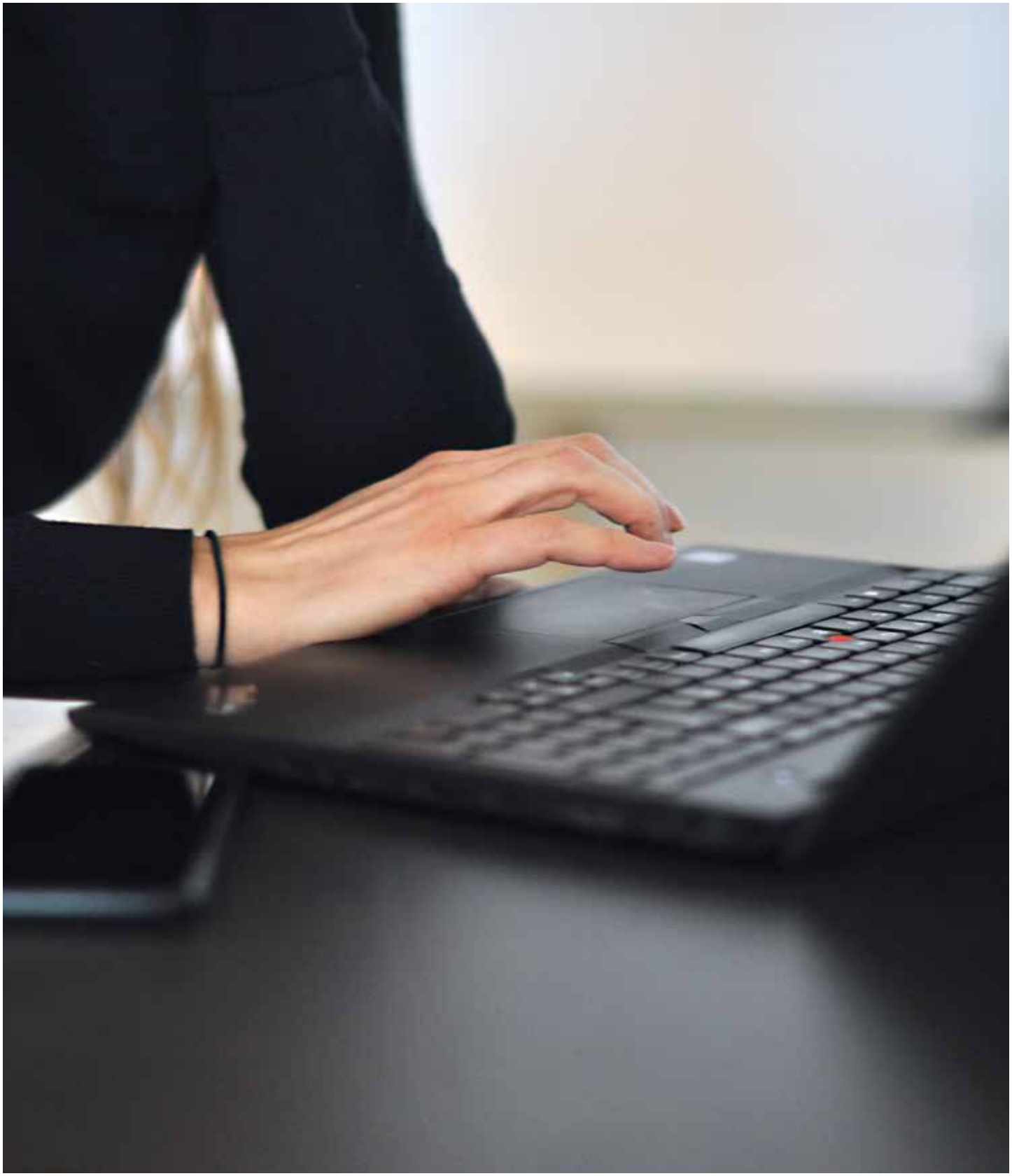
Brud på persondatasikkerheden i Zoologisk Have København (ZOO)

Datatilsynet udtalte i 2020 alvorlig kritik af, at det bl.a. var alt for let at få uretmæssig adgang til personoplysninger om årskortholderne hos Zoologisk Have i København.

Det viste sig, at det tekniske setup af loginsiden for årskortholdere gjorde det nemt for uvedkommende at få adgang til andres personoplysninger. Derudover var der unøjagtigheder i kommunikationen i forbindelse med bruddet på persondatasikkerheden.

ZOO fik påbud om at berigtige den ufyldestgørende information til alle registrerede og påbud om at informere de registrerede om bruddet i de tilfælde, hvor der var en høj risiko.

Datatilsynet fandt, at det havde været alt for nemt at opnå uautoriseret adgang til årskortholderes personoplysninger. Login for årskortholdere var en kombination af to numeriske værdier uden begrænsning i antallet af loginforsøg. ZOOs beskrivelse til Datatilsynet og kommunikationen med de registrerede af de foranstaltninger, ZOO traf for at håndtere bruddet, var ikke retvisende i forhold til, hvad ZOO reelt gjorde, og dette modsvarede ikke Datatilsynets opfattelse af risikoscenarierne.



ZOO havde ikke underrettet de registrerede (årskortholderne), for hvem der var en høj risiko, og den information, der i øvrigt blev givet helt generelt var ikke retvisende og angav ikke sandsynlige konsekvenser, risikoscenarier eller varigheden af bruddet. Derfor hjalp kommunikationen ikke de registrerede med at vurdere, hvilke forholdsregler de eventuelt skulle tage for at beskytte sig selv.

Passende sikkerhedsforanstaltninger trods brud på persondatasikkerheden i Salling

Datatilsynet har i 2020 truffet afgørelse i en sag, hvor en medarbejder hos Salling lukkede en tidligere ansat ind i et aflukket portnerlokale og viste den tidligere ansatte videoovervågningsmateriale fra forretningens område, hvor der fremgik billeder af den tidligere ansattes ekskæreste, som var ude at shoppe med en veninde.

Trods episoden fandt Datatilsynet, at Salling havde truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passede til de risici, der foreligger ved den pågældende behandling af personoplysninger, og at virksomheden ikke kunne anses for ansvarlig for den pågældende hændelse.

Ud over mange af de foranstaltninger Salling har truffet, lagde Datatilsynet vægt på, at en medarbejder bevidst og mod bedre vidende på flere måder – f.eks. ved at give en tidligere ansat adgang til bygningen – brød virksomhedens interne retningslinjer. Datatilsynet fandt endvidere, at medarbejderen foretog indtil flere handlinger, som lå udover, hvad der med rimelighed kunne forventes, at Salling skulle have været forberedt på eller skulle have truffet foranstaltninger med henblik på at undgå.

Datatilsynet endte derfor med kun at udtale kritik af, at anmeldelse af bruddet på persondatasikkerheden var sket for sent.

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).
- 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.

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 visse tilladelser er tilgængelige på hjemmesiden. Endvidere offentliggøres der på hjemmesiden løbende et udvalg af konkrete tilladelser og afslag på tilladelse.

Nedenfor omtales eksempler på afgørelser i tilladelsessager, som Datatilsynet har behandlet i 2020. Ud over sager inden for de ovenfor omtalte områder omtales også en tilladelse efter TV-overvågningslovens § 4 c, stk. 3, som er den første af sin art.

Tilladelse til behandling af personoplysninger efter databeskyttelseslovens § 7, stk. 4

Efter databeskyttelsesforordningens artikel 9, stk. 1, gælder et forbud mod behandling af særlige kategorier af personoplysninger, herunder helbredsoplysninger og oplysninger om race eller etnisk oprindelse. 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, kan forbuddet mod behandlingen af særlige kategorier af oplysninger under nærmere angivne omstændigheder fraviges, hvis behandlingen af oplysningerne er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret. Hjemmel til sådan behandling af oplysninger findes bl.a. i databeskyttelseslovens § 7, stk. 4. Hvis behandlingen ikke foretages for en offentlig myndighed, kan behandling efter denne bestemmelse kun ske med Datatilsynets tilladelse.

