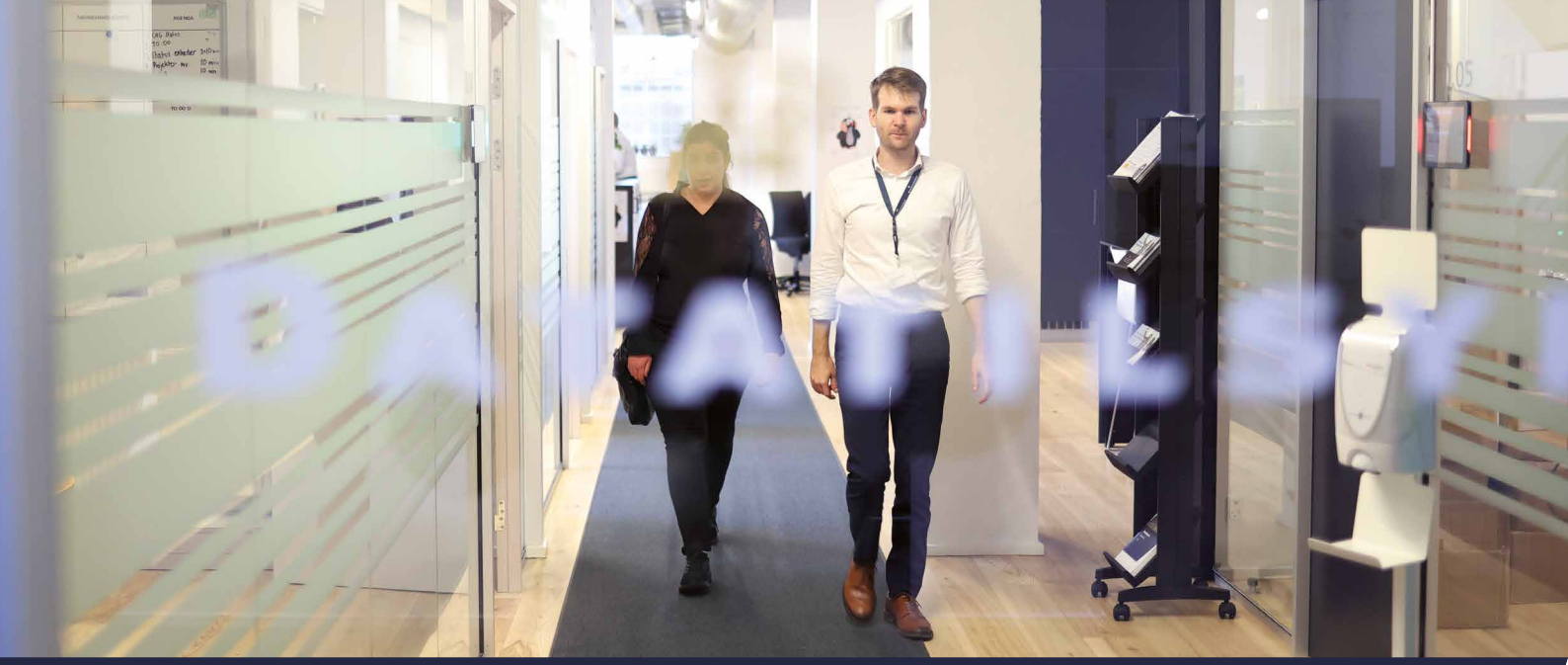


Datatilsynet

Årsberetning

2021

DATATILSYNET

Datatilsynet

Årsberetning

2021

DATATILSYNET

Indhold

Til Folketinget

Datatilsynet har i 2021 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 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 2021 har Datatilsynet offentliggjort fem nye nationale vejledninger om databeskyttelsesreglerne, som supplerer de 27 nationale vejledninger, der er offentliggjort i perioden fra 2017 til 2020.

Datatilsynet har i 2021 også offentliggjort en række vejledende hjemmesidetekster om f.eks. kommuners offentliggørelse af personoplysninger i offentligt tilgængelige webarkiver og om rollefordelingen, når private er leverandører til det offentlige. Endvidere har tilsynet udarbejdet en ny infografisk informationspjece om, hvad man som borger skal vide om databeskyttelse, ligesom Datatilsynet i december 2021 har offentliggjort en tjekliste til vuggestuer og børnehaver om brug af billeder og videoer.

Tilsynet har ydermere opdateret tidligere udgivne vejledninger og vejledende tekster, bl.a. vejledningen om overførsel af oplysninger til tredjelande. Opdateringen skete bl.a. for at afspejle den seneste udvikling på området, herunder Brexit, Europa-Kommissionens vedtagelse af nye standardkontraktbestemmelser og EU-Domstolens seneste praksis, herunder navnlig afgørelsen i den såkaldte Schrems II-sag.

Herudover har Datatilsynet i 2021 udarbejdet yderligere en episode til tilsynets podcast om databeskyttelsesforordningen, der er særligt relevant for SMV-segmentet. Podcasten, som nu består af i alt 21 episoder, er blevet taget rigtig godt imod af andre dataansvarlige, herunder også kommunerne, og af særligt interesserede borgere.

Datatilsynet yder en aktiv indsats på vejledningsområdet i europæiske sammenhænge. Tilsynet har i 2021 – i regi af Det Europæiske Databeskyttelsesråd – bidraget til udarbejdelsen af fem 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.

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 2021 behandlet flere større og ganske principielle sager om behandling af personoplysninger hos såvel offentlige myndigheder som private virksomheder.

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, ligesom tilsynet har holdt oplæg herom i mange forskellige sammenhænge.

National evaluering af databeskyttelsesreglerne

Justitsministeriet igangsatte i februar 2020 en national evaluering af databeskyttelsesreglerne. Evalueringsarbejdet foregik i to parallelle spor:

Det ene spor omfattede en række juridiske undersøgelser om mulighederne for at begrænse databeskyttelsesforordningens anvendelse på mindre aktører, at indføre en påbudsordning, at indføre en forhåndstilkendegivelsesordning og at forenkle reglerne i databeskyttelsesloven.

Det andet spor omfattede en erfaringsindsamling bestående af en bred høring af interessenter med henblik på at belyse, i hvilke situationer der i praksis opleves tvivl om databeskyttelsesreglerne. Justitsministeriet modtog i den forbindelse en række høringssvar, som viste bl.a., at der er problemstillinger, som går igen på tværs af interessenter.

Datatilsynet har både i 2020 og 2021 deltaget aktivt i denne nationale evaluering. Til brug for erfaringsindsamlingen – og Justitsministeriets afsluttende rapport – bidrog Datatilsynet således med et omfattende bidrag. Bidraget, som er tilgængeligt på bl.a. Datatilsynets hjemmeside, indeholder mulige løsninger og vejledning om de problemstillinger, som interessenterne har rejst.

Specialudvalg om det internationale databeskyttelsesarbejde

Datatilsynet nedsatte i 2020 som led i opfølgningen på tilsynets nye strategiske grundlag fra samme år 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.

I 2021 har Datatilsynet besluttet også at nedsætte et specialudvalg om det internationale databeskyttelsesarbejde. Formålet med specialudvalget er at give tilsynets interessenter et bedre indblik i Datatilsynets internationale databeskyttelsesarbejde samt en mulighed for at bidrage til dette arbejde og dermed styrke Datatilsynets varetagelse af danske interesser i det internationale samarbejde. Et centralt element i databeskyttelsesforordningen er et øget og mere formaliseret samarbejde mellem de europæiske datatilsyn, som har til formål at harmonisere fortolkningen af databeskyttelsesreglerne i EU.

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 2021 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.

Adfærdskodekser

Efter databeskyttelsesforordningen er det muligt for sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige og databehandlere, at udarbejde såkaldte adfærdskodekser, eller ændre eller udvide sådanne kodekser med henblik på at specificere anvendelsen af forordningen. En adfærdskodeks kan eksempelvis bruges inden for visse brancher, hvor bestemte problemstillinger kan gøres mere overskuelige at overholde for dataansvarlige eller databehandlere ved udarbejdelse af konkrete retningslinjer. En adfærdskodeks skal derfor være tilstrækkeligt fokuseret på bestemte data-

beskyttelsesretlige områder og problemstillinger i den pågældende sektor, og den skal kunne tilvejebringe tilstrækkeligt klare og præcise løsninger til disse områder og problemstillinger.

En kodeks skal godkendes af Datatilsynet efter forelæggelse af et udkast i overensstemmelse med reglerne i databeskyttelsesforordningens kapitel IV, afdeling 5.

En adfærdskodeks, som regulerer behandlingsaktiviteter for private organer, skal endvidere have et akkrediteret kontrolorgan. Kontrolorganets opgave er blandt andet at sikre, at de dataansvarlige og databehandlere, som er tilsluttet kodeksen, overholder kodeksens retningslinjer.

I sommeren 2021 godkendt Datatilsynet en adfærdskodeks om behandling af personoplysninger som led i sognepleje for menighedsråd i Danmark. Adfærdskodeksen, der er udarbejdet af Kirkeministeriet i samarbejde med Landsforeningen af Menighedsråd, er den første af sin art herhjemme.

Adfærdskodeksen opstiller konkrete retningslinjer og procedurer med henblik på at sikre en lovlig behandling af personoplysninger for menighedsrådet som dataansvarlig. Særligt indgår emner som dataansvar, de generelle behandlingsprincipper, behandlingsgrundlag, oplysningspligten, sikker op-

bevaring og sikker kommunikation mv. Målet med adfærdskodeksen er at lette overholdelsen af de databeskyttelsesretlige regler for de menighedsråd, der tilslutter sig kodeksen.

Det er frivilligt at tilslutte sig kodeksen, og det er kun de menighedsråd, som formelt vælger at tilslutte sig kodeksen, som skal overholde de indeholdte retningslinjer og procedurer.

Etablering af ekstern whistleblowerordning

Den 24. juni 2021 vedtog Folketinget loven om beskyttelse af whistleblowere med det formål at gennemføre Europa-Parlamentets og Rådets direktiv 2019/1937/EU af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten, i dansk ret (lov nr. 1436 af 29. juni 2021).

Der blev med loven indført en omfattende ramme for beskyttelse af whistleblowere, bl.a. ved i vidt omfang at pålægge offentlige myndigheder og en lang række private virksomheder og organisationer pligt til at etablere interne whistleblowerordninger. Som supplement til de interne whistleblowerordninger blev det endvidere besluttet, at Datatilsynet skulle etablere en ekstern whistleblowerordning til modtagelse og behandling af indberetninger vedrørende overtrædelser af visse områder af EU-retten og indberetninger om alvorlige lovovertrædelser og øvrige alvorlige forhold.

Den eksterne whistleblowerordning i Datatilsynet trådte i kraft den 17. december 2021, som også var datoen for lovens ikrafttrædelse. Den eksterne whistleblowerordning i Datatilsynet er uafhængig og selvstændig, hvilket indebærer, at arbejdet med whistleblowerindberetninger holdes adskilt fra Datatilsynets øvrige opgaver og funktioner og fungerer uafhængig af tilsynets øvrige virksomhed. Det betyder bl.a., at Datarådet ikke beskæftiger sig med whistleblowerordningen.

Udover at behandle whistleblowerindberetninger om overtrædelser af EU-retten inden for en række områder, herunder offentligt udbud, produktsikkerhed, miljøbeskyttelse, fødevaresikkerhed m.fl., behandler den eksterne whistleblowerordning indberetninger om alvorlige lovovertrædelser eller øvrige alvorlige forhold. Det indebærer, at der som udgangspunkt skal være tale om oplysninger, som er af offentlig interesse, og at der således skal bestå en reel samfundsinteresse i oplysningerne.

Ikke alle og enhver kan foretage indberetninger til den eksterne whistleblowerordning – for at opnå beskyttelse som whistleblower skal der være tale om oplysninger, som man er kommet i besiddelse af som led i en arbejdsrelateret aktivitet. Det betyder, at man ikke kan indberette oplysninger om forhold, som man f.eks. har fået kendskab til som borger i en kommune – her må man i stedet bruge de klagemuligheder, der er inden for det pågældende område.

Datatilsynet har etableret hjemmesiden www.whistleblower.dk, hvor man kan læse mere om den eksterne whistleblowerordning i Datatilsynet.

Valby, marts 2022

Kristian Korfits Nielsen
Formand, Datarådet

Cristina Angela Gulisano
Direktør, Datatilsynet

Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2021 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 2021, 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 2021 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.

Ekstern whistleblowerordning i Datatilsynet

Den 24. juni 2021 vedtog Folketinget loven om beskyttelse af whistleblowere med det formål at gennemføre Europa-Parlamentets og Rådets direktiv 2019/1937/EU af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten, i dansk ret (lov nr. 1436 af 29. juni 2021). Derudover blev der med loven indført en omfattende ramme for beskyttelse af whistleblowere i dansk ret, bl.a. ved i vidt omfang at pålægge offentlige myndigheder og en lang række private virksomheder og organisationer pligt til at etablere interne whistleblowerordninger.

Som supplement til de interne whistleblowerordninger blev det endvidere besluttet, at Datatilsynet skulle etablere en ekstern whistleblowerordning til modtagelse og behandling af indberetninger vedrørende overtrædelser af visse områder af EU-retten og indberetninger om alvorlige lovovertrædelser og øvrige alvorlige forhold.

Den eksterne whistleblowerordning trådte i kraft den 17. december 2021, som også var datoen for lovens ikrafttrædelse.

Den eksterne whistleblowerordning i Datatilsynet er uafhængig og selvstændig, hvilket indebærer, at arbejdet med whistleblowerindberetninger holdes adskilt fra Datatilsynets øvrige opgaver og funktioner og fungerer uafhængig af tilsynets øvrige virksomhed. Det betyder bl.a., at Datarådet ikke beskæftiger sig med whistleblowerordningen.

De af Datatilsynets medarbejdere, som behandler whistleblowerindberetninger i den eksterne whistleblowerordning, er særligt autoriseret til at arbejde med disse indberetninger og er underlagt en særlig tavshedspligt med hensyn til oplysninger, der indgår i indberetningerne.

Udover at behandle whistleblowerindberetninger om overtrædelser af EU-retten inden for en række områder, herunder offentligt udbud, produktsikkerhed, miljøbeskyttelse, fødevaresikkerhed m.fl., behandler den eksterne whistleblowerordning indberetninger om alvorlige lovovertrædelser eller øvrige

alvorlige forhold. Det indebærer, at der som udgangspunkt skal være tale om oplysninger, som er af offentlig interesse, og at der således skal bestå en reel samfundsinteresse i oplysningerne.

Ikke alle og enhver kan foretage indberetninger til den eksterne whistleblowerordning – for at opnå beskyttelse som whistleblower skal der være tale om oplysninger, som man er kommet i besiddelse af som led i en arbejdsrelateret aktivitet. Det betyder, at man ikke kan indberette oplysninger om forhold, som man f.eks. har fået kendskab til som borger i en kommune – her må man i stedet bruge de klagemuligheder, der er inden for det pågældende område.

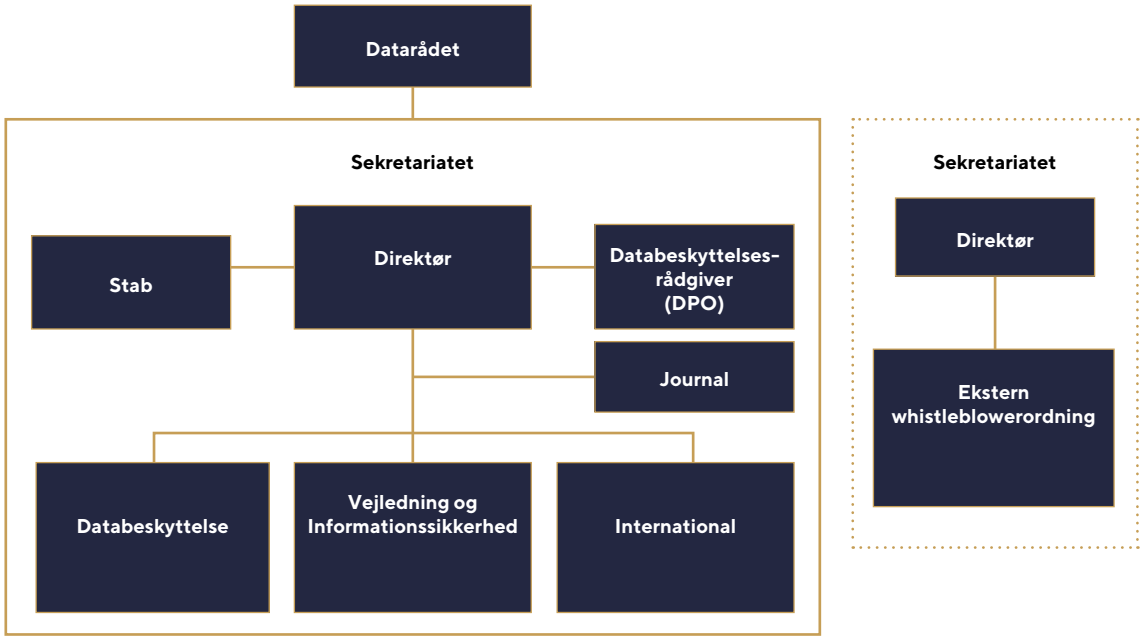
Datatilsynet har etableret hjemmesiden www.whistleblower.dk, hvor man kan læse mere om den eksterne whistleblowerordning i Datatilsynet.

Datatilsynets organisation

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

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

Datatilsynets organisationsdiagram 2021



Datarådet

Justitsministeren nedsætter Datarådet, 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 kvalificationer.

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

Datarådets medlemmer (pr. 31. december 2021)

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

Tilsynets sekretariat består af ca. 65 medarbejdere (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 2021, der kan findes på undersiden "Årsberetninger og årsrapporter" på Datatilsynets hjemmeside.

Sekretariatets medarbejdere (pr. 31. december 2021)

(Oversigten viser antallet af medarbejdere og ikke antallet af årsværk. Der kan derfor være visse afvigelser i forhold til den økonomiske årsrapport for 2021)

Direktør, cand.jur. Cristina Angela Gulisano
Kommitteret, cand.jur. Birgit Kleis
Kontorchef, cand.jur. Astrid Mavrogenis
Kontorchef, cand.jur. Anders Aagaard
Chefkonsulent, cand.jur. Eva Volfing
Chefkonsulent, cand.jur. Morten Juul Gjermundbo
Chefkonsulent, cand.jur. Karina Kok Sanderhoff
Chefkonsulent, cand.jur. Katrine Valbjørn Trebbien
Chefkonsulent, cand.jur. Susanne Richter (orlov)
Specialkonsulent, cand.jur. Anahita Khatam-Lashgari
Specialkonsulent, cand.soc. Gry Wad
Specialkonsulent, cand.jur. Kenni Elm Olsen
Specialkonsulent, cand.jur. Lea Bruun
Specialkonsulent, cand.jur. Liv Palmelund Osborg
Specialkonsulent, cand.jur. Louise Ellemann Christensen
Specialkonsulent, cand.jur. Marianne Halkjær Ebbesen
Specialkonsulent, cand.jur. Pernille Ørum Walther (orlov)

Specialkonsulent, cand.jur. Sarah Hersom Kublitz (orlov)
Controller, cand.merc.aud. Yimin Huang Nielsen
Stabsmedarbejder, cand.soc. Anne Bech
Stabsmedarbejder, cand.jur. Sidsel Kloppenburg
Kommunikationskonsulent, cand. mag. Anders Due
It-sikkerhedskonsulent, cand. jur. Allan Frank
It-sikkerhedskonsulent, cand.polyt. Julia Ilu Sommer
It-sikkerhedskonsulent, Ph.d., Martin Mehl Lauridsen Schadegg
It-sikkerhedskonsulent, politiassistent Poul Erik Høj Weidick
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
Kontorfuldmægtig Anne-Marie Müller
Kontorfuldmægtig Mette-Maj Aner Leilund
Kontorfuldmægtig Pernille Jensen
Kontorfunktionær Anette Sørensen
Kontorfunktionær Camilla Knutsdotter Hallingby
Kommunikationsfuldmægtig, cand.public. Johan Engstrøm
Kommunikationsfuldmægtig, cand.mag. Natascha Helverskov Jørgensen
Kommunikationsfuldmægtig, cand.mag. Hisar Sindi
Fuldmægtig, cand.jur. Anna Carolina Jensen
Fuldmægtig, cand.jur. Andreas Droob Kristensen
Fuldmægtig, cand.jur. Anette Borring-Møller (orlov)
Fuldmægtig, cand.jur. Astrid Malte Ivens De Carvalho (orlov)
Fuldmægtig, cand.jur. Betty Nielsen Husted
Fuldmægtig, cand.jur. Camilla Meineche
Fuldmægtig, cand.jur. Caroline Rasmussen
Fuldmægtig, cand.jur. Charlotte Nørtoft Poulsen
Fuldmægtig, cand.jur. Kasper Folmar
Fuldmægtig, cand.jur. Lise Fredskov (orlov)
Fuldmægtig, cand.jur. Line Sørensen
Fuldmægtig, cand.jur. Mads Nordstrøm Kjær
Fuldmægtig, cand.jur. Malene Højbjerg
Fuldmægtig, cand.jur. Maria Freja Reffeldt Bircherod Calundan
Fuldmægtig, cand.jur. Mia Kamille Frølund Thomsen
Fuldmægtig, cand.jur. Nikolaj Niss Rohde
Fuldmægtig, cand.jur. Ramus Martens
Fuldmægtig, cand.jur. Rasmus Arslev
Fuldmægtig, cand.jur. Rasha Suhiela Said Eleish
Fuldmægtig, cand.jur. Sara Koch Jørgensen
Fuldmægtig, cand.jur. Sara Samanlu
Fuldmægtig, cand.jur. Susanne Dige Nielsen
Fuldmægtig, cand.jur. Victoria Lenchler-Huebertz
Fuldmægtig, cand.jur. Zenia Dinesen (orlov)
Stud.jur. Amalie Pilgaard Stubdrup
Stud.jur. Ali Tarek Mohamad
Stud.jur. Amalie Overkær Lund Jensen
Stud.jur. Jonatan Aarkrogh Ubbesen
Stud.jur. Oskar Magnus Høgedal
Stud.BEng. Bjørn Wade Patterson
Stud.datamatiker., cand.mag. Lars Brogaard Kaiser

Året i tal

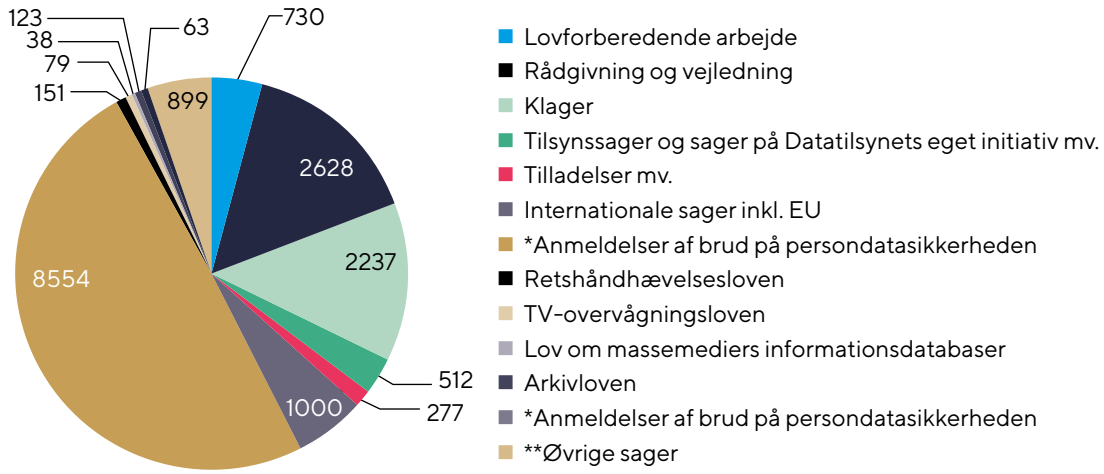
I det følgende afsnit findes oplysninger om antallet af nye sager, som er oprettet i Datatilsynets journalsystem i 2021.

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 **17.291** nye sager i 2021.

Fordeling af oprettede sager i 2021	
Lovforberedende arbejde	730
Rådgivning og vejledning	2.628
Klager	2.237
Tilsynssager og sager på Datatilsynets eget initiativ mv.	512
Tilladelser mv.	277
Internationale sager inkl. EU	1.000
Anmeldelser af brud på persondatasikkerheden*	8.554
Retshåndhævelsesloven	151
TV-overvågningsloven	79
Lov om massemediers informationsdatabaser	38
Arkivloven	123
Sager om Grønland og Færøerne	63
Øvrige sager**	899
Sager i alt	17.291

Oprettede sager i 2021



Bemærkninger

Der kan optræde mindre afvigelser i tallene, f.eks. hvor nogle sager er blevet omjournaliseret eller konstateret fejloprettet.

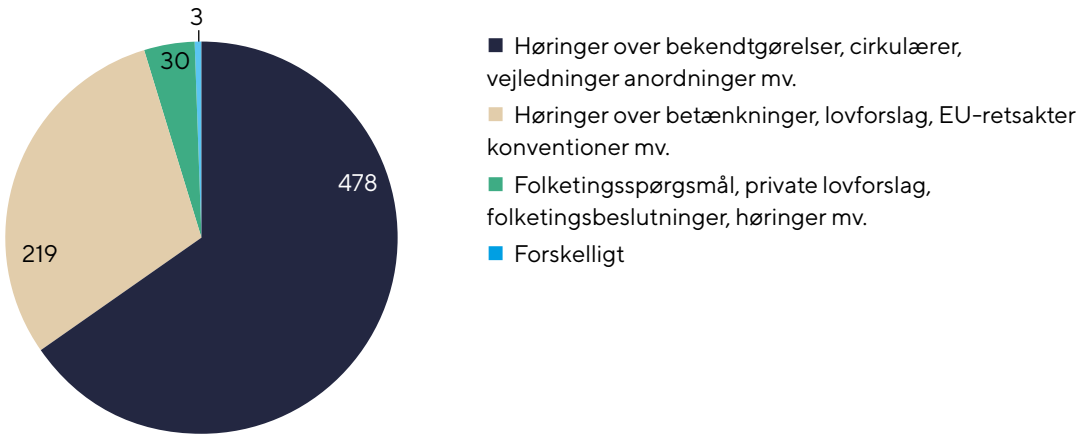
* Anmeldelser af brud på persondatasikkerheden efter retshåndhævelsesloven er ikke medtaget i antallet af anmeldelser af brud på persondatasikkerheden, men fremgår af sagsgruppen "Retshåndhævelsesloven".

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

Lovforberedende arbejde
(Høringer, folketingspørgsmål mv.)

Fordeling af sager vedr. lovforberedende arbejde	
Høringer over bekendtgørelser, cirkulærer, vejledninger, anordninger mv.	478
Høringer over betænkninger, lovforslag, EU-retsakter, konventioner mv.	219
Folketingsspørgsmål, private lovforslag, folketingsbeslutninger, høringer mv.	30
Forskelligt	3
Sager i alt	730

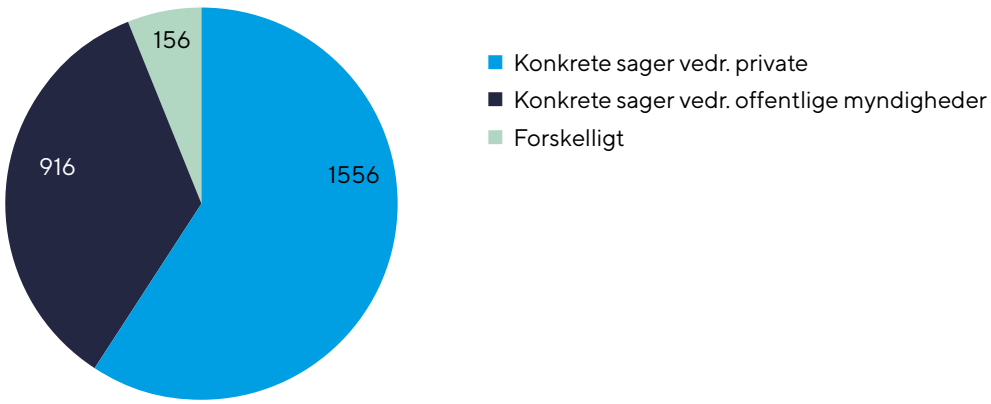
Sager vedrørende lovforberedende arbejde



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

Fordeling af sager vedr. rådgivning og vejledning	
Konkrete sager vedr. private	1556
Konkrete sager vedr. offentlige myndigheder	916
Forskelligt	156
Sager i alt	2628

Fordeling af sager vedr. rådgivning og vejledning

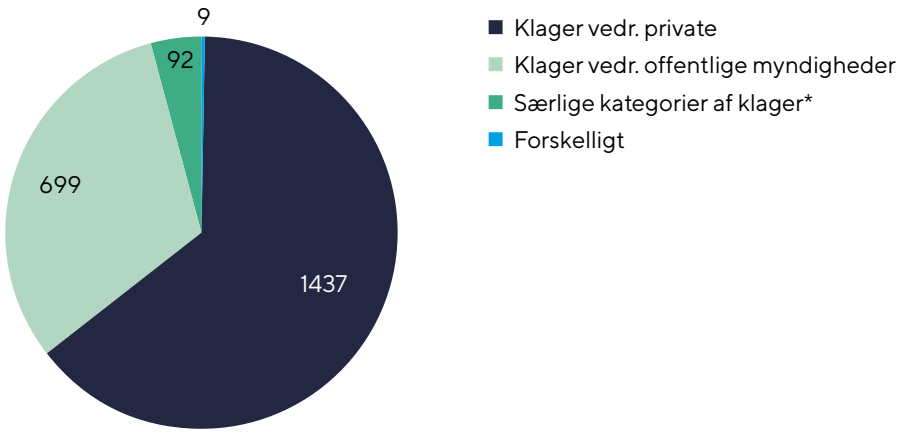


Tilsyn
(Klager)

Fordeling af klagesager	
Klager vedr. private	1437
Klager vedr. offentlige myndigheder	699
Særlige kategorier af klager *	92
Forskelligt	9
Sager i alt	2237

*Klager over kreditoplysningsbureauer

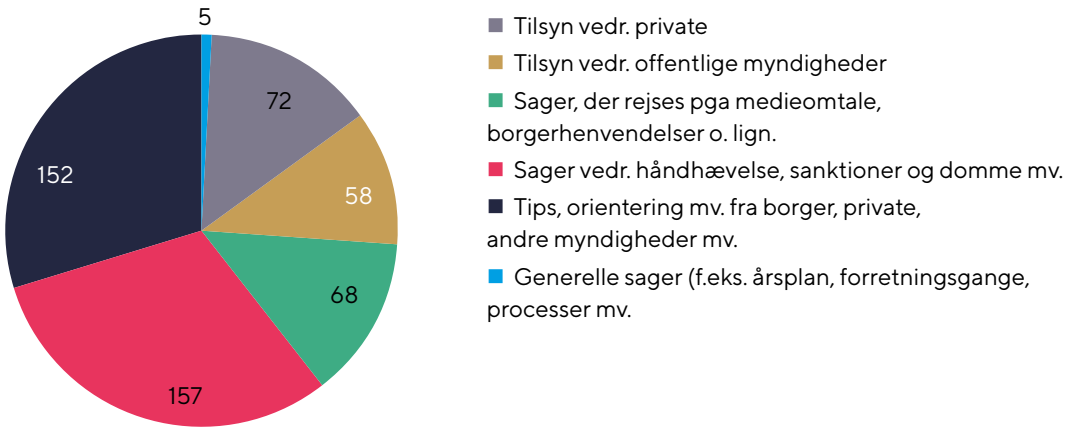
Klagesager



Sager på Datatilsynets eget initiativ

Fordeling af tilsynssager og sager på Datatilsynets eget initiativ mv.	
Tilsyn vedr. private	72
Tilsyn vedr. offentlige myndigheder	58
Sager, der rejses pga. medieomtale, borgerhenvendelse o.lign.	68
Sager vedr. håndhævelse, sanktioner og domme mv.	157
Tips, orientering mv. fra borgere, private, andre myndigheder mv.	152
Generelle sager (f.eks. årsplan, forretningsgange, processer mv.)	5
Sager i alt	512

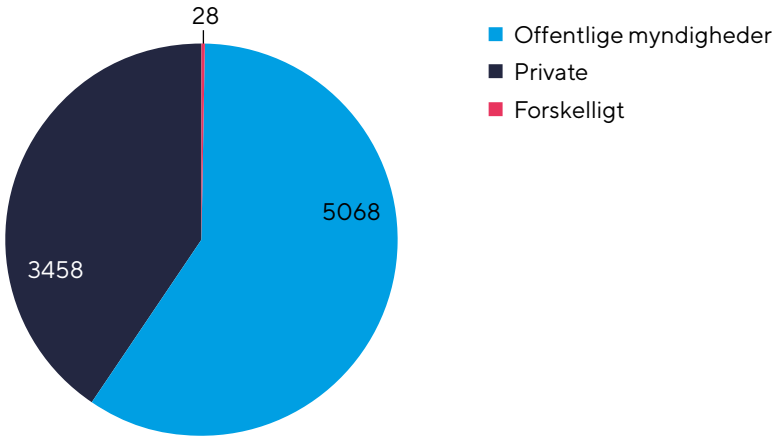
Sager på Datatilsynets eget initiativ



Anmeldelser af brud på persondatasikkerheden

Fordeling af anmeldelser af brud på persondatasikkerheden	
Offentlige myndigheder	5068
Private	3458
Forskelligt	28
Sager i alt	8.554

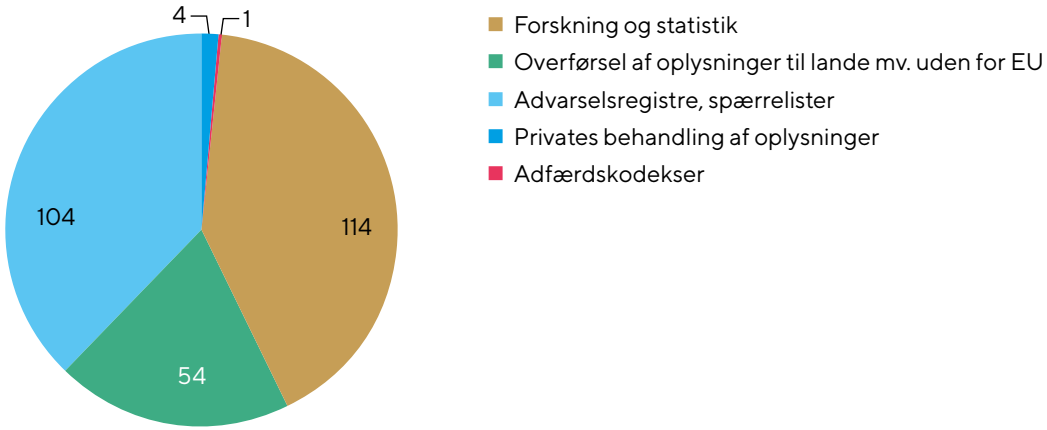
Fordelingen af anmeldelser af brud på persondatasikkerheden



Tilladelser mv.