Ved hver anmodning om tilladelse vurderer Datatilsynet særligt, om behandlingen er nødvendig af hensyn til en væsentlig samfundsmæssig interesse, og om behandlingen af oplysningerne i stedet ville kunne ske på baggrund af et andet behandlingsgrundlag - eksempelvis samtykke.

Hvis Datatilsynet beslutter at meddele tilladelse, kan tilsynet fastsætte nærmere vilkår for behandlingen af oplysningerne jf. databeskyttelseslovens § 7, stk. 4, 3. pkt. Vilkårene kan variere fra sag til sag og kan eksempelvis omhandle, under hvilke omstændigheder oplysningerne kan videregives, og hvor længe oplysningerne kan opbevares. Vilkårene er supplerende og præciserende i forhold til databeskyttelsesforordningen og databeskyttelsesloven, og databeskyttelsesreglerne finder således anvendelse i det omfang, der er tale om forhold, der ikke er reguleret i vilkårene.

Datatilsynet behandler årligt omkring 10 anmodninger om tilladelse efter § 7, stk. 4.

Størstedelen af de tilladelser, Datatilsynet har meddelt efter denne bestemmelse, vedrører organisationer, som tilbyder rådgivning og støtte til udsatte grupper, og som f.eks. ikke har mulighed for at indhente samtykke fra de rådssøgende. Der kan eksempelvis være tale om mindreårige, som ikke selv kan

give samtykke, eller om at organisationens rådgivning har en sådan karakter, at et krav om samtykke kan forhindre, at personer henvender sig for at søge hjælp.

Ikke krav om tilladelse til kreditoplysningsbureauvirksomhed

Datatilsynet behandlede i 2020 en ansøgning fra virksomheden Managed Risk ApS om tilladelse til at drive virksomhed med behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse (kreditoplysningsbureau) i henhold til databeskyttelseslovens §§ 19 og 26, stk. 1, nr. 2.

Virksomheden havde oplyst, at den havde udviklet statistiske modeller, som – på grundlag af en flerhed af oplysninger – kunne udregne en score og et budget vedrørende såvel fysiske som juridiske personer.

Oplysningerne ville blive indhentet hos den registreredes selv og hos eksterne kilder, og ville blive behandlet på grundlag af den registreredes samtykke.

Efter at ansøgningen havde været forelagt Datarådet, udtalte Datatilsynet, at der ikke skulle indhentes tilladelse fra tilsynet til behandlingen, idet behandlingen skete på grundlag af den registreredes samtykke.

Baggrunden for dette var, at databeskyttelsesforordningen ikke giver medlemsstaterne, i dette tilfælde Danmark, mulighed for at stille krav om forudgående tilladelse fra tilsynsmyndigheden, når behandlingen udelukkende baserer sig på den registreredes samtykke.

Uanset at Datatilsynets forudgående tilladelse ikke skulle indhentes, påpegede tilsynet, at databeskyttelsesreglerne skulle overholdes, i hvilken forbindelse tilsynet særligt henledte virksomhedens opmærksomhed på de grundlæggende principper for behandling af personoplysninger i databeskyttelsesforordningens artikel 5, de registreredes rettigheder og reglerne om behandlingssikkerhed.

Tilladelse til førelse af retsinformationssystem

Datatilsynet behandlede i 2020 en sag, hvor J.H. Schultz Information A/S anmodede tilsynet om tilladelse til førelse af et retsinformationssystem. J.H. Schultz Information A/S ønskede at udvikle et nyt juridisk informationssystem, der bl.a. skulle indeholde en database over domme og afgørelser, som skulle stilles til rådighed for medlemsvirksomheder af Danske Advokater, offentlige myndigheder og juridiske funktioner hos Danmarks største virksomheder.

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.

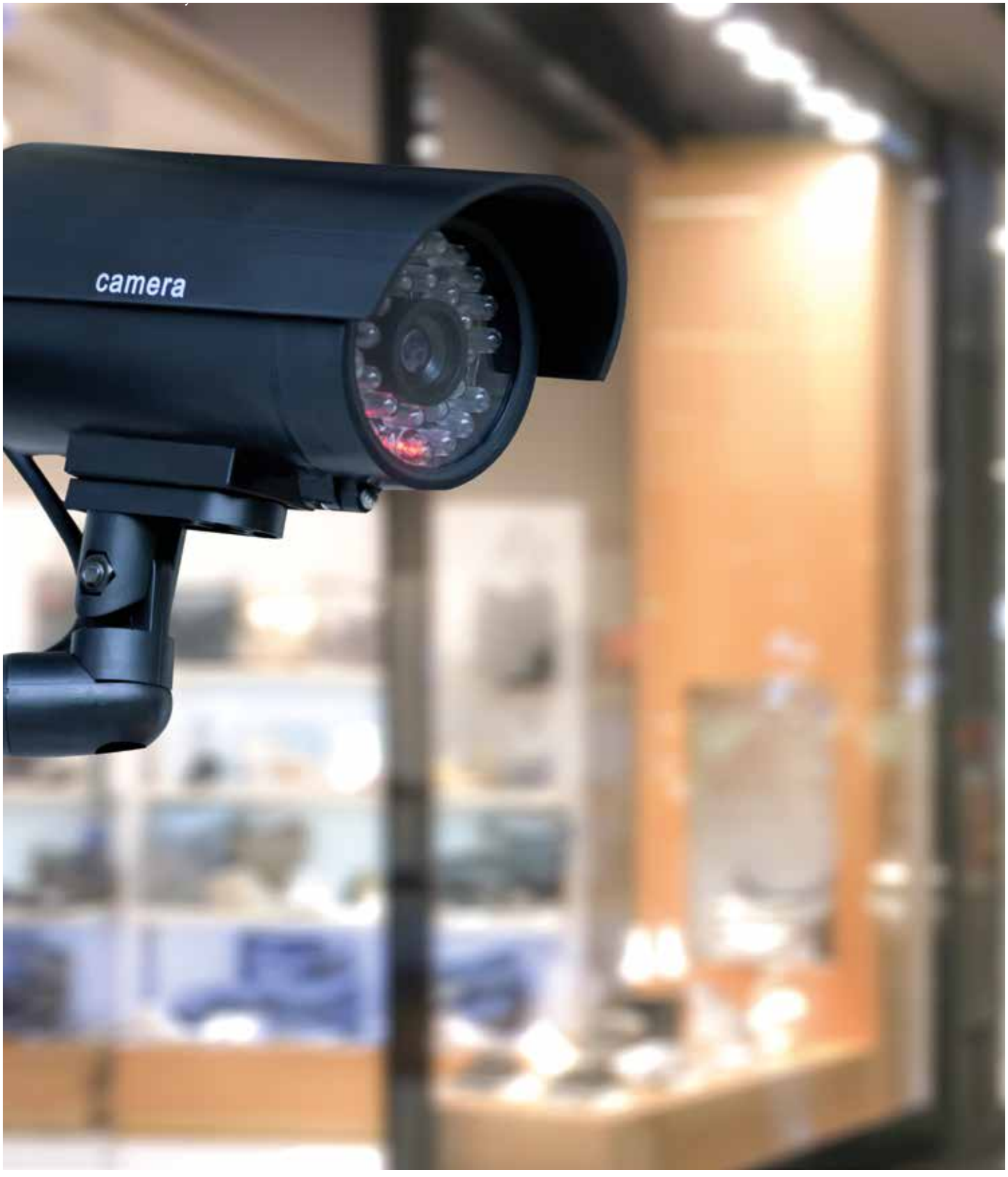
Hvis personoplysninger behandles efter lovens § 9, stk. 1, må disse oplysninger ikke senere behandles i andet øjemed. Det samme gælder behandling af andre personoplysninger, hvis behandlingen alene foretages med henblik på at føre retsinformationssystemer.