Tilladelser mv.	
Forskning og statistik	114
Overførsel af oplysninger til lande mv. uden for EU	54
Advarselsregistre, spærrelister	104
Privates behandling af oplysninger	4
Adfærdskodekser	1
Sager i alt	277

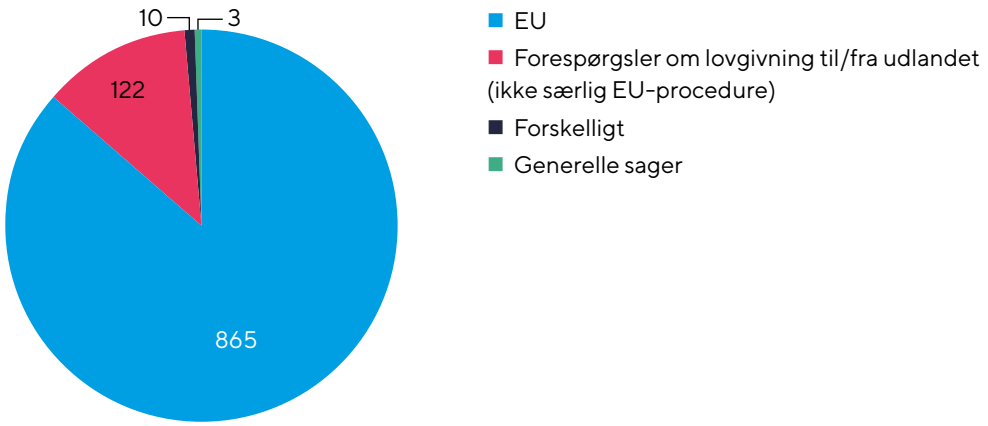
Tilladelser mv.



Internationale sager

Fordeling af internationale sager	
EU	865
Forespørgsler om lovgivning til/fra udlandet (ikke særlig EU-procedure)	122
Forskelligt	10
Generelle sager	3
Sager i alt	1000

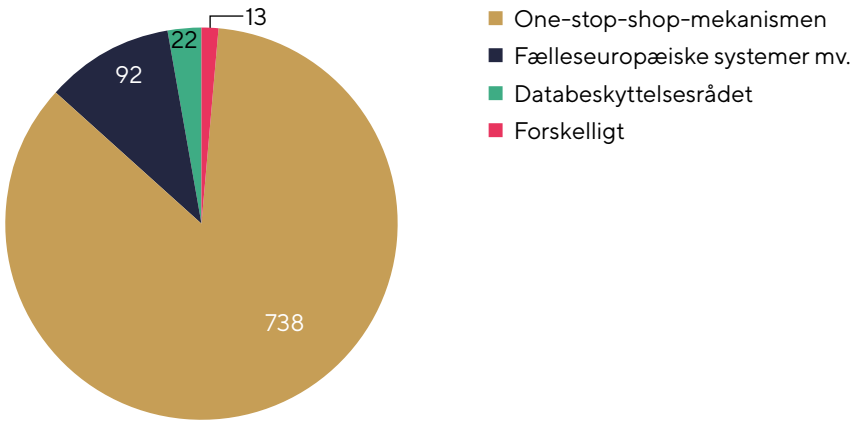
Fordelingen af internationale sager



Fordeling af EU-sager

Fordeling af EU-sager	
One-stop-shop-mekanismen	738
Fælleseuropæiske systemer mv.	92
Databeskyttelsesrådet	22
Forskelligt	13
Sager i alt	865

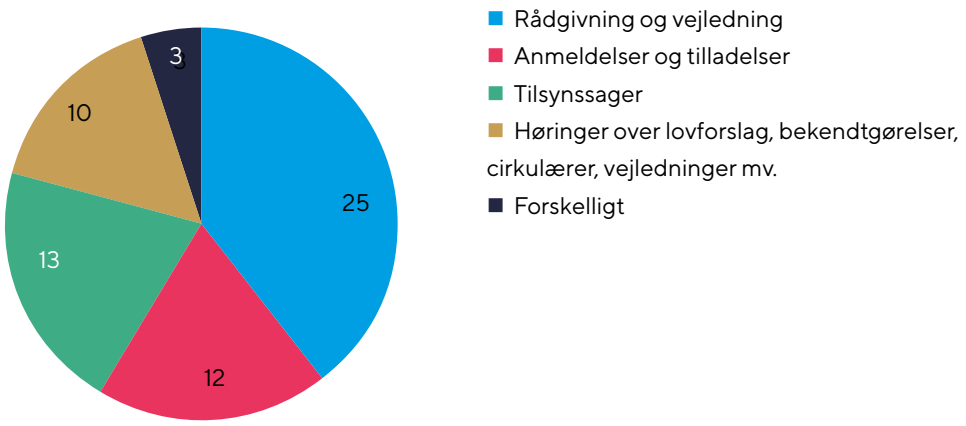
Fordelingen af EU-sager



Grønland og Færøerne

Fordeling af sager vedr. Grønland og Færøerne	
Rådgivning og vejledning	25
Anmeldelser og tilladelser	12
Tilsynssager	13
Høringer over lovforslag, bekendtgørelser, cirkulærer, vejledninger mv.	10
Forskelligt	3
Sager i alt	63

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

Datatilsynet har i 2021 offentliggjort fem nye nationale vejledninger om databeskyttelsesreglerne, som supplerer de 27 nationale vejledninger, som tilsynet har offentliggjort fra 2017 til 2020. Datatilsynet yder også en aktiv indsats på vejledningsområdet i europæiske sammenhænge og har i regi af Det Europæiske Databeskyttelsesråd bidraget til udarbejdelsen af fem nye fælleseuropæiske vejledninger om databeskyttelsesforordningen. Alle de nævnte vejledninger og skabeloner kan findes på Datatilsynets hjemmeside.

Datatilsynet har i 2021 også offentliggjort en række vejledende hjemmesidetekster om f.eks. kommuners offentliggørelse af personoplysninger i offentligt tilgængelige webarkiver og om rollefordelingen, når private er leverandører til det offentlige. Endvidere har tilsynet udarbejdet en ny infografisk informationspjece om, hvad man som borger skal vide om databeskyttelse, ligesom Datatilsynet i december 2021 har offentliggjort en tjekliste til vuggestuer og børnehaver om brug af billeder og videoer.

Tilsynet har ydermere opdateret tidligere udgivne vejledninger og vejledende tekster, bl.a. vejledningen om overførsel af oplysninger til tredjelande. Opdateringen skete bl.a. for at afspejle den seneste udvikling på området, herunder Brexit, Europa-Kommissionens vedtagelse af nye standardkontraktbestemmelser og EU-Domstolens seneste praksis, herunder navnlig afgørelsen i den såkaldte Schrems II-sag.

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 også i 2021 sat sine naturlige begrænsninger for Datatilsynets muligheder for deltagelse samt omfanget af relevante arrangementer.

Datatilsynets podcast – "Bliv klogere på GDPR"

Siden lanceringen i september 2019 har Datatilsynet produceret 21 tilgængelige episoder af tilsynets podcast "Bliv klogere på GDPR". I 2021 opnåede podcasten 56.258 afspilninger, hvilket totalt set udgør 136.076 afspilninger (pr. 31. december 2021).

Podcastepisoderne tager fat i et afgrænset emne inden for GDPR og foregår typisk som en dialog mellem to af tilsynets medarbejdere i en uformel tone, hvor de juridiske problemstillinger forklares i øjenhøjde med konkrete og virkelighedsnære eksempler.

Som et supplement til Datatilsynets opdaterede vejledning om overførsel af personoplysninger til tredjelande, udgav tilsynet i juli 2021 to podcast-episoder, der på baggrund af Schrems II-afgørelsen indeholder en genindspilning af episoden *"#10 Tredjelands overførsler – hvornår og hvad gælder?"* med en generel introduktion til emnet samt et helt nyt afsnit *"#21 Tredjelandsoverførsler – situationen efter Schrems II"*, der dykker ned i konsekvenserne af Schrems II-afgørelsen. Det helt nye afsnit har bl.a. fokus på overførselsværktøjer, supplerende foranstaltninger, de fire essentielle garantier og et essentielt, ækvivalent beskyttelsesniveau.

Datatilsynets podcast er således et supplement til den mere traditionelle, skriftlige vejledning, som tilsynet 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.

Datatilsynets podcast er tilgængelig på alle gængse streamingtjenester.

National evaluering af databeskyttelsesreglerne

Justitsministeriet igangsatte i februar 2020 en national evaluering af databeskyttelsesreglerne. Evalueringsarbejdet foregik i to parallelle spor:

Det ene spor omfattede en række juridiske undersøgelser om mulighederne for at begrænse databeskyttelsesforordningens anvendelse på mindre aktører, at indføre en påbudsordning, at indføre en forhåndstilkendegivelsesordning og at forenkle reglerne i databeskyttelsesloven.

Det andet spor omfattede en erfaringsindsamling bestående af en bred høring af interessenter med henblik på at belyse, i hvilke situationer i praksis der opleves tvivl om databeskyttelsesreglerne. Justitsministeriet modtog i den forbindelse en række høringssvar, som viste bl.a., at der er problemstillinger, som går igen på tværs af interessenter, herunder i forhold til:

- Behov for mere (konkret) vejledning
- Begreberne dataansvarlig og databehandler
- Overførsel til lande uden for EØS (såkaldte tredjelande)
- Anmeldelse af brud på persondatasikkerheden
- Behandlingssikkerhed, risikovurderinger og konsekvensanalyser
- Fortegnelse og andre dokumentationskrav
- Offentlige myndigheders anvendelse af artikel 6, stk. 1, litra e
- Opbevaringsbegrænsning og sletning
- Oplysningspligt
- Retten til indsigt
- Forskning
- Arkivering

Til brug for erfaringsindsamlingen – og Justitsministeriets afsluttende rapport – bidrog Datatilsynet med et omfattende bidrag. Bidraget, som er tilgængeligt på bl.a. Datatilsynets hjemmeside, indeholder mulige løsninger og vejledning om de problemstillinger, som interessenterne har rejst.

Ny vejledning om udveksling af personoplysninger med politiet

I forbindelse med Justitsministeriets nationale evaluering af databeskyttelsesreglerne og den dertilhørende erfaringsindsamling, som er omtalt ovenfor, gav politiet udtryk for, at politiet ofte oplevede, at dataansvarlige – af frygt for at overtræde databeskyttelsesreglerne – ikke ønskede at bistå politiet ved at udlevere relevante oplysninger.

Det er afgørende for politiets effektive opgavevaretagelse, at politiet kan få udleveret relevante oplysninger – herunder personoplysninger – når politiet som led i sin myndighedsudøvelse retter henvendelse til private aktører eller offentlige myndigheder.

Datatilsynet offentliggjorde på den baggrund i 2021 – under inddragelse af Rigspolitiet og Justitsministeriet – en vejledning om udveksling af personoplysninger med politiet, som har til formål at illustrere rammerne for videregivelse af personoplysninger til politiet.

Vejledningen, som gennemgår det retlige grundlag for udveksling af personoplysninger med politiet og gennemgår typiske situationer, hvor man kan komme i tvivl om, hvorvidt det er i orden at videregive personoplysninger til politiet, illustrerer, at der er ganske vide rammer for videregivelse af personoplysninger til politiet.

Nye vejledninger om fastsættelse af bøder til virksomheder og privatpersoner

Databeskyttelsesforordningen og databeskyttelsesloven lægger op til et væsentligt forhøjet bødeniveau, ligesom det med forordningen er forudsat, at medlemsstaterne harmoniserer sanktionerne, dog under hensyn til det generelle indkomstniveau i den pågældende medlemsstat.

Datatilsynet har derfor i samarbejde med Rigsadvokaten og Rigspolitiet i 2021 udarbejdet nogle overordnede retningslinjer, der indeholder et klart og gennemskueligt grundlag for Datatilsynets indstilling af bødepåstande, som tager udgangspunkt i de vurderingskriterier, som fremgår af databeskyttelsesforordningen og databeskyttelsesloven.

I januar 2021 udgav Datatilsynet en bødevejledning, som opstiller en model for beregning af bøder til virksomheder. I september 2021 udgav tilsynet ligeledes en vejledning vedrørende udmåling af bøder til fysiske personer, som i højere grad baserer sig på standardiserede bøder. Begge vejledninger tager udgangspunkt i den erfaring tilsynet har opnået gennem vurderingen af sager de første år efter den 25. maj 2018, og i den erfaring der er gjort hos de øvrige europæiske tilsynsmyndigheder. Vejledningerne er endvidere arbejdsdokumenter, der løbende vil blive udbygget efterhånden som Datatilsynet, anklagemyndigheden og domstolene håndterer flere straffesager på området, og i takt med at praksis, såvel nationalt som i EU, udvikles.

Det bemærkes i den forbindelse, at de europæiske tilsynsmyndigheder med undtagelse af Danmark og Estland har hjemmel til at udstede administrative bøder, som er bindende, hvis de ikke appelleres. Der vil således med tiden foreligge både administrativ og domstolspraksis. Endvidere bemærkes, at Datatilsynet med databeskyttelseslovens § 42 har fået hjemmel til at udstede administrative bødeforlæg. Det er dog en betingelse for udstedelse af administrative bødeforlæg, at der, udover at modtageren erkender overtrædelsen, foreligger et klart bødeniveau. Det forventes derfor, at der med tiden, efterhånden som praksis bliver udbygget, vil kunne fastsættes "standardiserede" bøder for nærmere angivne overtrædelser af de databeskyttelsesretlige regler.

I øvrigt bemærkes, at Det Europæiske Databeskyttelsesråd (EDPB) ligeledes arbejder på retningslinjer for bødeudmålingen efter databeskyttelsesforordningen. Såvel beregningsmodellen som bødeniveauet i nærværende vejledning kan således påvirkes af dette fælleseuropæiske arbejde.

Ny quick guide til brug af cookies

I februar 2021 udgav Datatilsynet i samarbejde med Rådet for Digital Sikkerhed og Erhvervsstyrelsen en quick guide til brug af cookies.

Quick guiden er udarbejdet med det formål at tydeliggøre, hvordan både reglerne i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet) og databeskyttelsesbeskyttelsesreglerne kan efterleves, når aktører placerer cookies på brugernes terminaludstyr.