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 behandlingen.

Datatilsynet vurderede, at betingelserne var opfyldt, og gav tilladelse til J.H. Schultz Information A/S' behandling af personoplysninger i forbindelse med førelse af et retsinformationssystem. Tilladelsen blev givet på en række vilkår udarbejdet i overensstemmelse med de generelle vilkår for retsinformationssystemer, som er offentliggjort på Datatilsynets hjemmeside.

Vilkårene er supplerende i forhold til reglerne i databeskyttelsesforordningen og databeskyttelsesloven, og i et vist omfang er de udtryk for en præcisering af disse 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.


camera

Tilladelse efter TV-overvågningslovens § 4 c, stk. 3

TV-overvågningsloven blev i 2018 ændret således, at der blev indført en adgang for erhvervsdrivende til at videregive billed- og lydoptagelser, der er optaget i forbindelse med tv-overvågning, internt i organisationen eller til andre erhvervsdrivende i kriminalitetsforebyggende øjemed, hvis en række nærmere betingelser er opfyldt, herunder at videregivelsen sker i et lukket system, jf. lovens § 4 c, stk. 2. Datatilsynets tilladelse skal indhentes, inden videregivelse iværksættes, jf. § 4 c, stk. 3. Datatilsynet kan fastsætte vilkår for tilladelsen.

Formålet med at udvide adgangen til at videregive billed- og lydoptagelser fra tv-overvågning i kriminalitetsforebyggende øjemed er, at erhvervsdrivende skal have mulighed for at advare hinanden om f.eks. omrejsende kriminelle.

Datatilsynet modtog i juli 2019 en ansøgning fra Dansk Erhverv om tilladelse til at videregive billed- og lydoptagelser. Videregivelsen skulle finde sted i systemet "Crimestat", som er udviklet af Dansk Erhverv i samarbejde med detailhandlen.

Datatilsynet gav i februar 2020 Dansk Erhverv tilladelse til at videregive billed- og lydoptagelser i det omhandlede system. Tilladelsen indeholder en række vilkår for systemet og for videregivelsen af oplysninger. Det er den første tilladelse, Datatilsynet har givet i medfør af TV-overvågningslovens § 4 c, stk. 3.

Tilladelsen er offentliggjort på tilsynets hjemmeside.

Internationalt arbejde

Med databeskyttelsesforordningen har det internationale samarbejde fået en ny og større betydning.

Databeskyttelsesområdet er via forordningen i langt højere omfang reguleret på EU-niveau, ligesom der med forordningen er etableret et mere formaliseret samarbejde mellem tilsynsmyndighederne i Europa.

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 en pragmatisk tilgang, der tager hensyn til de registrerede såvel 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. Datatilsynet har på den baggrund udarbejdet en strategi for det internationale arbejde, som skal være med til at sikre dette, ligesom strategien skal sikre, at tilsynet kan deltage aktivt og kvalificeret såvel på arbejdsgruppeniveau som på møder i Det Europæiske Databeskyttelsesråd (EDPB) og på den måde få gjort danske synspunkter gældende i rette tid og på rette sted.

Datatilsynet deltager i alle arbejdsgrupper under EDPB, ligesom tilsynet aktivt involverer sig i arbejdet med udarbejdelse af vejledninger mv., både som ledende skribent på udvalgte dokumenter og som medforfatter på andre.

Herudover deltager Datatilsynet i det øvrige internationale samarbejde på databeskyttelsesområdet, herunder Global Privacy Assembly, Europarådet og det nordiske samarbejde.

I 2020 har det internationale samarbejde i høj grad været præget af Covid-19 pandemien. Det gælder både praktisk i form af fysiske møder, som enten er blevet afholdt online eller er blevet udskudt, og indholdsmæssigt i form af databeskyttelsesretlige spørgsmål, som håndteringen af udbruddet har givet anledning til.

Derudover har der i EDPB-regi navnlig været fokus på at klarlægge konsekvenserne af Brexit for databeskyttelsesområdet og konsekvenserne af EU-Domstolens dom i den såkaldte Schrems II-sag om overførsel af personoplysninger til tredjelande.

Det Europæiske Databeskyttelsesråd

Det Europæiske Databeskyttelsesråd (EDPB) er et uafhængigt EU-organ, som skal sikre en ensartet anvendelse af databeskyttelsesforordningen og retshåndhævelsesdirektivet i hele EU.

EDPB består af repræsentanter for medlemsstaternes tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). EØS-landene og EU-Kommissionen deltager også i EDPB-møder, men har ikke stemmeret. Danmark er repræsenteret ved Datatilsynets direktør.

Med henblik på at sikre en ensartet anvendelse af databeskyttelsesreglerne kan EDPB 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.
- Afgive 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 medlemsstaternes tilsynsmyndigheder, og som har grænseoverskridende virkninger.
- Træffe bindende afgørelser om fortolkningen af databeskyttelsesreglerne, 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.

EDPB har sin egen forretningsorden, som indeholder regler om bl.a. organisering, samarbejdet mellem medlemmer og arbejdsmetoder. Hvor afstemning er nødvendig, træffer EDPB som udgangspunkt afgørelse med simpelt flertal blandt sine medlemmer.

EDPB bistås af et sekretariat, som udfører sine opgaver efter instruks fra formanden. Sekretariatet er placeret i Bruxelles, hvor rådets fysiske møder også afholdes.

EDPB holder normalt møder af to dages varighed en gang om måneden. Som følge af Covid-19 er dette udgangspunkt dog blevet fraveget markant i 2020. For det første har det siden udbruddet ikke være muligt at mødes fysisk, hvorfor møderne har været afholdt online. For det andet har det – bl.a. for at adressere forskellige spørgsmål vedrørende håndteringen af Covid-19 – været nødvendigt at mødes med kortere intervaller, hvilket har medført, at der i 2020 blev afholdt i alt 27 møder.

Arbejdet med forberedelsen af vejledninger, udtalelser, afgørelser mv., som EDPB skal godkende, forestås primært af 12 ekspertarbejdsgrupper, som normalt mødes med 1-2 måneders intervaller i Bruxelles. Ligesom EDPB-møderne er arbejdsgruppemøderne i 2020 siden Covid-19-udbruddet blevet afholdt online og med kortere intervaller.

- EDPB's egen hjemmeside: www.edpb.europa.eu
- Twitter-profil: @EU_EDPB
- LinkedIn-profil: European Data Protection Board.

På kanalerne er det muligt at følge med i rådets arbejde, ligesom der på Datatilsynets hjemmeside og LinkedIn-profil løbende bliver offentliggjort vejledninger, nyheder, events mv. fra EDPB. Indholdet findes på undersiden "Internationalt".

I 2020 vedtog EDPB en række vejledninger mv. om aktuelle databeskyttelsesretlige emner. Bl.a. gav Covid-19-udbruddet anledning til at udstede retningslinjer om behandling af helbredsoplysninger med henblik på videnskabelig forskning og om brug af lokaliseringsdata og kontaktopsporingsredskaber.

Derudover havde EDPB fokus på at vejlede om de praktiske konsekvenser af EU-Domstolens dom i den såkaldte Schrems II-sag om overførsel af personoplysninger til tredjelande.

EDPB havde endvidere fokus på at klarlægge konsekvenserne af Brexit for databeskyttelsesområdet, herunder for den fremtidige overførsel af personoplysninger til Storbritannien.

Endelig traf EDPB den første bindende afgørelse i en sag om grænseoverskridende behandling af personoplysninger omfattet af den særlige tvistbilæggelsesprocedure i databeskyttelsesforordningen.

EU-Kommissionens evaluering

EU-Kommissionen er i medfør af databeskyttelsesforordningens artikel 97 forpligtet til hvert fjerde år at gennemgøre en evaluering af anvendelsen af forordningen. EU-Kommissionen havde på den baggrund bl.a. anmodet Det Europæiske Databeskyttelsesråd (EDPB) om en udtalelse til brug for den første evaluering.