Quick guiden tager udgangspunkt i, at efter e-databeskyttelsesdirektivet skal en brugers samtykke indhentes, før der må placeres cookies. Hvis der efterfølgende sker behandling af de oplysninger, der gemmes i cookies, skal behandlingen have hjemmel i de databeskyttelsesretlige regler, hvor samtykke typisk også vil være den mest passende hjemmel. Der gælder i den forbindelse de samme kriterier for begge samtykker, idet samtykket skal være udtryk for en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra brugerne.

Quick guiden giver en række bud på, hvad aktørerne skal være særligt opmærksomme på. Bl.a. fremhæves det, at brugerne skal have mulighed for at foretage en aktiv handling, hvorfor forudafkrydsede felter eller klik-videre-funktioner ikke er forenelige med betingelserne til samtykke.

Endvidere sætter Quick guiden fokus på, hvilke informationer der skal gives til brugerne ved placering af cookies, hvordan disse informationer gives, og hvilken rolle en hjemmesideindehaver indtager i den sammenhæng, herunder om denne er selvstændig dataansvarlig eller fælles dataansvarlig med eventuelle samarbejdspartnere.

Ny vejledning om certificeringsordninger og akkrediteringskrav til kontrolorganer

Datatilsynet udgav i april 2021 en ny vejledning om certificeringsordninger. Certificeringsordninger er en måde, hvorpå en organisation kan opnå et certifikat, der demonstrerer, at organisationen overholder GDPR på visse områder. I vejledningen kan man bl.a. læse mere om, hvad en databeskyttelsesretlig certificeringsordning er, hvem der kan udarbejde en certificeringsordning, hvad man kan bruge en certificeringsordning til, og hvordan en certificeringsordning godkendes. Man kan også læse om, hvordan man som myndighed eller virksomhed tilslutter sig en certificeringsordning.

En certificeringsordning laves af et eller flere certificeringsorganer. Et certificeringsorgan er den virksomhed eller myndighed, der udsteder certifikater igennem certificeringsordningen. Et certificeringsorgan skal først akkrediteres (godkendes) af DANAK, før de må udstede certifikater.

Datatilsynet offentliggjorde i foråret 2021 også en række supplerende krav, som en myndighed eller virksomhed skal opfylde, hvis de vil være et certificeringsorgan. Kravene, som Datatilsynet offentliggjorde, supplerer en række krav, der er fastsat i databeskyttelsesforordningen og en ISO-standard.

Opdatering af vejledning om samtykke

I maj 2021 opdaterede Datatilsynet vejledningen om samtykke med uddybninger, præciseringer og aktuel praksis. Det fremgår i den opdaterede vejledning, at offentlige myndigheder som udgangspunkt ikke kan behandle personoplysninger på baggrund af samtykke. Endvidere er det blevet uddybet, at krav om "samtykke" fra borgerne i anden lovgivning ikke nødvendigvis er ensbetydende med, at behandlingen af personoplysninger skal ske på baggrund af et samtykke.

Eksempel 8 er blevet ændret i den opdaterede vejledning. Dette er ikke et udtryk for, at det tidligere eksempel 8 var forkert, men Datatilsynet har konstateret, at eksemplet har givet anledning til misforståelser. Derfor indeholder den opdaterede version et nyt eksempel, der er med til at forklare, hvornår et samtykke er specifikt. Det fremgår også, at det, at man scroller eller swiper igennem en hjemmeside eller anden tilsvarende brugeraktivitet på en hjemmeside, ikke anses for en utvetydig viljestilkendegivelse.

Tjeklisten har fået et nyt udseende, som betyder, at den er mere brugbar som reel tjekliste, da man nu kan printe eller kopiere denne og bruge den direkte. Endelig er vejledningens tidligere afsnit 5 om overgang fra persondataloven til databeskyttelsesforordningen blevet fjernet.

Det er fortsat Datatilsynets opfattelse, at de, der før 25. maj 2018 behandlede personoplysninger på baggrund af et samtykke, ikke skulle indhente samtykker på ny, hvis samtykket var i overensstemmelse med betingelserne i databeskyttelsesforordningen. Afsnittet er alene fjernet, da det er Datatilsynets vurdering, at dette ikke længere er relevant næsten tre år efter databeskyttelsesforordningen begyndte at finde anvendelse.

Optimering af Datatilsynets hjemmeside

I maj 2021 relancerede Datatilsynet også en optimeret udgave af tilsynets hjemmeside www.datatilsynet.dk. Hjemmesidens brugerflade er blevet optimeret med fokus på den gode brugeroplevelse for hjemmesidens mange daglige besøgende:

- Enklere og mere intuitiv brugerflade.
- Omstrukturering af menuer, undersider og indhold.
- Bedre præsentation af dansk og internationalt vejledningsmateriale.
- Bedre søgefunktion.

Både nyt og eksisterende vejledningsmateriale – samt mere generelt indhold om databeskyttelse – er nu kategoriseret på en intuitiv måde, så Datatilsynets mange forskellige interessenter nemmere kan finde frem til den viden, de har brug for, når de søger efter vejledning – hvad enten de er borgere eller dataansvarlige og/eller databehandlere.

Kommuners offentliggørelse af personoplysninger i offentligt tilgængelige webarkiver

Datatilsynet behandlede i 2021 en række klagesager, der i forskellige afskygninger omhandler spørgsmålet om kommuners offentliggørelse af personoplysninger i forbindelse med behandling af byggesager mv.

Det har tidligere været Datatilsynets praksis, at kommunerne i deres byggesagsarkiver m.v. har kunnet offentliggøre personoplysninger, som ikke var fortrolige.

Den teknologiske udvikling har imidlertid betydet, at borgere og myndigheder kommunikerer digitalt i langt større omfang end tidligere, og at der i den forbindelse indsamles flere og flere personoplysninger. Dette har øget behovet for, at personoplysninger, som måske i sig selv fremstår harmløse, beskyttes.

Fremadrettet vil det derfor – efter at spørgsmålet har været behandlet i Datarådet – være Datatilsynets praksis, at e-mailadresser og telefonnumre ikke kan offentliggøres i de offentligt tilgængelige webarkiver. Det samme er tilfældet med hensyn til korrespondancer, som ikke vedrører den konkrete ejendom.

Datatilsynets praksisændring gælder ikke bagudrettet, dvs. at kommunerne ikke som følge af praksisændringen er forpligtet til at gennemgå allerede offentliggjort materiale. Skulle kommunen imidlertid modtage en indsigelse fra en registreret, skal indsigelsen behandles i overensstemmelse med den nye praksis.

På Datatilsynets hjemmeside – på undersiden "Kommunale forhold" – findes en vejledende tekst, ligesom tilsynet løbende vil offentliggøre nye afgørelser til belysning af den nye praksis.

Opdatering af vejledning om overførsel til tredjelande

Datatilsynet offentliggjorde i juli 2021 en opdateret vejledning om overførsel af personoplysninger til tredjelande. Opdateringen skete bl.a. for at afspejle den seneste udvikling på området, herunder Brexit, Europa-Kommissionens vedtagelse af nye standardkontraktbestemmelser og EU-Domstolens seneste praksis, herunder navnlig afgørelsen i den såkaldte Schrems II-sag (se nærmere herom i afsnittet Internationalt arbejde).

Den opdaterede vejledning har fortsat et generelt sigte, der giver en grundlæggende introduktion til reglerne om overførsel til tredjelande. Datatilsynet har herudover arbejdet med selve opbygningen af vejledningen med henblik på at gøre indholdet mere handlingsorienteret. De forskellige afsnit er opbygget, så de understøtter den beslutningsproces, man skal igennem, når man ønsker at overføre personoplysninger til et tredjeland. Der er endvidere tilført en række nye praktiske eksempler, der bl.a. skal illustrere, hvornår der er tale om en overførsel til et tredjeland.

Brug af kropsbårne kameraer (bodycams)

I august 2021 udarbejdede Datatilsynet en kort vejledende tekst om, hvilke forpligtelser og overvejelser man som dataansvarlig har og skal være særligt opmærksom på ved brug af kropsbårne kameraer – de såkaldte bodycams.

Af den vejledende tekst fremgår det, at hvis man som dataansvarlig optager billeder og lyd ved brug af kropsbårne kameraer (bodycams), er man i udgangspunktet underlagt de almindelige databeskyttelsesretlige regler og principper og ikke reglerne i tv-overvågningsloven. Behandling af personoplysninger ved brug af kropsbårne kameraer (bodycams) kan derfor kun finde sted, hvis de grundlæggende

behandlingsprincipper om bl.a. lovlighed, rimelighed og gennemsigtighed, formålsbegrænsning samt opbevaringsbegrænsning er opfyldt.

Derudover skal man som dataansvarlig sikre sig et såkaldt behandlingsrundlag. I den forbindelse er det vigtigt at være opmærksom på, at der gælder særlige regler, man skal overholde, når man behandler oplysninger om strafbare forhold eller oplysninger af følsom karakter (f.eks. helbredsoplysninger eller oplysninger om religiøs eller politisk overbevisning) på billed- og lydoptagelserne.

Den dataansvarlige er ligeledes ansvarlig for – ved hjælp af passende tekniske og organisatoriske foranstaltninger – at beskytte personoplysninger mod uautoriseret eller ulovlig behandling samt mod hændeligt tab, tilintetgørelse eller beskadigelse. Det bør endvidere alene være særligt autoriseret personale, der har adgang til optagelserne.

Det er den dataansvarliges ansvar, at personoplysninger ikke behandles i strid med de databeskyttelsesretlige regler. Det gælder også, hvis man anvender en databehandler.

Endvidere fremgår det af den vejledende tekst, at Datatilsynet anbefaler, at den dataansvarlige udarbejder og udleverer en medarbejderinstruks til de medarbejdere, der bliver udstyret med kropsbårne kameraer (bodycams). Medarbejderinstruksen skal som minimum indeholde retningslinjer for brug af kropsbårne kameraer (bodycams), herunder hvornår kameraet må aktiveres, oplysningspligt og vejledning om de registreredes rettigheder.

Den dataansvarlige har endvidere en oplysningspligt over for de personer, som fremgår af billed- og lydoptagelser fra kropsbårne kameraer (bodycams). Oplysningspligten kan eksempelvis opfyldes i form af orientering på den dataansvarliges hjemmeside, markering på uniformer, skiltning ved indgange eller andre relevante steder og så vidt muligt i forbindelse med selve billed- og lydoptagelsen.

Den dataansvarlige skal derudover være parat til at iagttage de registreredes rettigheder - det betyder bl.a., at de personer, der optræder på optagelserne, eksempelvis kan have ret til indsigt, sletning, berigtigelse mv.

Det fremgår herudover af den vejledende tekst, at opbevaring af billed- og lydoptagelser fra kropsbårne kameraer (bodycams), som indeholder personoplysninger, skal overholde det grundlæggende princip om opbevaringsbegrænsning, hvilket bl.a. indebærer, at oplysningerne skal slettes, når de ikke længere er nødvendige i forhold til formålet med behandlingen.

Den dataansvarlige skal i øvrigt sikre sig, at anden relevant lovgivning overholdes i forbindelse med behandlingen af billed- og lydoptagelser fra kropsbårne kameraer (bodycams), herunder straffelovens regler om freds- og æreskrænkelser.

Personoplysninger – få et hurtigt overblik

I august 2021 udgav Datatilsynet en kort og letlæselige guide, der opsamler de mest grundlæggende informationer omkring begrebet personoplysninger.

Der er nogle helt grundlæggende forpligtelser, den dataansvarlige skal opfylde, når der behandles personoplysninger. Guiden indeholder derfor også en definition på, hvad en behandling af personoplysninger er, og hvornår den dataansvarlige må behandle personoplysninger.

Guiden findes på Datatilsynets hjemmeside på undersiden "Borger".

Den generelle informationspjece

I august 2021 udgav Datatilsynet en generel informationspjece, der i et grafisk design opsamler en række af de vigtigste informationer om databeskyttelse og databeskyttelsesforordningen.

Pjecen indeholder tre vigtige informationspunkter:

- Generel information om databeskyttelse.
- Vejledning om borgernes rettigheder.
- Information om, hvordan borgeren kan klage til Datatilsynet.

Pjecen findes på Datatilsynets hjemmeside på undersiden "Hvad siger reglerne?"

Udtalelse om offentlige myndigheders brug af interesseafvejningsreglen

Datatilsynet modtog i juli 2021 en henvendelse fra Herning Kommune om bl.a. det retlige grundlag (hjemmel) for behandling af oplysninger om pårørende til ansatte i forbindelse med krisebreve og om oplysningspligten i den henseende.

Ved krisebreve forstås en notits på den ansattes personalesag eller lignende, f.eks. en liste, hvor Herning Kommunes ansatte kan få indført en pårørendes telefonnummer med henblik på, at den pårørende kan kontaktes (af kommunen), hvis der sker et uheld involverende den ansatte.

De oplysninger, som vil blive behandlet om den ansattes pårørende i denne kontekst, kan ikke antages at have en sådan karakter, at oplysningerne vil være omfattet af databeskyttelsesforordningens artikel 9.

Datatilsynet udtalte bl.a., at tilsynet var enige med Herning Kommune i, at kommunen efter omstændighederne vil kunne behandle oplysninger om den pårørendes telefonnummer på grundlag af den pårørendes samtykke, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra a.

Det var imidlertid samtidig Datatilsynets vurdering, hvilket Herning Kommune også havde henvist til, at det vil indebære visse vanskeligheder, herunder at Herning Kommune – i det omfang kommunen forestår indhentelsen af samtykke – skal have et retligt grundlag for at behandle de oplysninger, som er nødvendige for at kunne kontakte den pårørende og bede om vedkommendes samtykke. Endvidere er der den risiko, at den ansatte – såfremt denne forestår indhentelsen af samtykke – aldrig får indhentet (forudgående) samtykke fra sin pårørende, f.eks. fordi det er for besværligt.

Datatilsynet udtalte endvidere, at det er tilsynets opfattelse, at der er et snævert rum for, at offentlige myndigheder kan behandle personoplysninger på grundlag af databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Dette vil være tilfældet, hvor behandlingen ikke vedrører den offentlige myndigheds opgavevaretagelse, men hvor behandlingen ikke desto mindre er nødvendig af hensyn til, at myndigheden kan fungere på en tilfredsstillende og hensigtsmæssig måde, herunder i forhold til den daglige drift af myndigheden, og aktiviteten, som foranlediger behandling af personoplysninger, i øvrigt er både saglig og lovlig for myndigheden at udføre.

Herning Kommunes behandling af oplysninger om kommunens ansattes pårørende var i den foreliggende situation lovlig, saglig og måtte karakterises som en (behandlings)aktivitet, der – uanset at den ikke er nødvendig for kommunens opgavevaretagelse – kunne anses for nødvendig for, at Herning Kommune på en hensigtsmæssig måde kunne fungere som offentlig myndighed, herunder med henblik på at varetage sine ansattes interesser.

Det var således Datatilsynets opfattelse, at Herning Kommunes behandling af oplysninger om kommunens ansattes pårørende i den foreliggende situation vil kunne ske på grundlag af databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Datatilsynet udtalte sig derudover i generelle vendinger om principperne for behandling af personoplysninger i databeskyttelsesforordningens artikel 5 og om oplysningspligten i databeskyttelsesforordningens artikel 14.

Lancering af nyhedsbrev

I september 2021 udsendte Datatilsynet for første gang et nyhedsbrev. Nyhedsbrevet har længe været efterspurgt af omverdenen og udsendes to gange om måneden som et supplement til de andre kanaler, Datatilsynet i forvejen benytter sig af.

I Datatilsynets nyhedsbrev kan man bl.a. finde de senest offentliggjorte afgørelser, nyt vejledningsmateriale, seneste nyt fra Det Europæiske Databeskyttelsesråd, generelle nyheder på databeskyttelsesområder og stillingsopslag fra Datatilsynet m.m. Tilmeldingen foregår via en formular på Datatilsynets hjemmeside.

Ny vejledning om tilsyn med databehandlere

Dataansvarlige, som overlader personoplysninger til eksterne leverandører (såkaldte databehandlere), skal føre et passende tilsyn med, om deres databehandlere overholder databeskyttelsesreglerne.

I oktober 2021 offentliggjorde Datatilsynet en ny praktisk anvendelig vejledning om, hvordan de dataansvarlige kan føre sådanne tilsyn.

Vejledningen indeholder en vejledende model med en simpel pointskala, som giver de dataansvarlige en indikation af, hvor risikofyldt behandlingen af personoplysninger er. I tilknytning hertil er der seks tilsynskoncepter, som de dataansvarlige kan vælge imellem afhængigt af antallet af point.