EDPB konstaterede i udtalelsen, at anvendelsen af forordningen i de første 20 måneder overordnet set har været en succes, selvom behovet for tilstrækkelige ressourcer fortsat er en udfordring i mange medlemsstater, ligesom også forskelle i nationale sagsbehandlingsprocedurer giver udfordringer.

Databeskyttelsesrådets udtalelse er tilgængelig på rådets hjemmeside.

Endvidere har justitsministeren i 2020 taget initiativ til en national evaluering af databeskyttelsesreglerne på nationalt plan. Evalueringen forventes færdig i første halvår 2021.

Nyt afgørelsesregister for one-stop-shop-sager

For at sikre øget transparens omkring tilsynsmyndighedernes samarbejde i sager om grænseoverskridende behandlinger, oprettede Det Europæiske Databeskyttelsesråd (EDPB) i 2020 et register over afgørelser behandlet efter den såkaldte one-stop-shop procedure i databeskyttelsesforordningens artikel 60.

One-stop-shop proceduren anvendes i sager om grænseoverskridende behandling af personoplysninger for at undgå, at tilsynsmyndighederne i flere medlemsstater behandler den samme sag. Der udpeges i stedet en ledende tilsynsmyndighed med ansvaret for sagens behandling og koordinationen med de berørte tilsynsmyndigheder. Når der træffes afgørelse i sagen, har samtlige berørte tilsyn således været inddraget.

Af en officiel oversigt, der løbende opdateres, fremgår bl.a. selve afgørelsen, hvilke bestemmelser sagen vedrørte, et kort resumé, samt hvem der var henholdsvis ledende og berørte tilsynsmyndigheder.

Oversigten er tilgængelig på EDPB's hjemmeside.

Første afgørelse om tvistbilæggelse

I november 2020 vedtog Det Europæiske Databeskyttelsesråd (EPDB) sin første bindende afgørelse efter reglerne i databeskyttelsesforordningen om tvistbilæggelse.

I sager om grænseoverskridende behandling af personoplysninger skal der i overensstemmelse med den såkaldte one-stop-shop procedure i databeskyttelsesforordningen identificeres en ledende tilsynsmyndighed, der står for sagsbehandlingen, herunder at træffe afgørelse i sagen. Herudover skal de tilsynsmyndigheder, der er berørte af sagen, give sig til kende. Når den ledende tilsynsmyndighed har udarbejdet et udkast til afgørelse, skal det forelægges de berørte medlemsstater, som har mulighed for at fremkomme med relevante og begrundede indsigelser. Hvis ikke den ledende tilsynsmyndighed er enig i indsigelserne, og tilsynsmyndigheden ikke ønsker at følge disse, skal sagen forelægges til tvistbilæggelse for EDPB, som træffer en bindende afgørelse vedrørende de pågældende indsigelser.

Det var den situation, som det irske datatilsyn befandt sig i, da tilsynet i en grænseoverskridende sag havde modtaget en række indsigelser til sit udkast til afgørelse fra de berørte tilsynsmyndigheder. Der var tale om en egen driftsag, som det irske datatilsyn havde taget op på baggrund af en anmeldelse af et sikkerhedsbrud fra Twitter International Company, som er etableret i Irland.

I sin afgørelse afviste EDPB de fleste indsigelser som værende ikke tilstrækkeligt begrundede, idet de ikke opfyldte kravet om at påvise en klar risiko for de registreredes rettigheder, hvis ikke indsigelserne blev fulgt. En række indsigelser blev endvidere afvist, idet EDPB ikke fandt tilstrækkeligt faktuelt grundlag i sagen til at kunne følge indsigelserne. Endelig fandt EDPB, at den foreslåede bødestørrelse ikke var tilstrækkeligt begrundet, og den irske tilsynsmyndighed skulle derfor revurdere udregningen af bødestørrelsen, således at denne svarede til overtrædelsen og havde en afskrækkende effekt.

Efter EDPB vedtog den bindende afgørelse, blev denne meddelt til det irske datatilsyn, som fik en frist på en måned til at træffe endelig afgørelse i sagen i overensstemmelse med EDPB's afgørelse. Det irske datatilsyn traf herefter endelig afgørelse i sagen den 9. december 2020.

Schrems II-sagen

I juli 2020 afsagde EU-Domstolen dom i den såkaldte Schrems II-sag, som vedrørte retsgrundlaget for overførsel af personoplysninger til USA.

EU-Domstolen erklærede den såkaldte Privacy Shield-ordning, som var et særligt retsgrundlag for overførsel personoplysninger til USA, for ugyldig, da ordningen ikke fandtes at sikre et tilstrækkeligt beskyttelsesniveau for de overførte personoplysninger i USA.

Der var i sagen også rejst spørgsmål om gyldigheden af EU-Kommissionens standardkontrakter, som er et generelt retsgrundlag for overførsel af personoplysninger til lande uden for EU/EØS (såkaldte tredjelande). EU-Domstolen fastslog, at standardkontrakterne fortsat er gyldige, men at der efter omstændighederne kan være behov for at iværksætte supplerende foranstaltninger, hvis beskyttelsesniveauet i tredjelandet ikke er tilstrækkeligt.

På denne baggrund iværksatte Datatilsynet sammen med de andre europæiske tilsynsmyndigheder i regi af Det Europæiske Databeskyttelsesråd (EDPB) en nærmere analyse af dommen og dens praktiske konsekvenser.

EDPB nedsatte i den forbindelse en task force, som fik til opgave at beskrive, hvilke krav der på baggrund af dommen skal stilles til beskyttelsesniveauet i tredjelande, som man ønsker at overføre personoplysninger til. Datatilsynet deltog i task forcens arbejde, som resulterede i, at EDPB i november 2020 vedtog en række anbefalinger herom. Task forcen tog i sit arbejde udgangspunkt i den tidligere Artikel 29-gruppes vejledning om de fire væsentlige europæiske garantier, som i sin tid blev udarbejdet på baggrund af Schrems I-afgørelsen.

EDPB nedsatte sideløbende hermed en anden task force, som fik til opgave at udarbejde anbefalinger om, hvordan behovet for iværksættelse af supplerende foranstaltninger – når beskyttelsesniveauet i tredjelandet ikke er tilstrækkeligt – kan imødekommes i praksis. Datatilsynet har deltaget i task forcens arbejde, som foreløbig har resulteret i et udkast til anbefalinger, som har været sendt i offentlig høring og forventes vedtaget i løbet af første halvår 2021.

Ud over de nævnte anbefalinger fra EDPB har Datatilsynet også selv udarbejdet en Q&A om dommen og dens konsekvenser.

Brexit

Storbritannien forlod EU den 31. januar 2021, hvilket indebærer, at Storbritannien ikke længere er omfattet af EU's regler.

Storbritannien vil derfor fremover være at betragte som et tredjeland, hvilket som udgangspunkt indebærer, at overførsel af personoplysninger til Storbritannien kræver, at der tilvejebringes et såkaldt overførselsgrundlag. Det fremgår imidlertid af den aftale, Storbritannien og EU har indgået om deres fremtidige forhold, at overførsler fra EU- og EØS-lande til Storbritannien kan fortsætte uændret i fire måneder – med mulighed for forlængelse med yderligere 2 måneder – regnet fra den 1. januar 2021. I denne periode kan der således fortsat overføres personoplysninger til Storbritannien uden tilvejebringelse af et overførselsgrundlag.

Storbritannien er endvidere ikke længere omfattet af den såkaldte one-stop-shop procedure, som er fastsat i databeskyttelsesforordningen for sager om grænseoverskridende behandling af personoplysninger. Datatilsynet har på den baggrund været i dialog med det britiske datatilsyn om håndteringen af konkrete grænseoverskridende sager, som allerede var påbegyndt, inden Storbritannien forlod EU.

Særlige internationale tilsynsforpligtelser

Schengeninformationssystemet (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.

Toldinformationssystemet (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.

Visuminformationssystemet (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 derudover 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 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 Markedsinformationssystemet (IMI)

Indre Markedsinformationssystemet 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 Markedsinformationssystemet (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.

Europarådet

Europarådet danner 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 2020 deltog Datatilsynet i Europarådets konvention 108-komitémøde. På mødet drøftedes en række aktuelle emner, herunder databeskyttelse i forbindelse med undervisning, digital identitet og tillægsprotokollen til Budapest-konventionen om IT-kriminalitet.

Berlin-gruppen

Den såkaldte "Berlin-gruppe", der har skiftet navn til "International Working Group on Data Protection in Technology", 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 "Working Papers", som er tilgængelige på gruppens hjemmeside.

Gruppen har i 2020 måtte aflyse alle sine fysiske møder. I årets løb har gruppen dog fortsat arbejdet på et skriftligt grundlag med aktuelle emner, som indeholder problemstillinger i relation til databeskyttelse og beskyttelse af privatliv, eksempelvis Covid-19 og databeskyttelse, 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 op mærksomhed 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.

I tillæg hertil afholder tilsynene en gang om året et nordisk samarbejdsmøde med deltagelse af såvel ledelse som sagsbehandlere og IT-eksperter samt et mindre opfølgningsmøde senere på året. Det nordiske samarbejdsmøde – der i 2020 skulle have været afholdt i Finland - blev imidlertid udskudt til 2021 som følge af Covid-19.

Den europæiske konference

Den Europæiske Konference for datatilsynsmyndigheder - også kaldet Forårskonferencen - afholdes én gang årligt. Konferencen, som i 2020 skulle have været afholdt i Kroatien, blev udskudt til 2021 som følge af Covid-19.

Global Privacy Assembly

Global Privacy Assembly (GPA) er et globalt forum, som har til formål at fremme samarbejdet mellem nationale databeskyttelsesmyndigheder.

GPA mødes årligt til en konference, hvor der vedtages resolutioner mv. om aktuelle emner. Resolutionerne forberedes inden konferencen i en række arbejdsgrupper, hvoraf Datatilsynet bl.a. deltager i den såkaldte Berlin-gruppe. Konferencen består af en lukket del forbeholdt de tilsynsmyndigheder, som er medlem af GPA og en åben del, der er tilgængelig for alle.

Konferencen skulle i 2020 skulle have været afholdt i Mexico, men blev på grund af Covid-19 afholdt online.

Datatilsynet deltog i konferencen, hvor GPA vedtog en række resolutioner om bl.a. håndteringen af Covid-19, kunstig intelligens og ansigtsgenkendelse. Der blev endvidere vedtaget en resolution, som skal give GPA mulighed for at spille en mere aktiv rolle i forhold til at skabe global opmærksomhed om databeskyttelsesretlige spørgsmål.

.

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 fore tages af færøske myndigheder og af private virksomheder, organisationer mv. gælder den færøske per sondatalov. Tilsynsmyndighed i forhold til denne lov er det færøske datatilsyn Dátueftirlitið.

Datatilsynet har i 2020 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 imidlertid i 2020 omkring 30 anmeldelser om behandling af personoplysninger fra grønlandske myndigheder og 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.

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 retshåndhævelsesloven 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 2020 har Datatilsynet bl.a. behandlet klagesager og anmeldelser fra de retshåndhævende myndigheder om brud på persondatasikkerheden.

Klagesag om bevisførelse i retten

Datatilsynet traf i 2020 afgørelse i en sag, hvor anklagemyndigheden i forbindelse med behandlingen af en retssag vedrørende et drabsforsøg - som led i bevisførelsen og under afhøringen af et vidne - afspillede et alarmopkald, hvor vidnet oplyste sit personnummer. Vidnet klagede efterfølgende til Datatilsynet over, at de tilstedeværende ved retsmødet blev bekendt med hendes personnummer.

Københavns Vestegns Politi oplyste i sagen, at anklagemyndigheden altid foretager en konkret vurdering af, hvilke beviser der er nødvendige for at løfte den samlede bevisbyrde, og at anklagemyndigheden derfor kun afspiller alarmopkald indeholdende personoplysninger, hvis dette skønnes nødvendigt for at sikre sagens oplysning for retten. Københavns Vestegens Politi oplyste desuden, at formålet med afspilning af et alarmopkald er, at retten skal danne sig et indtryk af, hvordan stemningen er på anmeldelsestidspunktet, herunder baggrundslyde fra gerningsmanden eller ofret, anmelderens stemmeføring og andre omstændigheder, der kan give retten et indtryk af sagens karakter.

Københavns Vestegns Politi bemærkede, at man i overensstemmelse med princippet om "bevisumiddelbarhed" (beviser skal fremføres umiddelbart for retten således, at retten kan danne sig et fuldstændigt indtryk af bevisets værdi og bevisets betydning for sagen), kan undlade at censurere alarmopkald – uanset om dette måtte være af hensyn til personoplysninger - fordi formålet med afspilningen kan gå tabt, idet retten ikke vil have mulighed for at høre alarmopkaldet uafbrudt og i sin helhed.

I den konkrete sag var det anklagemyndighedens vurdering, at klagers vidneforklaring understøttede, at der kunne være informationer på alarmopkaldet i form af baggrundslyde mv., som kunne have betydning for domstolens vurdering af sagen. I sammenhæng med sagens øvrige omstændigheder, herunder sagens karakter, og at vidnet ikke havde nogen direkte relation med tiltalte, var det derfor den anklagerfaglige vurdering, at afspilning af alarmopkaldet var nødvendig for at løfte den samlede bevisbyrde.

Datatilsynet fandt, at Københavns Vestegns Politis behandling af personoplysninger var sket i overensstemmelse med reglerne i retshåndhævelseslovens § 9 og § 4, stk. 3, og at der ikke var grundlag for at tilsidesætte Københavns Vestegns Politis vurdering af, at afspilningen af alarmopkaldet var nødvendig for at retsforfølge den pågældende strafbare handling.

Ved vurderingen lagde Datatilsynet vægt på, at det er anklagemyndighedens opgave at afgøre, hvilke beviser der skal føres for retten, og at anklagemyndigheden ved tilrettelæggelse af bevisførelsen skal sørge for, at alle beviser, der belyser den begåede kriminalitet, bliver ført for retten.

Datatilsynet lagde endvidere vægt på, at klagers vidneforklaring understøttede, at der kunne være informationer på alarmopkaldet i form af baggrundslyde mv., der kunne være af betydning for domstolens vurdering af sagen, og at Københavns Vestegns Politis afspilning af alarmopkaldet – på baggrund af oplysningens karakter sammenholdt med sagens alvor og princippet om bevisumiddelbarhed – var proportionel.

Datatilsynet bemærkede afslutningsvist, at endelig afgørelse om dørlukning tilkommer domstolene.

Kriminalforsorgens håndtering af anmodning om indsigt

Datatilsynet behandlede i 2020 en klagesag vedrørende Kriminalforsorgens håndtering af en fængselsbetjents anmodning om indsigt.

Fængselsbetjenten havde anmodet Kriminalforsorgen om indsigt i dokumenter, der kunne bekræfte, at han (som led i sin ansættelse) havde deltaget i voldsomme episoder, herunder rapporter om magtanvendelse, observationscelleanbringelser, sikringscelleanbringelser samt rapporter om trusler og eventuelle rapporter om selvmordsforsøg eller andre voldsomme selvbeskadigelser.

Til en start gav Kriminalforsorgen fængselsbetjenten et afslag på hans anmodning om indsigt med den begrundelse, at det af tekniske årsager ikke var muligt at fremsøge alle de episoder, som han havde deltaget i, og at det alene var muligt at fremsøge rapporter, som fængselsbetjenten selv havde skrevet. Fængselsbetjenten klagede herefter over Kriminalforsorgens afslag på indsigt til Datatilsynet.