Koncepterne stiller gradvis større og større krav til de dataansvarliges gennemførelse af tilsynene. Større risiko giver flere point, og flere point betyder, at der stilles flere krav til de dataansvarliges tilsyn med deres databehandlere.

I vejledningen er der en række praktiske eksempler, som illustrerer pointtælling og brug af tilsynskoncepterne.

Vejledningen er bl.a. lavet på baggrund af efterspørgsel fra Datatilsynets interessenter, som tilsynet også har inddraget løbende i forbindelse med udarbejdelsen.

Brug af personoplysninger i testøjemed

Datatilsynet udgav i oktober 2021 endvidere en ny vejledende tekst om hvordan og hvornår, virksomheder og myndigheder kan bruge personoplysninger til test af it-systemer.

Det fremgår af den vejledende tekst, at Datatilsynet anerkender, at det efter omstændighederne kan være velbegrundet og nødvendigt at bruge personoplysninger ved udvikling og test af it-systemer.

I den vejledende tekst er beskrevet, hvornår virksomheder og myndigheder må bruge personoplysninger til test af it-systemer, og hvilke rettigheder og pligter, de bør have styr på i den forbindelse. Teksten inkluderer også nogle af de sikkerhedsmæssige overvejelser, som er vigtige at have for øje.

Vejledende tekst om dataansvaret mellem private leverandører og offentlige myndigheder

Datatilsynet får løbende spørgsmål om placeringen af dataansvaret, når private leverandører udfører opgaver eller leverer ydelser til offentlige myndigheder.

I Datatilsynets og Justitsministeriets vejledning om dataansvarlige og databehandlere fra november 2017 redegøres nærmere for de forskellige begreber, og hvad man kan lægge vægt på, når man skal vurdere, om man er dataansvarlig eller databehandler.

Som supplement til den generelle vejledning offentliggjorde Datatilsynet i november 2021 en vejledende tekst om rollefordelingen, når private er leverandører til det offentlige.

Den vejledende tekst indeholder en række eksempler, herunder rollefordelingen i forbindelse med indsamling af affald, brug af personlighedstests og brug af selvstændige konsulenter, og er udarbejdet efter inddragelse af relevante interessenter.

Oprettelse af nyt specialudvalg

Datatilsynet har i slutningen af 2021 nedsat et nyt specialudvalg om det internationale databeskyttelsessamarbejde.

Med databeskyttelsesforordningen har det internationale samarbejde fået en ny og større betydning. Databeskyttelsesområdet er via databeskyttelsesforordningen i langt højere grad reguleret på EU-niveau, ligesom der med forordningen er etableret et mere formaliseret samarbejde mellem tilsynsmyndighederne i Europa.

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. Det gælder både på det generelle plan i form af bl.a. vejledninger og udtalelser og på det konkrete plan i forhold til afgørelser i konkrete sager.

Specialudvalget er nedsat med det formål at give Datatilsynets interessenter et bedre indblik i det internationale databeskyttelsesarbejde samt en mulighed for at bidrage til dette arbejde og dermed styrke tilsynets varetagelse af danske interesser i det internationale samarbejde.

Specialudvalget vil fungere som et supplement til Datatilsynets øvrige interessentinddragelse. Medlemmerne af udvalget er udpeget af Datatilsynet og består af bl.a. flere offentlige myndigheder og interesseorganisationer.

I specialudvalget vil der være en fast dialog mellem Datatilsynet og udvalgsmedlemmerne fire gange om året, som skal sikre vidensdeling og inddragelse i tilsynets internationale arbejde.

Samtidig skal de faste specialudvalgsmøder sikre, at Datatilsynet får løbende indsigt i, hvilke konkrete problemstillinger der rører sig i samfundet, og som kan være relevante at inddrage i det internationale arbejde, herunder eksempelvis udarbejdelse af vejledninger fra Det Europæiske Databeskyttelsesråd.

Det første møde i specialudvalget blev afholdt i januar 2022.

Man kan læse mere om specialudvalget på Datatilsynets hjemmeside på undersiden "Specialudvalg om det internationale databeskyttelsessamarbejde".

Tjekliste til vuggestuer og børnehaver ved brug af billeder og video

Datatilsynet offentliggjorde i december 2021 en tjekliste, som skal hjælpe børnehaver og vuggestuer med at overholde databeskyttelsesreglerne, når de bruger billeder og video af børn og medarbejdere. Tjeklisten er opbygget som en kvikguide og indeholder en række gode råd bl.a. om, hvordan institutionerne passer på billeder, og hvor længe billeder må ligge på intranettet.

Eksempler i tjeklisten illustrerer, hvad billeder af børn og medarbejdere må bruges til, herunder om det er nødvendigt med samtykke. Tjeklisten indeholder også et bilag med forklaring af databeskyttelsesreglerne.

Kommunernes Landsforening og Landsorganisationen Danske Daginstitutioner har været inddraget under udarbejdelsen for at sikre, at tjeklisten dækker behovet hos deres medlemmer.

Nye fælleseuropæiske vejledninger

Det Europæiske Databeskyttelsesråd (EDPB) har i 2021 vedtaget en række vejledninger mv. om aktuelle databeskyttelsesretlige emner:

Vejledende tekst om opbevaring af betalingskortoplysninger i forbindelse med online køb

EDPB vedtog i maj 2021 en vejledende tekst om det retlige grundlag i databeskyttelsesforordningen for at opbevare betalingskortoplysninger (kortnummer og udløbsdato) med det formål at facilitere og lette fremtidige online-køb.

Den vejledende tekst gennemgår de forskellige behandlingsgrundlag i databeskyttelsesforordningens artikel 6 og konklusionen er, at samtykke fra den registrerede (forbrugeren) forekommer som det eneste mulige lovlige grundlag for behandlingen, når der opbevares betalingskortoplysninger for at muliggøre og lette fremtidige online-køb.

Den vejledende tekst fra EDPB er i øvrigt i tråd med Forbrugerombudsmandens retningslinjer for betalingsmodtageres håndtering af betalinger ved fjernsalg.

Vejledning om eksempler på brud på persondatasikkerheden

EDPB vedtog i december 2021 en vejledning om eksempler på brud på persondatasikkerheden. Datatilsynet har deltaget indgående i arbejdet med denne vejledning, og de beskrevne eksempler er alle af praktisk relevans for danske dataansvarlige.

Vejledningen gennemgår typeeksempler af brud på persondatasikkerheden. Der er fokus på de risici de enkelte typetilfælde indeholder, både i forhold til den risikovurdering behandlingen giver anledning til og de sikkerhedsforanstaltninger, der er indført.

Vejledningen giver konkrete anvisninger på forståelsen af – særligt to – praktiske udfordringer for de dataansvarlige. Den nedre "bagatelgrænse" for, hvornår et brud skal anmeldes, og de situationer, hvor et brud udgør en høj risiko for de registrerede, og der skal ske underretning af disse.

Der er særlige eksempler om ransomware, eksfiltrering af data, menneskelige fejl og tabte dokumenter eller filer.

Vejledningen har for hvert eksempelområde også en beskrivelse af, hvilke mitigerende foranstaltninger en dataansvarlig kan benytte for at forebygge brud.

Vejledning om stemmestyrede assistenter

EDPB vedtog i marts 2021 en vejledning om stemmestyrede assistenter. Vejledningen blev herefter sendt i offentlig høring, og i juli 2021 vedtog EDPB vejledningen endeligt.

Stemmestyrede assistenter, som er den funktionalitet, hvor forbrugselektronik – udstyret med en mikrofon – kan betjenes via stemmekommandoer, har de senere år fundet vej til flere og flere elektroniske produkter. Der er væsentlige databeskyttelsesretlige overvejelser forbundet med teknologien, bl.a. i forhold til den relativt indgribende videregivelse af al lyd i omgivelserne, behandlingsgrundlag, opbevaring af data, brugen af kunstig intelligens og de registreredes rettigheder.

Vejledningen gennemgår bl.a. de databeskyttelsesretlige regler på området og retter sig primært til de professionelle aktører, der benytter de pågældende teknologier. Vejledningen slår endvidere fast, at det ofte vil være tilfældet, at produktudvikling af og brug af de pågældende teknologier i et nyt produkt udløser pligten for den dataansvarlige til at lave en konsekvensanalyse.

Vejledning om begreberne dataansvarlig og databehandler

I september 2020 vedtog EDPB endvidere en vejledning om dataansvarlige og databehandlere. Vejledningen blev herefter sendt i offentlig høring, og i juli 2021 vedtog EDPB vejledningen endeligt.

Vejledningen har til formål at forklare, hvad der skal forstås ved begreberne dataansvarlig og databehandler i databeskyttelsesforordningen, og hvordan disse begreber skal afgrænses i forhold til hinanden. Det er vigtigt, at man kender sin rolle, når man behandler personoplysninger, da kravene til en dataansvarlig og en databehandler er forskellige.

Vejledningen er henvendt til praktikere og indeholder derfor en lang række eksempler, som i en praktisk kontekst skal illustrere, hvordan man konkret fastlægger rollefordelingen mellem de involverede parter, og hvilke konsekvenser det indebærer.

Der er tale om en opdatering af den tidligere gældende vejledning fra 2010. Den nye vejledning tager – i modsætning til den tidligere vejledning – sit udgangspunkt i databeskyttelsesforordningen, som introducerede nye bestemmelser om bl.a. databehandleres forpligtelser. Derudover tager den nye vejledning også højde for EU-Domstolens seneste praksis om fælles dataansvar.

Målrettet markedsføring ("targeting") på sociale medier

EDPB vedtog i september 2020 en vejledning om målrettet markedsføring – såkaldt "targeting". Vejledningen blev herefter sendt i offentlig høring, og i april 2021 vedtog EDPB vejledningen endeligt. Targeting er en hyppigt anvendt markedsføringsmekanisme for udbydere af sociale medier og især på platforme, som brugerne kan benytte gratis.

Targeting adskiller sig fra mere traditionelle markedsføringsmetoder i sin målrettethed, der bevirker, at personer eller selskaber har mulighed for at kommunikere specifikke meddelelser og relevant indhold direkte til brugerne. Targeting af brugerne sker på baggrund af en lang række forskellige kriterier, som udvikles på baggrund af oplysninger om brugerne, som disse selv har delt. Dette kan f.eks. være en oplysning om brugerens civilstand. Targeting benyttes bl.a. i reklame- og markedsføringsøjemed og til at fremme kulturelle og politiske interesser.

Formålet med vejledningen er først og fremmest at klarlægge rollerne og ansvaret ved behandling af personoplysninger i forbindelse med målrettet markedsføring mod brugere af sociale medier. Det er således i særdeleshed dataansvarlige og databehandlere, der benytter sig af targeting, som vejledningen er relevant for. Vejledningen forsøger endvidere at identificere de risici, der er for registreredes fundamentale rettigheder og frihedsrettigheder.

Vejledning om brug af adfærdskodekser som overførselsgrundlag

EDPB vedtog i juli 2021 en vejledning om brugen af adfærdskodekser som overførselsgrundlag. Vejledningen er efterfølgende sendt i offentlig høring, og det er forventningen, at vejledningen vil blive endeligt vedtaget i 2022.

Ved overførsel af personoplysninger til tredjelande finder reglerne i databeskyttelsesforordningens kapitel V anvendelse. Det indebærer bl.a., at man ved overførsel af personoplysninger til tredjelande skal sørge for at have et overførselsgrundlag. Kapitel V i databeskyttelsesforordningen angiver forskellige mulige overførselsgrundlag, herunder bl.a. muligheden for anvendelsen af adfærdskodekser som overførselsgrundlag.

Der er tale om adfærdskodekser, som er særligt godkendt med henblik på at kunne anvendes som overførselsgrundlag.

Vejledningen fra EDPB har til formål at præcisere anvendelsen af adfærdskodekser som overførselsgrundlag. Vejledningen sigter også mod at give praktisk vejledning om indholdet af sådanne adfærdskodekser, deres vedtagelsesproces samt de krav og garantier, som adfærdskodekserne skal opfylde. Vejledningen skal ligeledes give større gennemsigtighed og sikre, at kodeejere, som ønsker at søge godkendelse af et adfærdskodeks til brug for overførsel af personoplysninger til tredjelande, får kendskab til processen og forstår de formelle krav til et sådant adfærdskodeks.

Vejledningen supplerer EDPB's vejledning fra 2019 om adfærdskodekser og overvågning, som fastlægger de generelle rammer for vedtagelsen af adfærdskodekser.

Vejledning om samspillet mellem databeskyttelsesforordningens artikel 3 og kapitel V

EDPB vedtog i november 2021 en vejledning om samspillet mellem databeskyttelsesforordningens artikel 3 om forordningens territoriale (geografiske) område og kapitel V (artikel 44-50) om overførsler af personoplysninger til tredjelande eller internationale organisationer. Vejledningen er efterfølgende sendt i offentlig høring, og det er forventningen, at vejledningen vil blive endeligt vedtaget i 2022.

Vejledningen sigter mod at bistå dataansvarlige og databehandlere i EU med at identificere, om en behandling udgør en overførsel til et tredjeland eller til en international organisation, og dermed om bestemmelserne i kapitel V i databeskyttelsesforordningen finder anvendelse.

Vejledningen giver en definition af begrebet "overførsel" ved at opstille tre kriterier, som alle tre skal være overholdt, for at der er tale om en overførsel til et tredjeland. Begrebet "overførsel" er væsentligt for at fastlægge, hvornår reglerne i kapitel V i databeskyttelsesforordningen finder anvendelse, samt hvornår man skal efterleve anbefalingerne om supplerende foranstaltninger, der er udarbejdet på baggrund af Schrems II-sagen.

Det følger også af vejledningen, at hvis en behandling ikke opfylder de tre kriterier, vil der ikke være tale om en overførsel i henhold til kapitel V i databeskyttelsesforordningen. Det Europæiske Databeskyttelsesråd understreger dog i vejledningen, at selvom en behandling ikke udgør en overførsel til et tredjeland, kan den stadig være forbundet med risici, som kan kræve iværksættelse af sikkerhedsforanstaltninger. I den forbindelse minder Det Europæiske Databeskyttelsesråd om, at dataansvarlige og databehandlere altid skal overholde alle relevante bestemmelser i databeskyttelsesforordningen, uanset om behandlingen finder sted i EU eller ej.

Vejledningen indeholder en række eksempler, som illustrerer anvendelsen af ovennævnte kriterier.

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 **730** sager i 2021 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 logning

I september 2021 sendte Justitsministeriet et lovforslag i høring om revision af de gældende logningsregler.

Formålet med lovforslaget var at bringe de gældende logningsregler i overensstemmelse med EU-retten. EU-Domstolen har således i en række afgørelser behandlet spørgsmålet om, under hvilke omstændigheder teleselskaber kan pålægges at registrere og opbevare (logge) samt udlevere oplysninger om teletrafik.

Justitsministeriet lagde på den baggrund i lovforslaget op til både at ændre reglerne om, hvornår teleudbydere er forpligtede til at logge oplysninger om teletrafik, og reglerne om politiets og anklagemyndighedens adgang til de pågældende oplysninger.

Det fremgik bl.a. af lovforslaget, at oplysninger logget med det formål at beskytte den nationale sikkerhed ville kunne videregives til brug for politiets og anklagemyndighedens efterforskning af grov kriminalitet. Dette blev i lovforslaget vurderet til at være forbundet med en væsentlig procesrisiko, idet EU-Domstolen i sin praksis havde fastslået, at adgangen til sådanne data i princippet kun kunne begrundes med et mindst lige så tungtvejende formål som dét, der havde begrundet selve logningsforpligtelsen.

EU-Domstolen havde dog ikke eksplicit taget stilling til den situation, hvor oplysninger lagret af hensyn til den nationale sikkerhed blev videregivet til brug for bekæmpelse af grov kriminalitet.

I sit høringssvar bemærkede Datatilsynet generelt, at de foreslåede regler måtte forventes at indebære behandling af store mængder personoplysninger. Reglerne burde derfor efter Datatilsynets opfattelse kun indføres, hvis vægtige samfundsmæssige hensyn talte for det, hvilket måtte bero på en politisk vurdering.

For så vidt angik reglerne om politiets og anklagemyndighedens adgang til loggede oplysninger bemærkede Datatilsynet bl.a., at princippet om formålsbegrænsning i databeskyttelsesforordningen indebærer, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål.

På den baggrund opfordrede Datatilsynet til, at det i lovforslaget så vidt muligt blev uddybet, hvorfor teleudbyderes videregivelse af loggede oplysninger til politiet vurderedes at være i overensstemmelse med princippet om formålsbegrænsning i de tilfælde, hvor oplysningerne er logget med henblik på at beskytte den nationale sikkerhed, men videregives til brug for bekæmpelse af grov kriminalitet.