Efter anmodning fra Datatilsynet oplyste Kriminalforsorgen, at det med systemleverandørens bistand alligevel var muligt at foretage en søgning efter specifikke rapporter, hvori fængselsbetjentens navn måtte være registreret, og at Kriminalforsorgen således havde meddelt fængselsbetjenten indsigt heri.

Kriminalforsorgen oplyste dog samtidig, at det ikke var muligt at foretage søgninger i rapporters fritekstfelter i det pågældende system med henblik på at afklare, om fængselsbetjentens navn måtte fremgå deri, da dette ville forudsætte en søgning i 8-10 mio. dokumenter i systemets dokumentserver, hvilket ikke kunne understøttes teknisk i systemet.

Efter en gennemgang af sagen - og efter at sagen havde været forelagt Datarådet - udtalte Datatilsynet kritik af, at Kriminalforsorgen ikke have givet klager indsigt i overensstemmelse med retshåndhævelseslovens § 15, da Kriminalforsorgen først meddelte indsigt efter tilsynets henvendelse vedrørende sagen.

For så vidt angår den del af klagen, som vedrørte indsigt i eventuelle oplysninger i fritekstfelter, og som ville forudsætte en søgning i 8-10 mio. dokumenter i systemets dokumentserver, fandt Datatilsynet, at anmodningen ville kunne afvises under henvisning til retshåndhævelseslovens § 19.

Tilsynet forudsatte i den forbindelse, at fritekstfelterne overvejende alene beskrev en funktion, som fængselsbetjenten havde varetaget på arbejdspladsen og ikke handlinger, som er udtryk for hans personlige valg og reaktioner, eller handlinger, som han var blevet udsat for.

Datatilsynet lagde endvidere vægt på, at Kriminalforsorgen allerede havde udfoldet betydelige bestræbelser på at fremfinde oplysninger om fængselsbetjenten, og at Kriminalforsorgen måtte antages at skulle anvende ikke ubetydelige ressourcer på at fremfinde eventuelle yderligere oplysninger om ham. Tilsynet lagde i tilknytning hertil også vægt på, at fængselsbetjenten ikke havde kunnet præcisere sin anmodning med henblik på at identificere yderligere oplysninger om ham.

Sagen var den første sag, hvor Datatilsynet traf afgørelse vedrørende retshåndhævelseslovens § 19 (tilsvarende bestemmelsen i databeskyttelsesforordningens artikel 12, stk. 5).

Anmeldelse af brud på persondatasikkerheden hos Københavns Politi

I september 2020 traf Datatilsynet afgørelse i en sag, hvor Rigspolitiets Center for Databeskyttelse havde anmeldt et brud på persondatasikkerheden hos Københavns Politi.

Sikkerhedsbruddet bestod i, at en borger havde kontaktet en medarbejder i Servicecenteret ved Københavns Politi og udgivet sig for at være ansat i Københavns Politis færdselsafdeling. Borgeren havde anmodet medarbejderen om at slå registreringsnummeret op på en bil, som han efter sigende skulle

have standset. Medarbejderen slog registreringsnummeret op i politiets system og videregav oplysninger om navn og adresse på ejeren af bilen, som var registreret med adressebeskyttelse. Sidst i samtalen anmodede medarbejderen borgeren om at oplyse sin medarbejderidentifikation, hvorefter borgeren lagde røret på. Efter opkaldet underrettede medarbejderen straks vagthavende om fejlen.

Københavns Politi oplyste i sagen, at før servicemedarbejdere må videregive oplysninger til ansatte i politiet, skal de spørge til den pågældendes navn og medarbejderidentifikation og kontrollere oplysningerne. Medarbejderen, der videregav oplysningerne, var bekendt med proceduren omkring udlevering af oplysninger, og det var en fejl, at vedkommende først spurgte ind til medarbejderidentifikation, efter at oplysningerne var videregivet.

Københavns Politi underrettede den registrerede om bruddet på persondatasikkerheden 8 dage efter hændelsen. Det var imidlertid ikke muligt for politikredsen at genskaffe den konkrete underretning til Datatilsynet.

Dagen efter underretningen kontaktede den registrerede Rigspolitiets Center for Databeskyttelse med en række spørgsmål til underretningen, som Rigspolitiet videresendte til Københavns Politi sammen med vejledning i, hvordan spørgsmålene skulle besvares.

Efter en gennemgang af sagen fandt Datatilsynet, at Københavns Politi ved at have videregivet oplysninger om en adressebeskyttet borgers navn og adresse til uvedkommende ikke havde levet op til kravene om et passende sikkerhedsniveau i retshåndhævelseslovens § 27, stk. 1. Ved vurderingen heraf lagde Datatilsynet vægt på, at sikkerhedsproceduren vedrørende servicemedarbejderes udlevering af personoplysninger ved opkald til Servicecenteret ikke havde været tilstrækkelig, idet proceduren havde været forbundet med en betydelig risiko for menneskelige fejl og forglemmelser hos medarbejderne. Datatilsynet lagde endvidere vægt på, at det ikke er usandsynligt, at en borger kan være i besiddelse af en politibetjents navn og medarbejderidentifikation, hvorved sikkerhedsproceduren selv uden medarbejderfejl, ikke havde medført et passende sikkerhedsniveau.

Datatilsynet fandt endvidere, at Københavns 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 bekendt med bruddet, jf. retshåndhævelseslovens § 28, stk. 1, og at Københavns Politi ikke havde underrettet den berørte registrerede uden unødig forsinkelse jf. retshåndhævelseslovens § 29, stk. 1.

I forhold til tidspunktet for underretningen lagde Datatilsynet vægt på, at Københavns Politi senest på det tidspunkt, hvor politikredsen konstaterede hændelsen, og hvor det måtte antages, at politikredsen var bekendt med, at bruddet indebar en høj risiko for den registrerede, burde have foretaget underretningen.

I tilknytning hertil bemærkede Datatilsynet, at en underretning efter retshåndhævelseslovens § 29 skal give den registrerede mulighed for at træffe de fornødne forholdsregler med henblik på at beskytte sig selv. På baggrund heraf indskærpede Datatilsynet over for Københavns Politi, at politikredsen orienterede medarbejderne om reglen i § 29, stk. 1, og fremadrettet sikrede, at de interne arbejdsgange i kredsen understøtter, at underretning af de registrerede sker uden unødig forsinkelse.

Endelig fandt Datatilsynet det tvivlsomt, at indholdet af underretningen til den registrerede om bruddet på persondatasikkerheden efterlevede retshåndhævelseslovens § 29, stk. 2, og tilsynet understregede vigtigheden i, at underretninger indeholder de oplysninger, som er påkrævet efter § 29, stk. 2.

Datatilsynet noterede sig i øvrigt, at Københavns Politi overvejede at ændre forholdsordren, således at medarbejdere i Servicecenteret ikke længere må videregive oplysninger til politiansatte, men at de i stedet henvises til andre kanaler. Datatilsynet noterede sig endvidere, at Servicecenteret hos Køben-

havns Politi – som følge af hændelsen – iværksatte en række initiativer, som skulle gøre medarbejderne i Servicecenteret opmærksomme på, hvordan de skal håndtere videregivelse af personoplysninger.

Samlet set fandt Datatilsynet, at der var grundlag for at udtale alvorlig kritik af, at Københavns Politis behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i retshåndhævelseslovens § 27, stk. 1, § 28, stk. 1, og § 29, stk. 1.

Alvorlig kritik af Kriminalforsorgens behandling af personoplysninger

Datatilsynet udtalte i august 2020 alvorlig kritik af en af Kriminalforsorgens behandlinger af personoplysninger, der ikke var sket i overensstemmelse med reglerne i retshåndhævelseslovens § 27, stk. 1.

Kriminalforsorgen havde siden 2010 stillet IT-udstyr – Det Sikrede Klientnetværk – til rådighed for indsatte, ansatte og undervisere til brug på Kriminalforsorgens institutioner. IT-udstyret var sikret med brugerprofiler, der indeholdt navn og i visse tilfælde også telefonnumre på indsatte, ansatte og undervisere. Kriminalforsorgen blev af en indsat gjort opmærksom på, at det var muligt – ved manipulation af URL-adressen, hvori der indgik fortløbende numre – at tilgå andre brugeres profiler og dermed få adgang til deres navn og evt. telefonnummer. Der kunne potentielt tilgås oplysninger om op mod 6.500 personer.

IT-udstyret var teknisk sikret mod enhver form for dataudtræk, og det var ikke muligt at foretage installation af programmer eller på anden måde ændre udstyrets opsætning, ligesom det ikke var muligt at koble eksterne enheder til udstyret. Systemet havde således ikke givet Kriminalforsorgen anledning til bekymring omkring sikkerheden.

Det Sikrede Klientnetværk, der var baseret på Microsoft Sharepoint, blev etableret i 2010, og der blev i den forbindelse ikke etableret korrekt adgangsstyring. Sårbarheden var således tilstede, før retshåndhævelsesloven fandt anvendelse.

Da Kriminalforsorgen blev gjort opmærksom på, at der let kunne findes oplysninger om personale på det sikrede netværk, blev systemet lukket ned.

Datatilsynet udtalte, at der påhviler den dataansvarlige en pligt til at identificere de risici, behandlingen udgør for de registrerede og til at sikre, at der indføres passende sikkerhedsforanstaltninger, der beskytter de registrerede mod disse risici. Det er Datatilsynets opfattelse, at systemer, hvori der gives adgang til personoplysninger via en URL, skal indrettes sådan, at det ikke ved simpel manipulation eller benyttelse af en let gennemskuelig sammenhæng, kan udledes en URL, der giver adgang til oplysninger om andre registrerede. Jo større risikoen er ved behandlingen af de registreredes oplysninger, des mere bør systemet sikres mod uautoriseret adgang og ikke kun via URL'en alene. Det bør kombineres med en anden form for adgangsstyring, f.eks. ved en individuelt udstedt token eller anden yderligere legitimationsoplysning. Et system som det beskrevne, der giver uberettiget adgang til andres personoplysninger ved blot at ændre i systemets URL, lever ikke op til kravet om passende sikkerhed, jf. retshåndhævelsesloven § 27, stk. 1.

Datatilsynet fandt, at det for en straffuldbyrdende myndighed er særligt relevant, at der er etableret procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Datatilsynet lagde særligt vægt på, at Kriminalforsorgen behandler store mængder personoplysninger om mange registrerede (indsatte, ansatte og undervisere), og at risikoen for de registrerede generelt må antages at være høj ved tab af f.eks. fortrolighed.

Tilsyn med PNR-loven

Datatilsynet fører i henhold til PNR-lovens regler tilsyn med behandlingen af personoplysninger hos Rigspolitiets passagerlisteoplysningsenhed (PNR-enhed). Enheden er ansvarlig for at indsamle, opbevare og behandle passagerlisteoplysninger (PNR-oplysninger) fra luftfartsselskaber og videregive PNR-oplysninger eller resultatet af behandlingen af disse oplysninger til kompetente myndigheder i Danmark og andre EU-medlemsstater mv.

I løbet af 2020 har Datatilsynet som led i dette tilsynsarbejde gennemført et tilsyn med Rigspolitiets overholdelse af PNR-lovens § 20, stk. 4, hvorefter enhver overførsel af PNR-oplysninger i henhold til lovens § 20 skal registreres. Endvidere har Rigspolitiets databeskyttelsesrådgiver mulighed for at underkaste overførslen efterfølgende kontrol.

Tilsynet blev afsluttet i første kvartal af 2021.

Databekymringspostkassen

Datatilsynet lancerede i juli 2019 en databekymringspostkasse i samarbejde med Dataetisk råd, hvor borgere kan henvende sig via e-mail med deres databekymringer. Lanceringen skete i forbindelse med nedsættelsen af Dataetisk Råd, da det er hensigten, at de indsendte databekymringer skal være med til at understøtte Dataetisk Råd i dets opgaver. Begge initiativer skete på baggrund af den tidligere regerings Sammenhængsreform om Digital Service i Verdensklasse. Initiativet forudsættes at ophøre med udgangen af 2022, hvorfor databekymringspostkassen nedlægges på dette tidspunkt, medmindre det politisk besluttes at føre den videre.

Datatilsynet modtog i 2020 i alt 64 databekymringer. Datatilsynet har dermed siden lanceringen den 4. juli 2019 indtil udgangen af 2020 modtaget i alt 122 databekymringer.

En generel tendens har været, at borgere har været bekymret for, at der behandles personoplysninger uden samtykke, og at der sker en viderebehandling, som den registrerede hverken kender til eller har samtykket til.

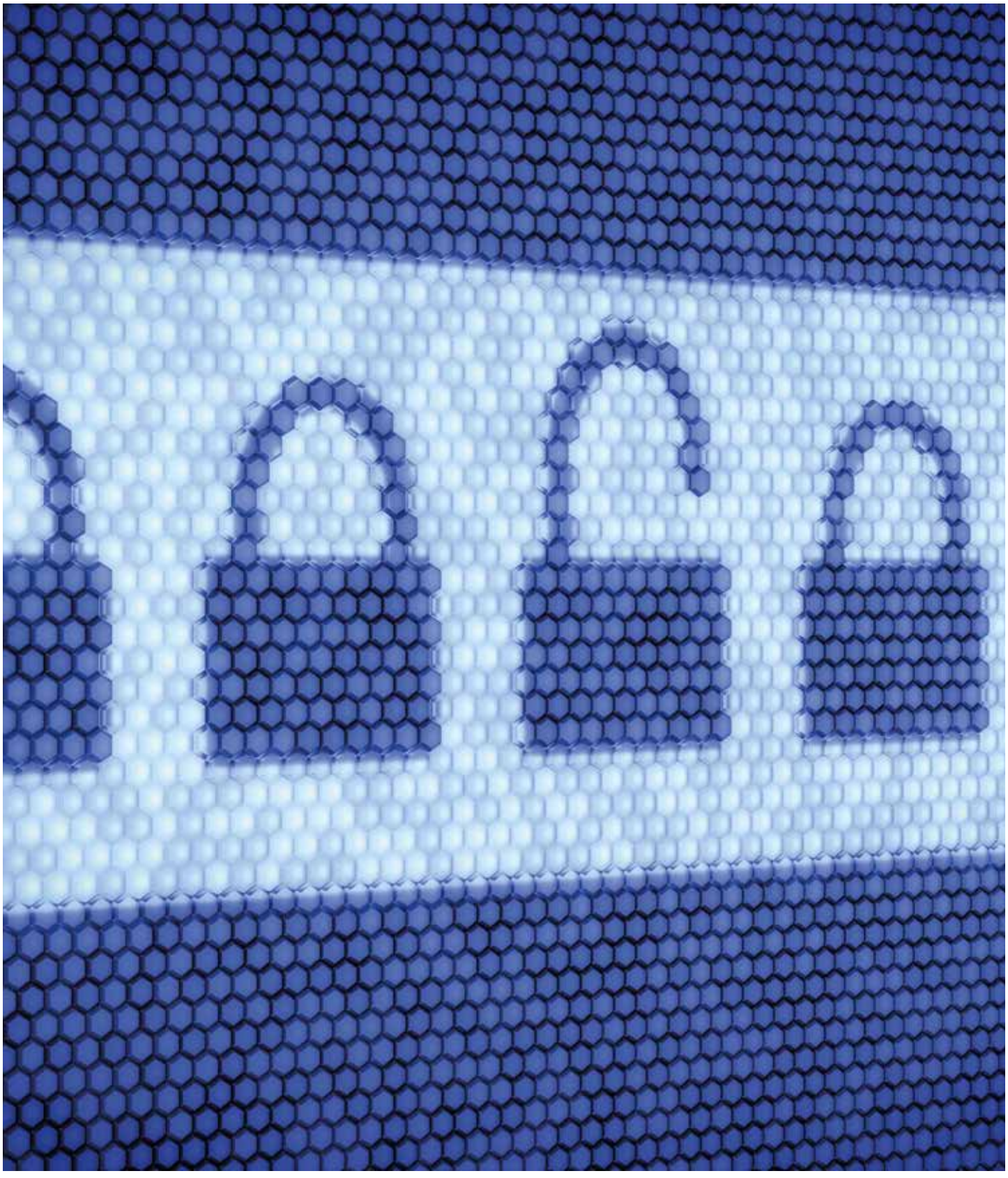
Databekymringerne har også i 2020 i høj grad omhandlet behandlingen af personoplysninger i den offentlige sektor. En række databekymringer har bl.a. angået offentlige myndigheders videregivelse af personoplysninger til uvedkommende, da borgere har oplevet at modtage personoplysninger om andre. Endvidere har borgere været bekymret for offentlige myndigheders brug af personnumre som journalnumre.