Automatisk nummerpladegenkendelse (ANPG)

Justitsministeriet og Rigspolitiet underrettede i februar 2021 Datatilsynet om en forestående udvidelse af politiets anvendelse af automatisk nummerpladegenkendelse (ANPG), som bl.a. havde baggrund i regeringens udspil fra 2019 om tryghed og sikkerhed i det offentlige rum.

Justitsministeriet forelagde i den forbindelse et foreløbigt udkast til ændring af den såkaldte ANPG-bekendtgørelse for Datatilsynet, ligesom Rigspolitiet – i overensstemmelse med retshåndhævelsesloven – havde udarbejdet en konsekvensanalyse.

Sagen blev forelagt for Datarådet i april 2021, og Datatilsynet afgav på den baggrund en række bemærkninger til Justitsministeriet og Rigspolitiet.

I november 2021 sendte Justitsministeriet et udkast til bekendtgørelse i offentlig høring om ændring af ANPG-bekendtgørelsen.

ANPG er et intelligent system med nummerpladescannere, som kan alarmere politiet, hvis et køretøj passerer et kamera. Nummerpladeoplysningerne kan herefter dels søges i relevante databaser, dels lagres med oplysninger om position samt data og tidspunkt vedrørende optagelsen. ANPG blev taget i brug i alle landets politikredse i slutningen af 2016.

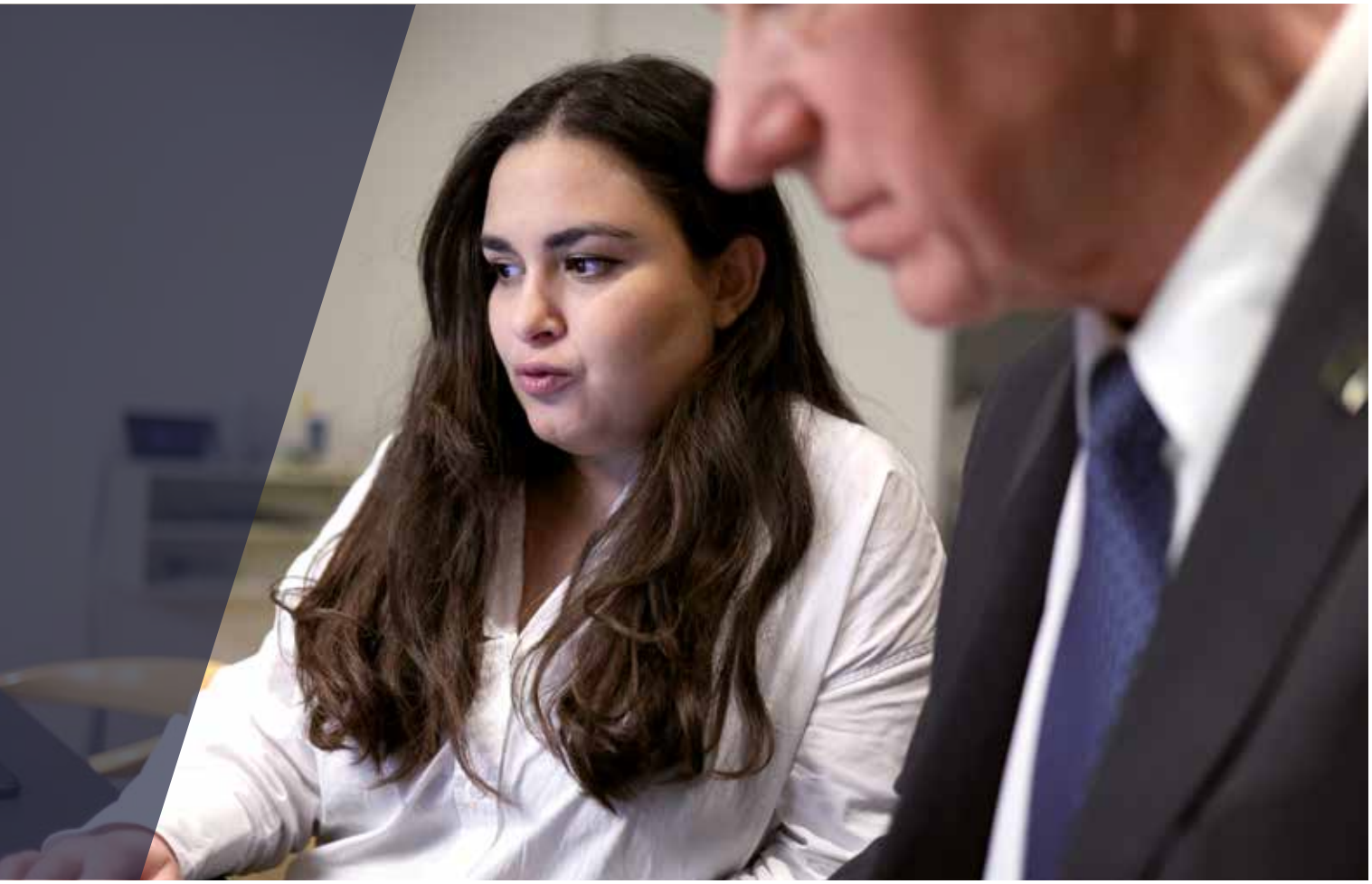
Indsamling af ANPG-oplysninger kan ske ved brug af enten stationært eller mobilt udstyr. Oplysninger om køretøjer, der er registreret på en såkaldt hotliste, opbevares i ANPG-systemets hit-del, mens oplysninger om andre køretøjer opbevares i en no hit-del.

Udkastet til ændringsbekendtgørelse lagde bl.a. op til at erstatte det gældende krav om en målrettet politiindsats for indsamlingen af oplysninger om no-hits ved hjælp af stationært udstyr med et krav om, at indsamlingen skal understøtte et eller flere strategiske indsatsområder i politiet, hvor anvendelsen af ANPG vurderes at være af væsentlig betydning.

Udkastet til ændringsbekendtgørelse lagde endvidere op til at udvide den generelle frist for at slette oplysninger om no-hits i ANPG-systemet fra 30 til 60 dage.

Sagen blev forelagt for Datarådet i december 2021, og Datatilsynet udtalte på den baggrund, at udkastet til ændringsbekendtgørelse ikke gav anledning til bemærkninger.

Datatilsynet opfordrede dog til, at der fastsættes nærmere retningslinjer for politiets indsamling af oplysninger om no-hits ved brug af stationært udstyr, herunder navnlig hvordan kravet om, at indsamlingen skal understøtte et eller flere strategiske indsatsområder i politiet, hvor ANPG vurderes at være af væsentlig betydning, vil blive anvendt i praksis.



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 2021 indgivet 10 politianmeldelser med indstilling om bøde efter databeskyttelsesforordningen. 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 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.

I januar 2021 udgav Datatilsynet endvidere en bødevejledning, som opstiller en model for beregning af bøder til virksomheder. I september 2021 udgav tilsynet ligeledes en vejledning vedrørende udmåling af bøder til fysiske personer, som i højere grad baserer sig på standardiserede bøder.

Begge vejledninger tager udgangspunkt i den erfaring tilsynet har opnået gennem vurderingen af sager de første år efter den 25. maj 2018, og i den erfaring der er gjort hos de øvrige europæiske tilsynsmyndigheder. Vejledningerne er endvidere arbejdsdokumenter, der løbende vil blive udbygget efterhånden som Datatilsynet, anklagemyndigheden og domstolene håndterer flere straffesager på området, og i takt med at praksis, såvel nationalt som i EU, udvikles.

Datatilsynet har 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 findes 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 beskyt-

telse 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.

"One stop shop"-mekanismen

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.

I afsnittet følger en række eksempler på klagesager, som Datatilsynet i 2021 traf afgørelse i:

Det Konservative Folkepartis manglende opfyldelse af oplysningspligten

Efter en række konkrete henvendelser i 2019 blev Datatilsynet opmærksom på Det Konservative Folkepartis behandling af personoplysninger i forbindelse med udsendelse af breve til udvalgte husstande angående valget til Europa-Parlamentet og folketingsvalget samme år.

Efter databeskyttelsesforordningens artikel 14 skal den dataansvarlige give den registrerede en række oplysninger, når den dataansvarlige indsamler oplysninger om den registrerede hos andre end den registrerede. Den dataansvarlige skal give oplysningerne til den registrerede af egen drift. Den registrerede har derfor krav på oplysningerne, selvom at den registrerede ikke har anmodet herom.

Den dataansvarlige kan undlade at opfylde oplysningspligten, hvis en af undtagelserne i forordningens artikel 14 eller databeskyttelseslovens § 22 finder anvendelse.

Det Konservative Folkeparti gjorde gældende, at opfyldelse af oplysningspligten kunne undlades med hjemmel i undtagelsen i databeskyttelsesforordningens artikel 14, stk. 5, litra c, ud fra den betragtning, at indsamlingen af navn og adresse med henblik på afsendelse af et brev, udgør en udtrykkelig fastsat rettighed efter dansk praksis, som ikke tilsidesætter hensynet til den registrerede (brevmodtageren).

Efter Datatilsynets opfattelse fandt forordningens artikel 14, stk. 5, litra c, ikke anvendelse. Endvidere fandt Datatilsynet, at der i øvrigt ikke var hjemmel til at undlade at opfylde oplysningspligten i hverken artikel 14 eller i databeskyttelseslovens § 22.

Datatilsynet fandt derfor, at Det Konservative Folkeparti ikke havde opfyldt sin oplysningspligt efter databeskyttelsesforordningens artikel 14 og udtalte kritik af partiet.

Regionale lægevagters optagelse af telefonsamtaler

Datatilsynet traf afgørelse i en sag, hvor en borger bl.a. klagede over, at Lægevagten Region Syddanmark havde optaget telefonsamtaler mellem hende og lægevagten, og at lægevagten efterfølgende afviste at slette telefonoptagelserne.

Under sagen kom det frem, at den pågældende lægevagt havde optaget og gemt ca. 7,5 millioner samtaler siden januar 2013.

Lægevagten var af den opfattelse, at optagelse af telefonsamtaler med borgere var materiale, som skulle anses for at udgøre en del af en patientjournal og derfor skulle opbevares i overensstemmelse med de regler, der gælder for opbevaring af oplysninger indeholdt i patientjournaler (som udgangspunkt 10 år efter sidste patientkontakt).

Efter sagen havde været forelagt Datarådet fandt Datatilsynet – bl.a. efter at have forelagt spørgsmålet for Sundheds- og Ældreministeriet – at optagelse af telefonsamtaler med lægevagten ikke kan anses for at være en del af en patientjournal. Spørgsmålet om, hvor længe lægevagten kunne opbevare optagelserne, skulle derfor i stedet afgøres efter de almindelige databeskyttelsesretlige regler.

Datatilsynet fandt, at en opbevaringsperiode på op til fem år ville være i overensstemmelse med databeskyttelsesreglerne. Datatilsynet lagde vægt på, at formålet med optagelse af telefonsamtaler hos lægevagten er at sikre dokumentation til brug for eventuelle klager over sundhedsfaglig behandling, og at der efter lov om klage- og erstatningsadgang inden for sundhedsvæsenet er mulighed for at klage op til fem år efter den dag, hvor klageforholdet fandt sted.

Datatilsynet udtalte på den baggrund alvorlig kritik af, at lægevagten havde opbevaret optagelser af telefonsamtaler, som var mere end fem år gamle, og meddelte lægevagten påbud om at slette alle optagelser af telefonsamtaler, som var mere end fem år gamle.

Offentliggørelse af personnummer på kommunal hjemmeside

Datatilsynet traf afgørelse i en sag, hvor en borger klagede til tilsynet over, at Vejen Kommune havde offentliggjort oplysninger om borgerens personnummer på kommunens hjemmeside.

Offentliggørelsen af borgerens personnummer skete i forbindelse med, at Vejen Kommune skulle publicere et høringssvar på kommunens hjemmeside, som var indsendt af borgeren via digital post. I den forbindelse kom Vejen Kommune ved en fejl til at offentliggøre borgerens personnummer, som fremgik af signaturbeviset. Kommunen havde ikke processer for kontrol inden offentliggørelse af materiale på kommunens hjemmeside, men havde derimod et screeningsværktøj, der havde til opgave at identificere personnumre, efter materialet var blevet gjort tilgængeligt på kommunens hjemmeside.

Datatilsynet fandt – efter at sagen havde været forelagt Datarådet – at det følger af kravet om passende sikkerhed, at offentlige myndigheder, der modtager eller udarbejder materiale med henblik på offentliggørelse, og hvor materialet ofte indeholder personoplysninger, eksempelvis vedhæftet eller i form af metadata, skal gennemføre kontrolforanstaltninger med henblik på at undgå utilsigtet offentliggørelse af personoplysninger.

Sådanne kontrolforanstaltninger indebærer efter Datatilsynets opfattelse som minimum en forudgående proces for at gennemgå materialet og alt efter personoplysningernes karakter og omfang vil det

normalt også være en passende sikkerhedsforanstaltning at gennemføre en supplerende forudgående manuel eller teknisk kontrol af, om oplysningerne rent faktisk er blevet slettet eller anonymiseret som tiltænkt.

Datatilsynet fandt herefter grundlag for at udtale kritik af, at Vejen Kommunes behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1, idet kommunen ikke havde gennemført passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau.

Offentliggørelse af festbilleder af børn og unge

Datatilsynet traf afgørelse i en sag om Epic Bookings offentliggørelse af billeder på Epic Bookings Facebookside. Der var tale om en sag, som tilsynet havde taget op på eget initiativ.

Et omfattende antal billeder - knap 500.000 - af navnlig børn og unge var at finde på virksomhedens facebookside. Billederne, som var fra 2013 og frem, var taget til fester og lignende arrangementer primært ved brug af et selfiekamera.

Efter at sagen havde været forelagt Datarådet, udtalte Datatilsynet alvorlig kritik af, at Epic Bookings offentliggørelse af billeder på virksomhedens facebookside var i strid med databeskyttelsesforordningens artikel 6, stk. 1, litra a, da der ikke var indhentet et gyldigt samtykke fra de registrerede, jf. artikel 4, nr. 11.

Endvidere udtalte Datatilsynet alvorlig kritik af, at indholdet i den informationstekst, der var opsat i en nærmere afgrænset zone ved og foran selfiekameraet, og at det "speak", som blev givet ved et arrangement, ikke levede op til kravene i databeskyttelsesforordningens artikel 12, stk. 1, og artikel 13, stk. 1 og 2.

Yderligere udtalte Datatilsynet alvorlig kritik af, at offentliggørelse uden tidsbegrænsning var i strid med princippet om opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra e.

Datatilsynet meddelte Epic Booking påbud om at slette alle billeder fra Epic Bookings facebookside, som var behandlet uden gyldigt samtykke og påbud om at fastsætte en generel frist på maksimalt 60 dage for sletning af billeder, som fremover ville blive offentliggjort af Epic Booking på Epic Bookings facebookside.

Tilsynet lagde vægt på, at de registrerede på tidspunktet for afgivelse af deres samtykke ikke havde haft mulighed for at til- eller fravælge de forskellige behandlingsformål, hvilket ikke er i overensstemmelse med databeskyttelsesreglernes krav til et gyldigt samtykke. De registrerede havde således ikke haft mulighed for at træffe et informeret valg, ligesom de ikke havde haft reel kontrol over behandlingen af oplysninger om dem selv. Tilsynet lagde endvidere vægt på, at det af den anvendte samtykketekst (informationsteksten) ikke fremgik, hvad formålene med behandlingen var, herunder at billederne også ville blive behandlet til markedsføringsmæssige formål.

Oplysningsteksten indeholdt endvidere ikke oplysning om tidsrummet for offentliggørelsen af billederne på facebooksiden.

I forhold til fastsættelse af den generelle frist for sletning lagde tilsynet vægt på hensynet til de afbillede personer, herunder den særlige beskyttelse som børn og unge nyder efter databeskyttelsesreglerne, samt behandlingens karakter i form af offentliggørelse. Endvidere lagde tilsynet vægt på, at en frist på maksimalt 60 dage efter tilsynets opfattelse ville være tilstrækkelig til at opfylde kundernes behov for at kunne tilgå billederne.

Videregivelse af kunders personnumre i forbindelse med salg af fordringer

Datatilsynet traf afgørelse i en sag, hvor Nordea Danmark (Nordea) videregav oplysninger om bankens kunder i forbindelse med et salg af fordringer til det luxembourgske selskab Ultimo Portfolio S.A. (UPI). Under sagen kom det bl.a. frem, at Nordea havde videregivet personnumre om bankens kunder i forbindelse med salget.