En ny tendens i 2020 har været, at flere databekymringer har omhandlet private virksomheders behandling af personoplysninger. Databekymringerne har i høj grad omhandlet private hjemmesider f.eks. muligheden for at slå oplysninger op om bilers ejere mv. ud fra bilens nummerplade og generelle bekymringer om hjemmesidernes indsamling af oplysninger. Bekymringerne har også angået cookieopsæt ningerne på flere hjemmesider. Derudover har borgere været bekymret for behandlingssikkerheden hos virksomhederne, herunder virksomhedernes mulighed for at modtage e-mails sikkert, da borgere oplever, at virksomhederne opfordrer deres kunder til at sende personoplysninger usikkert.

Databekymringerne i 2020 har også omhandlet den ekstraordinære situation som følge af Covid-19.

Bekymringerne har angået både indsamling og videregivelse af helbredsoplysninger, men også omlægningen af eksamensformerne og de programmer, som er blevet anvendt til at sikre mod snyd under prøverne.

Endvidere har en del af databekymringerne omhandlet videregivelse og viderebehandling af personoplysninger. Flere borgere frygter, at deres personoplysninger bliver benyttet til formål, som de ikke har givet tilladelse til, eller som de ikke er bekendt med.



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. 802 af 9. juni 2020 om ændring af lov om tv-overvågning..

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. 1078 af 20. september 2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser.
- Bekendtgørelse nr. 1079 af 20. september 2017 om behandling af personoplysninger i Politiets Efterforskningsstøttedatabase (PED).
- 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 med senere ændringer 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.
- Bekendtgørelse nr. 829 af 8. juni 2020 om tilbagemelding om væsentlige helbredsmæssige fund fra anmeldelsespligtige sundhedsvidenskabelige og sundhedsdatavidenskabelige forskningsprojekter samt visse registerforskningsprojekter.
- Bekendtgørelse nr. 1104 af 30. juni 2020 om helt eller delvis opbevaring her i landet af personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning.

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 og under opdatering nu)
- Vejledning af oktober 2017 om databeskyttelsesforordningen - generel informationspjece (under opdatering)
- Vejledning af november 2017 om dataansvarlige og databehandlere
- Vejledning af december 2017 om databeskyttelsesrådgivere (under opdatering)
- Vejledning af januar 2018 om adfærdskodekser og certificeringsordninger (opdateret i december 2018)
- Vejledning af januar 2018 om fortegnelse (opdateret august 2020)
- 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 juni 2019 om overførsel af personoplysninger til tredjelande (under opdatering)
- Vejledning af november 2018 om databeskyttelse i forbindelse med ansættelsesforhold (opdateret i august 2020)
- Vejledning af oktober 2019 om kreditoplysningsbureauer
- Vejledning af oktober 2019 om videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige
- Vejledning af november 2019 om advarselsregistre
- Vejledning af november 2019 om spærrelister
- Vejledning af februar 2020 om behandling af personoplysninger om hjemmesidebesøgende
- Vejledning af november 2020 om optagelse af telefonsamtaler

De oplistede vejledninger er offentliggjort på Datatilsynets hjemmeside under punktet "Vejledninger", hvor der også løbende vil blive offentliggjort nye vejledninger.

Vejledninger fra Justitsministeriet

- Vejledning af juni 2017 om udveksling af personoplysninger som led i den koordinerede myndighedsindsats over for rocker- og bandekriminalitet.
- Vejledning af december 2018 - Ofte stillede spørgsmål om frivillige foreningers behandling af personoplysninger.
- Vejledning af december 2018 om behandling af personoplysninger i SSP-samarbejdet.
- Vejledning af juli 2020 om lokationskravet i databeskyttelsesloven.
- Vejledning af august 2020 om udveksling af personoplysninger som led i indsatsen mod radikalisering og ekstremisme.
- Vejledninger fra Det Europæiske Databeskyttelsesråd.

Spørgsmål om Justitsministeriets vejledninger kan rettes til Justitsministeriet.

Vejledninger mv. fra Det Europæiske Databeskyttelsesråd (EDPB)

- 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)
- 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)
- Anbefalinger om de europæiske væsentlige garantier for overvågningsforanstaltninger (EDPB recommendations 2/2020)
- Anvendelse af lokaliseringsdata og kontaktopsporingsværktøjer i forbindelse med Covid-19-udbruddet (EDPB Guideline 4/2020)
- Behandling af personoplysninger i forbindelse med forbundne køretøjer og mobilitetsrelaterede applikationer (EDPB guideline 1/2020)
- Behandling af sundhedsdata med henblik på videnskabelig forskning i forbindelse med Covid-19-udbruddet (EDPB guideline 3/2020)
- 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)
- Brug af videoudstyr til behandling af personoplysninger (EDPB guideline 3/2019)

- Certificering (EDPB guideline 1/2018)
- Dataansvarlig og databehandler (EDPB guideline 7/2020)
- Dataportabilitet, retten til (wp242)
- Databeskyttelsesrådgivere, DPO'ere (wp243)
- Foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger (EDPB recommendations 1/2020)
- 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)
- Målrettet markedsføring i forhold til brugere af sociale medier (EDPB guideline 8/2020)
- Overførsel af personoplysninger mellem offentlige myndigheder og organer uden for EØS (EDPB guideline 2/2020)
- Relevant og begrundet indsigelse i henhold til forordningen (EDPB guideline 9/2020)
- Restriktioner i henhold til artikel 23 i GDPR (EDPB guideline 10/2020)
- Samtykke (wp259)
- Samtykke i henhold til forordningen (EDPB guideline 5/2020)
- Samspillet mellem det andet direktiv om betalingstjenester og GDPR (EDPB guideline 6/2020)
- Territorialt anvendelsesområde for databeskyttelsesforordningen (EDPB Guideline 3/2018)
- Tredjelandsoverførsler, tilstrækkeligt databeskyttelsesniveau (wp254)
- Tredjelandsoverførsler, undtagelser i særlige situationer (EDPB guideline 2/2018) (EDPB guideline 1/2019)
- Brug af videoudstyr til behandling af personoplysninger (EDPB guideline 3/2019)
- Behandling af personoplysninger i forbindelse med forbundne køretøjer og mobilitetsrelaterede applikationer (EDPB guideline 1/2020)

De nævnte vejledninger mv. er offentliggjort på EDPB's hjemmeside og kan tilgås via Datatilsynets hjemmeside under punktet "EDPB-vejledninger", hvor der løbende vil blive offentliggjort nye vejledninger mv.

Årsberetning

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

Foto: Datatilsynet

ISBN nr. 978-87-999222-5-3

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