Efter en gennemgang af sagen, hvor Datatilsynet bl.a. indhentede udtalelser fra Skattestyrelsen, fandt tilsynet, at Nordeas videregivelse af sine kunders personnumre og andre personoplysninger var sket inden for rammerne af de databeskyttelsesretlige regler.

Datatilsynet lagde bl.a. vægt på, at Nordea i medfør af skatteindberetningslovens regler var forpligtet til at videregive identifikationsoplysninger om deres kunder i forbindelse med salget af fordringer. For så vidt angik videregivelsen af kundernes personnumre, var det afgørende, at UPI – som erhvervende kreditor af fordringerne – fik mulighed for at iagttage sin indberetningspligt efter skatteindberetningsloven.

På den baggrund fandt Datatilsynet, at Nordea var pålagt en retlig forpligtelse til at videregive sine kunders personoplysninger, og at behandlingen derfor kunne ske efter databeskyttelsesforordningens artikel 6, stk. 1, litra c, jf. skatteindberetningslovens § 13, stk. 2, og § 52, stk. 1.

Endvidere fandtes Nordea at have hjemmel til at videregive sine kunders personnumre ved salget af fordringer i medfør af databeskyttelseslovens § 11, stk. 2, nr. 1, jf. skatteindberetningslovens § 13, stk. 2, og § 52, stk. 1.

Erhvervsstyrelsens optagelse af telefonsamtaler

Datatilsynet traf afgørelse i en sag, hvor en borger klagede over, at Erhvervsstyrelsen havde optaget en telefonsamtale mellem ham og styrelsen uden først at have indhentet et samtykke hertil.

Under sagen kom det frem, at Erhvervsstyrelsen siden den 1. juni 2018 havde optaget samtlige indgående telefonopkald til styrelsens kundecenter. Optagelserne blev foretaget med det formål at have dokumentation ved indgivelse af politianmeldelse med henblik på at beskytte medarbejderne i styrelsens kundecenter mod trusler mv. og til brug for oplæring samt løbende uddannelse af kundecenterets medarbejdere af hensyn til myndighedens vejledningspligt.

Datatilsynet fandt – efter at sagen havde været forelagt Datarådet – at Erhvervsstyrelsens generelle praksis, hvorefter der uden undtagelse skete optagelse af telefonsamtaler med borgere, virksomheder mv., som ringede ind til styrelsen for råd og vejledning, ikke kunne anses for nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.

Datatilsynet lagde i den forbindelse vægt på, at det – bl.a. henset til Erhvervsstyrelsens myndighedsopgaver – måtte antages at have undtagelsens karakter, at borgere og virksomheder ringede ind og truede styrelsens medarbejdere i en sådan grad, at styrelsen ville foretage politianmeldelse.

Datatilsynet fandt endvidere, at Erhvervsstyrelsens optagelse af telefonsamtaler til brug for kvalitets- og uddannelsesmæssige formål kun kunne ske på baggrund af et samtykke fra de registrerede.

Datatilsynet udtalte på den baggrund alvorlig kritik af Erhvervsstyrelsens behandling af personoplysninger i forbindelse med optagelse af telefonsamtaler.

Brugen af Chromebooks i folkeskolens undervisning

På baggrund af klager fra forældre og indberettede brud på persondatasikkerheden fra flere kommuner tog Datatilsynet en sag op af egen drift om brug af Google Chromebooks i folkeskolens undervisning.

Datatilsynet traf i 2021 afgørelse i den første af de underliggende konkrete sager. Sagen vedrørte brugen af Google Chromebooks i folkeskoler i Helsingør Kommune.

I afgørelsen konstaterede Datatilsynet, at folkeskoleloven generelt giver kommunerne ret til at vælge det it-udstyr og de programmer, der skal bruges i undervisningen. Det påhviler i den forbindelse kommunen som dataansvarlig at sikre, at it-udstyret og programmerne bliver brugt på en sådan måde, at databeskyttelsesreglerne overholdes. Særligt at de udførte behandlinger ikke går ud over det formål, folkeskoleloven foreskriver. Datatilsynet nævnte som eksempel på et sådan formål videregivelse, hvor oplysninger bruges til markedsføring eller profilering af ydelser.

I den konkrete sag havde kommunen efter Datatilsynets opfattelse ikke foretaget de fornødne vurderinger af risikoen for de registreredes rettigheder.

Datatilsynet udtalte, at det for dele af brugeroprettelsen til Chromebook og brugen af G-Suite er nødvendigt at konfigurere adgangen til applikationerne og måden, de fungerer på, for at disse kan benyttes lovligt.

Da kommunen ikke havde vurderet dette, havde kommunen heller ikke dokumentation for, at konfiguration var sket på en måde, der passede til de risici, der var for de registrerede.

Datatilsynet konstaterede, at de manglende vurderinger førte til flere overtrædelser af forordningen. Datatilsynet gav derfor Helsingør Kommune et påbud om at bringe behandlingen af oplysninger i overensstemmelse med forordningen. Hvis kommunen ikke kunne nedbringe risikoen ved behandlingerne, fik kommunen pålagt en begrænsning, der gør, at kommunen ikke må behandle de pågældende oplysninger efter en given frist.

Herudover udtalte tilsynet alvorlig kritik af kommunens behandlinger. Tilsynet gav også Helsingør kommune en advarsel om, at brug af tillægsprodukter til G-Suite ikke ville kunne behandles lovligt uden en foretaget konsekvensanalyse, hvor risici ved behandlingen var nedbragt til mindre end en høj risiko for de registreredes rettigheder og frihedsrettigheder.

Indsigt i et forsikringsselskabs overvågningsmateriale

I 2021 traf Datatilsynet afgørelse i en konkret sag, hvor If Skadeforsikring havde nægtet at give en tidligere kunde indsigt i overvågningsmateriale med henvisning til, at kunden ville bruge materialet i forbindelse med en mulig retssag mod forsikringsselskabet.

I sagen anmodede et advokatselskab på vegne af en borger om indsigt i oplysninger om borgeren, som If Skadeforsikring havde indsamlet i forbindelse med overvågning af den pågældende borger.

If Skadeforsikring afviste at udlevere overvågningsmaterialet bestående af observationsrapporter, fotos og videoer, fordi der forelå afgørende hensyn til *dels* forsikringsselskabets egne interesser i at kunne forsvare sig mod en mulig efterfølgende retssag, og *dels* politiets mulighed for at efterforske en potentiel alvorlig lovovertrædelse, som borgerens ret til indsigt måtte vige for.

Datatilsynet fandt, at If Skadeforsikring i den konkrete sag ikke havde påvist afgørende hensyn, som borgerens ret til indsigt burde vige for. De oplysninger, som var indsamlet om kunden i forbindelse med den iværksatte overvågning, fandtes ikke at have et indhold, der kunne medføre en nærliggende fare for, at private interesser ville lide skade af væsentlig betydning. Det forhold, at de indsamlede personoplysninger med stor sandsynlighed ville kunne inddrages i forbindelse med en eventuel retstvist, udgjorde ikke et så afgørende hensyn til forsikringsselskabets interesser, at oplysningerne, som var indsamlet om klager i forbindelse med overvågningen, kunne undtages fra retten til indsigt.

Datatilsynet bemærkede, at indsigtsretten netop har til formål at give registrerede adgang til at kontrollere oplysningernes rigtighed og behandlingens lovlighed, og undtagelser hertil derfor forudsætter, at der konkret foreligger aktuelle afgørende hensyn, som den registreredes ret til indsigt findes at burde vige for.

Endvidere lagde Datatilsynet vægt på, at der ikke forelå en risiko for, at politiets efterforskning kunne forstyrres, idet If Skadeforsikring allerede havde indgivet anmeldelse til politiet – og dermed udleveret overvågningsmaterialet til politiet – da forsikringsselskabet afviste at give borgeren indsigt i de pågældende oplysninger.

Foreningers behandling af personoplysninger på private computere og e-mailkonti

Datatilsynet traf afgørelse i en sag vedrørende Dansk Selskab for Akutmedicins behandling af personoplysninger på bestyrelsesmedlemmers private computere og e-mailkonti.

Efter at sagen havde været forelagt Datarådet, udtalte Datatilsynet, at Dansk Selskab for Akutmedicin ikke havde truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passede til de risici, der var ved foreningens behandling af personoplysninger, jf. databeskyttelsesforordningens artikel 32, stk. 1.

Tilsynet lagde bl.a. vægt på, at det følger af forordningens krav om passende sikkerhed, at foreninger eller organisationer, der lader bestyrelsesmedlemmer behandle personoplysninger, som foreningen eller organisationen er dataansvarlig for, skal gennemføre passende sikkerhedsforanstaltninger i forbindelse hermed.

Der skal kunne føres kontrol med, at den behandling af personoplysninger, som bestyrelsesmedlemmerne foretager, sker under iagttagelse af de sikkerhedsforanstaltninger, som foreningen eller organisationen som dataansvarlig har besluttet skal implementeres. Dette kan eksempelvis være adgangskontrol, kryptering af data og andre tekniske sikkerhedsforanstaltninger på det udstyr og e-mailkonti, som foreningens eller organisationens bestyrelsesmedlemmer anvender i deres opgavevaretagelse. Herudover skal foreningen eller organisationen også – hvor det er relevant – fastsætte retningslinjer og procedurer for bestyrelsesmedlemmernes anvendelse af udstyret.

Endvidere fandt Datatilsynet, at det vil være vanskeligt for en dataansvarlig at føre kontrol med den sikkerhed, hvorunder bestyrelsesmedlemmerne behandler personoplysninger på deres private computere, som eksempelvis hvilken adgangskontrol det enkelte bestyrelsesmedlem har på sin private computer, samt hvordan bestyrelsesmedlemmet opbevarer eller transporterer sin private computer, og hvordan sikkerheden på den private computer måtte være konfigureret eller hvor mange potentielt skadelige applikationer, der er installeret.

Datatilsynet lagde herudover vægt på, at i tilfælde som denne sag, hvor de behandlinger af personoplysninger, der skal foretages, består af vurderinger og kommunikation af fortrolige eller følsomme oplysninger, skal der etableres en løsning, som sikrer, at denne fortrolighed ikke undermineres. Der må således ikke sendes følsomme eller fortrolige personoplysninger ukrypteret over netværk, som den dataansvarlige ikke har fuld kontrol over, f.eks. ukrypterede e-mails på internettet. I disse situationer skal man således anvende en sikker løsning. Dette kunne f.eks. være brug af foreningens e-Boks, fælles foreningsportal med differentieret adgang eller brug af en intern mailklient med den fornødne sikkerhed, f.eks. i form af separate e-mailkonti med individuel adgang for de, der behandler personoplysninger og mulighed for fornøden kryptering på afsendelse og modtagelse af e-mails.

Datatilsynet kunne tilslutte sig Dansk Selskab for Akutmedicins egen vurdering af, at selskabet ikke havde haft et tilstrækkeligt sikkerhedsniveau for personoplysninger modtaget ved eksterne henvendelser.

På den baggrund fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at Dansk Selskab for Akutmedicins behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1.

Automatisk udfyldning af oplysninger ved køb på hjemmeside

Datatilsynet traf afgørelse i en sag vedrørende Rito ApS' behandling af personoplysninger i forbindelse med automatisk udfyldning af personoplysninger om kunder ved køb på virksomhedens hjemmeside.

Efter at sagen havde været forelagt Datarådet, udtalte Datatilsynet, at Rito ApS ved at anvende en funktionalitet, hvorved oplysninger om tidligere kunder potentielt kunne tilgås af andre uvedkommende brugere, ikke levede op til kravene om et passende sikkerhedsniveau i databeskyttelsesforordningens artikel 32.

Tilsynet lagde bl.a. vægt på, at en eventuel videregivelse af personoplysninger om tidligere kunder til andre brugere af hjemmesiden som udgangspunkt ikke var tilsigtet – dvs. at det ikke var formålet med løsningen, at brugere skulle have adgang til informationer om andre kunder. Tilsynet lagde i den forbindelse vægt på, at Rito ApS havde implementeret visse foranstaltninger med henblik på at forbygge misbrug af adgangen til autoudfyldte oplysninger, herunder en begrænsning til at foretage maksimalt ti opslag fra samme ip-adresse inden for 24 timer og overvågning af uregelmæssig adfærd.

Endvidere fandt Datatilsynet, at Rito ApS' nye løsning, hvor den enkelte kunde skulle acceptere, at virksomheden gemte oplysningerne til senere automatisk adresseudfyldelse fortsat ikke levede op til kravene om et passende sikkerhedsniveau i databeskyttelsesforordningens artikel 32. Det var tværtimod Datatilsynets opfattelse, at Rito ApS' nye løsning for indhentelse af accept kunne være medvirkende til at øge opmærksomheden på den manglende sikkerhed, hvilket i sig selv kunne føre til, at risikoen for misbrug blev forøget.

Datatilsynet lagde endvidere vægt på, at den pågældende information til kunderne og deres eventuelle accept ikke øgede sikkerheden for behandlingen af de registreredes oplysninger. Efter tilsynets opfattelse kan registrerede ikke give afkald på fornøden sikkerhed ved at give samtykke til et sikkerhedsniveau, der ikke lever op til kravene i databeskyttelsesforordningens artikel 32.

På den baggrund fandt Datatilsynet grundlag for at udtale kritik af, at Rito ApS' behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32.

Datatilsynet meddelte Rito ApS påbud om at ophøre med at anvende den af Rito ApS beskrevne autoudfyldningsfunktionalitet, hvilket gjorde sig gældende, uanset om der var indhentet en form for accept fra kundernes side eller ej.

Datatilsynet fandt i forlængelse af sagen anledning til at overveje, hvorvidt det – inden for rammerne af databeskyttelsesforordningens artikel 32 – er muligt for virksomheder at anvende en løsning, der autoudfylder oplysninger om brugere på den dataansvarliges hjemmeside.

Det er i den forbindelse Datatilsynets umiddelbare vurdering, at løsninger med autoudfyldning af oplysninger, hvor den registrerede på forhånd har verificeret sig tilstrækkeligt på anden måde, eksempelvis via et unikt log-in på hjemmesiden, vil leve op til kravene om sikkerhed i databeskyttelsesforordningens artikel 32.

Manglende indsigt i sædbanks oplysninger

Datatilsynet traf afgørelse i en sag, hvor en borger klagede over, at Cryos International ApS havde afslået hans anmodning om indsigt i antallet af donorbørn, som var undfanget ved sæddonation fra ham, og oplysninger om hvor mange af disse børn, der måtte have en enlig mor.

Datatilsynet fandt, at oplysningen om, hvor mange af børnene der måtte have en enlig mor, ikke udgjorde en personoplysning om den pågældende borger og dermed ikke var omfattet af borgerens indsigtsret.

Det var derimod Datatilsynets opfattelse, at oplysningen om antallet af donorbørn, som var undfanget ved sæddonation fra borgeren, måtte anses for at være en personoplysning om borgeren. Datatilsynet fandt endvidere, at denne oplysning ikke kunne undtages fra retten til indsigt som følge af databeskyttelseslovens § 22, stk. 1.

Datatilsynet udtalte herefter kritik af Cryos International ApS, idet virksomheden ikke i fornødent omfang havde meddelt borgeren indsigt efter databeskyttelsesforordningens artikel 15. Datatilsynet meddelte endvidere Cryos International ApS påbud om at meddele borgeren indsigt i antallet af donorbørn, som var undfanget ved sæddonation fra ham.

Ved vurderingen af, at oplysningerne ikke kunne undtages fra indsigtsret, lagde Datatilsynet vægt på, at der alene var tale om en oplysning om antallet af donorbørn, som ikke gjorde borgeren i stand til at identificere og opsøge børnene. Desuden fandt Datatilsynet, at borgerens indsigt i oplysningen om antallet af donorbørn, som var undfanget ved sæddonation fra ham, ikke medførte en sådan nærliggende fare for, at private interesser, herunder børnenes interesser, ville lide skade af væsentlig betydning, at der var grundlag for at undtage oplysninger fra indsigtsret.

MeToo-sager

Datatilsynet har i årets løb modtaget flere klager over behandling af personoplysninger i forbindelse med iværksættelse og gennemførelse af flere advokatundersøgelser vedrørende seksuel krænkelse mv.

Sagerne forventes afklaret i løbet af 2022.

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 løbende en række sager op på baggrund af konkrete hændelser, f.eks. presseomtale, henvendelser fra borgere mv.

Særlige fokusområder for dele af Datatilsynets tilsynsaktiviteter i 2021

Datatilsynet offentliggjorde i januar 2021 en oversigt over, hvilke områder tilsynet særligt ville fokusere på, når det gjaldt de tilsynsaktiviteter, Datatilsynet selv sætter i værk i løbet af året.

Oversigt over særlige fokusområder for dele af Datatilsynets tilsynsaktiviteter i 2021

Tilladelser til at føre kreditoplysningsbureau, advarselsregistre og spærrelister
Kreditoplysningsbureauer kan på nærmere fastsatte vilkår få tilladelse fra Datatilsynet til at behandle personoplysninger med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed. Datatilsynet besluttede at føre tilsyn med kreditoplysningsbureauers behandling af personoplysninger, herunder overholdelse af de vilkår, som Datatilsynet har fastsat for kreditoplysningsbureauernes behandling af personoplysninger.

Datatilsynet besluttede endvidere at sætte fokus på behandling af personoplysninger i forbindelse med førelse af advarselsregistre og spærrelister. Datatilsynet ville i den forbindelse føre tilsyn med, om de vilkår, som Datatilsynet har fastsat i forbindelse med en række tilladelser til at føre advarselsregistre og spærrelister, blev overholdt.

Konkret valgte Datatilsynet at føre tilsyn med en række private virksomheder mv., der alle besad en tilladelse fra Datatilsynet til enten at drive kreditoplysningsbureauvirksomhed, føre et advarselsregister eller en spærreliste.

Inkassobureauers oplysningspligt og sletning
Der findes i databeskyttelsesforordningen en række helt centrale regler, der omhandler de registreredes rettigheder, herunder regler om den dataansvarliges oplysningspligt ved behandling af personoplysninger og om indsigt i de oplysninger, der behandles om de registrerede. Reglerne skal være med til at sikre, at behandling af personoplysninger foregår på en rimelig og gennemsigtig måde.

Forordningen indeholder også en grundlæggende regel om, at når personoplysninger ikke længere er nødvendige, skal de slettes eller anonymiseres. Reglen bidrager til at sikre mod en unødvendig ophobning af data, idet dette principielt altid indebærer en vis forøget risiko for krænkelse af de registrerede. f.eks. ved at uvedkommende får fat i oplysningerne.

Datatilsynet valgte i 2021 at føre tilsyn med en række inkassobureauers håndtering af reglerne om oplysningspligt. Endvidere valte Datatilsynet at føre tilsyn med inkassobureauernes opbevaring, herunder håndtering af og procedurer for sletning af personoplysninger.

Pengeinstitutters procedure for indsigtsanmodninger
Med henblik på fokus på de registreredes rettigheder, jf. ovenfor valgte Datatilsynet i 2021 også at føre tilsyn med en række pengeinstitutters procedure for håndtering af den registreredes ret til indsigt.

Tv-overvågning
Den 1. juli 2020 trådte en ændring af tv-overvågningsloven i kraft. Med ændringen er der bl.a. skabt mere lempeligere rammer for det område, som kan tv-overvåges, da tv-overvågning ikke længere umiddelbart er begrænset af et afstandskrav ved overvågning af området omkring egne indgange og facader. Lovændringen indebærer også, at kommuner i videre omfang kan foretage tv-overvågning af områder, som benyttes til almindelig færdsel, og som ligger i tilknytning til eller i forlængelse af en restaurationsvirksomhed.

Datatilsynet besluttede i 2021 – navnlig i lyset af ovenstående lovændring – at føre tilsyn med en række private og offentlige myndigheders behandling af personoplysninger i forbindelse med tv-overvågning.

Myndigheders videregivelse af personnumre til borgere
Datatilsynet er på baggrund af konkrete henvendelser blevet opmærksom på, at nogle offentlige myndigheder videregiver oplysninger om borgeres personnummer til andre borgere i forbindelse med myndighedernes sagsbehandling.

Datatilsynet besluttede i 2021 at føre tilsyn med offentlige myndigheders videregivelse af personnumre til borgere med henblik på at undersøge, i hvilket omfang dette finder sted, og hvad baggrunden herfor er.

Forskning
På baggrund af en foreløbig rapport fra Kammeradvokaten om forskellige problemstillinger i forbindelse med forskningsprojekter på Statens Serum Institut (SSI) indledte Datatilsynet i efteråret 2020 en nærmere undersøgelse af forholdene hos SSI.

Med henblik på at undersøge, om de problemstillinger, som tilsyneladende gør sig gældende hos SSI, går igen hos andre lignende dataansvarlige, valgte Datatilsynet endvidere at igangsætte flere skriftlige tilsyn med offentlige institutioner, som udfører forskning. I forlængelse heraf var det også tilsynets hensigt, at der i 2021 skulle iværksættes tilsyn med en eller flere private forskningsinstitutioner.

Behandling af personoplysninger om hjemmesidebesøgende
Som opfølgning på Datatilsynets vejledning fra februar 2020 om behandling af personoplysninger om hjemmesidebesøgende besluttede Datatilsynet at fastholde fokus på området og iværksætte tilsyn på området i 2021.

Persondatasikkerhed - inkl. brud på persondatasikkerheden
Myndigheder eller virksomheder har – som dataansvarlige og som databehandlere – et ansvar for at etablere et passende sikkerhedsniveau, når de behandler personoplysninger. Hvis der sker et brud på persondatasikkerheden har den dataansvarlige som udgangspunkt et ansvar for at anmelde bruddet til Datatilsynet, ligesom den dataansvarlige også i nogle tilfælde skal underrette de berørte registrerede om bruddet.

Datatilsynet modtog i 2020 knap 9.000 anmeldelser af brud på persondatasikkerheden. Brudene giver tilsynet et indgående kendskab til de udfordringer, der er i forhold til sikkerheden hos dataansvarlige og databehandlere. På baggrund af bl.a. de anmeldte brud har tilsynet identificeret en række områder, hvor risikoen for manglende efterlevelse af databeskyttelsesreglerne, herunder reglerne om passende sikkerhed, ses at være størst.

Datatilsynet besluttede derfor at føre tilsyn i 2021 med sikkerheden inden for følgende områder:

- adgangs- og rettighedsstyring,
- anvendelse af personoplysninger i forbindelse med it-udvikling og test,
- håndtering af personoplysninger, som "tages ud af" dertil indrettede it-systemer, f.eks. på bærbare elektroniske medier eller på papir mv. (uddatamateriale), og
- om brud på persondatasikkerheden håndteres og anmeldes i overensstemmelse med reglerne herom.

Alt efter karakteren af de pågældende områder rettede tilsynene sig i varierende grad mod forskellige dataansvarlige i den private og i den offentlige sektor, herunder bl.a. kommuner, sundhedssektoren og politiet samt mod fællesoffentlige digitale løsninger. I tilknytning hertil vil Datatilsynet iværksætte en mere generel screening af sikkerhedsområder hos et større antal dataansvarlige.

Kontrol med databehandlere
Myndigheder og virksomheder kan som dataansvarlige overlade personoplysninger til andre aktører, der som databehandlere herefter står for behandlingen af oplysningerne. De enkelte dataansvarlige har en selvstændig forpligtelse til at føre kontrol med, om en databehandler overholder den dataansvarliges instrukser for behandlingen. Tilsvarende har databehandleren en selvstædighed forpligtelse til at leve op til databeskyttelsesreglerne. I praksis oplever Datatilsynet imidlertid jævnligt brud på persondatasikkerheden hos databehandlere – brud som de dataansvarlige efter omstændighederne ville kunne have forebygget ved en effektiv kontrol med de respektive databehandlere.

Da brugen af databehandlere er meget udbredt og således udgør en meget væsentlig del af digitaliseringen i Danmark, er risikoen for de registrerede tilsvarende stor, hvis databehandlere i bred forstand ikke lever op til databeskyttelsesreglerne, og i tilknytning hertil, hvis de dataansvarlige ikke fører en tilstrækkelig kontrol med databehandlere.

Derfor har Datatilsynet siden 2016 haft et løbende fokus på kontrol med databehandlere, og i maj 2019 afgav Rigsrevisionen i forlængelse heraf også en beretning til Statsrevisorerne om "outsourcede persondata". En af Rigsrevisionens konklusioner i beretningen er, at mange myndigheder har haft en utilstrækkelig styring af databehandlere og bl.a. alt for sjældent har udarbejdet risikovurderinger.

Der er således stadig behov for, at både Datatilsynet og myndighederne arbejder meget mere med området, og tilsynet besluttede derfor at føre tilsyn med en række statslige myndigheders kontrol med databehandlere i 2021.

Overførsel af personoplysninger til tredjelande
Når en myndighed eller virksomhed overfører personoplysninger til lande uden for EØS (tredjelande), kræves det, at der foreligger et såkaldt overførselsgrundlag. Formålet hermed er at sikre, at databeskyttelsesreglerne ikke udvandes, når oplysningerne forlader EØS.

Med den såkaldte Schrems II-afgørelse i 2020 slog EU-Domstolen fast, at man som dataeksportør er forpligtet til at sikre et essentielt tilsvarende beskyttelsesniveau i tredjelandet, og at dette i nogle tilfælde kræver, at man – ud over at tilvejebringe et overførselsgrundlag – iværksætter supplerende foranstaltninger.

Datatilsynet besluttede i 2021 – navnlig i lyset af Schrems II-afgørelsen – at føre tilsyn med en række virksomheders og offentlige myndigheders overførsel af personoplysninger til tredjelande.

Behandling af personoplysninger i fælleseuropæiske informationssystemer
Datatilsynet er tilsynsmyndighed for danske myndigheders behandling af personoplysninger i forbindelse med anvendelsen af en række fælleseuropæiske informationssystemer. Det drejer sig bl.a. om Schengen-informationssystemet (SIS), Visuminformationssystemet (VIS), EU-fingeraftryksregisteret (Eurodac), Toldinformationssystemet (CIS) og Informationssystemet for det indre marked (IMI).

Datatilsynet besluttede i 2021 at føre tilsyn med en række myndigheders behandling af personoplysninger i forbindelse med anvendelsen af nogle af de nævnte informationssystemer.

PNR-loven
PNR-loven udgør den retlige ramme for politiets indsamling og behandling af de passagerlisteoplysninger (PNR-oplysninger), som luftfartsselskaberne er i besiddelse af om deres passagerer. Oplysningerne må ifølge loven alene behandles til nogle særligt opregnede formål.

Der er i medfør af loven etableret en PNR-enhed i Rigspolitiet, som er ansvarlig for bl.a. at indsamle, opbevare, og videregive oplysningerne. Datatilsynet er udpeget til at føre tilsyn med PNR-enheden.

Datatilsynet besluttede i 2021 at føre tilsyn med Rigspolitiets overholdelse af en række af lovens bestemmelser.

Retshåndhævelsesloven
Retshåndhævelsesloven gælder for politiets, anklagemyndighedens, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, når behandlingen foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner. Datatilsynet fører tilsyn med de retshåndhævende myndigheders behandling af personoplysninger omfattet af loven – dog med undtagelse af domstolene. Datatilsynet behandler endvidere klagesager og tager sager op af egen drift på området. Datatilsynet valgte i 2021 at føre tilsyn med udvalgte retshåndhævende myndigheders overholdelse af en række af lovens bestemmelser (Læs mere herom i afsnittet Del. 2: Retshåndhævelsesloven).

Oversigt over udførte tilsyn i 2021

Offentlige myndigheder:
Ankestyrelsen
Arktisk Kommando, Forbindelseselement Færøerne
Allerød Kommune
Beskæftigelsesministeriet
Bornholms Politi
Brøndby Kommune
Digitaliseringsstyrelsen – MitID
Esbjerg Kommune
Forsvarsministeriets Personalestyrelse
Frederikshavn Kommune
Frederikssund Kommune
Fyns Politi
Færøernes Politi
Gentofte Kommune
Gladsaxe Kommune
Greve Kommune
Grønlands Statistik
Guldborgsund Kommune
Gældsstyrelsen
Hedensted Kommune
Hillerød Kommune
Hjemrejsestyrelsen
Høje-Taastrup Kommune
Hjørring Kommune
Jammerbugt Kommune
Kalundborg Kommune
Kommuneqarfik Sermersooq
Kriminalforsorgen på Færøerne
Københavns Kommune
Køge Kommune
Lolland Kommune
Mariagerfjord Kommune
Middelfart Kommune
Norddjurs Kommune
Nordjyllands Politi
Odsherred Kommune
Plejeboligcenter Fælledgården
Plejecenter Smedegade
Randers Kommune
Region Hovedstaden
Region Nordjylland
Region Midtjylland
Region Sjælland
Rigshospitalet Glostrup
Rigsombudsmanden på Færøerne
Rigspolitiet

Ringkøbing-Skjern Kommune
Ringsted Kommune
Roskilde Kommune
Slagelse Sygehus
Styrelsen for Forebyggelse og Sociale forhold
Styrelsen for International Rekruttering og Integration
Sundhedsdatastyrelsen
Sønderborg Kommune
Tønder Kommune
Udbetaling Danmark
Varde Kommune

Private virksomheder:
Aktieselskabet Th. Wessel & Vett. Magasin Du Nord
Alsik A/S
AP Pension Livsforsikringsaktieselskab
Arbejdernes Landsbank
Basisbank
Berlingske Media
Bisnode
Brobizz A/S
Brødrene A & O Johansen A/S
Cabinn A/S
CAH II A/S
CNP Assurances Danmark, filial af CNP Assurances, Frankrig
Collectia
Dagrofa ApS
Danske Andelsinkasso A/S
Danske Andelskassers Bank A/S
Danske Bank
Danish Crown A/S
Dansk forening for international motorkøretøjsforsikring, DFIM
Danske Inkasso A/S
Danica Pension Livsforsikringsaktieselskab
Danske Speditører
Euler Hermes Danmark
Experian
Forbrugsforeningen af 1886
Grakom Arbejdsgivere
Glostrup Apotek
Hans Just A/S
Hornskov Vindberg
Hotel D'Angleterre ApS
Inco CC København A/S
Industriens Pensionsforsikring A/S
Johannes Fog A/S
JP Politikens Hus
Jutlander Bank A/S
Jyske Bank A/S
Katsorsaavik Nuuk ApS

KMD
Kredinor A/S
Kræftens Bekæmpelse
Kurhotel Skodsborg A/S
København Østerbro Apotek
Lemvigh-Müller A/S
Louis Poulsen A/S
Lån & Spar Bank A/S
Mark Industrie
Munkebjerg Hotel
Mælkebøttecentret, Nuuk
Nykredit Bank A/S
Pensam A/S
Pensiondanmark Pensionsforsikringsaktieselskab
PFA Pension, Forsikringsaktieselskab
Rejsekort A/S
Ringkøbing Landbobank Aktieselskab
Ruths Hotel A/S
Saxo Bank A/S
Sergel A/S
Scandic Hotel A/S
Scanlico Denmark A/S
Sparekassen Kronjylland
Spar Nord Bank A/S
Sparekassen Sjælland-Fyn
Strand- & Badehotel Marienlyst A/S
Sydbank A/S
Topdanmark Livsforsikring A/S
Vestjysk Bank A/S
Velliv, Pension & Livsforsikring A/S
Villa Copenhagen A/S
Visma Rating

Fælleseuropæiske systemer

Arbejdstilsynet
Erhvervsstyrelsen
Rigspolitiet
Toldstyrelsen
Udlændinge- og Integrationsministeriet

Tilsyn baseret på digital screening

Offentlige myndigheder:
Brøndby Kommune
Frederikssund Kommune
Greve Kommune
Hedensted Kommune
Jammerbugt Kommune

Mariagerfjord Kommune
Middelfart Kommune
Norddjurs Kommune
Ringsted Kommune
Tønder Kommune
Vesthimmerlands Kommune

Private:
Alsik A/S
AP Pension Livsforsikringsaktieselskab
Cabinn A/S
CAH II A/S
CNP Assurances Danmark, filial af CNP Assurances, Frankrig
Danica Pension Livsforsikringsaktieselskab
Hotel D'Angleterre ApS
Industriens Pensionsforsikring A/S
Kurhotel Skodsborg A/S
Munkebjerg Hotel
Pensam A/S
Pensiondanmark Pensionsforsikringsaktieselskab
PFA Pension, Forsikringsaktieselskab
Ruths Hotel A/S
Scandic Hotel A/S
Strand- & Badehotel Marienlyst A/S
Topdanmark Livsforsikring A/S
Velliv, Pension & Livsforsikring A/S
Villa Copenhagen A/S

Tilsyn med brug af tilsynsprogram ved online eksamen

Datatilsynet traf i 2021 afgørelse i en sag, hvor Datatilsynet på baggrund af en telefonisk henvendelse besluttede at undersøge IT-Universitetets (ITU) brug af et tilsynsprogram ved en onlineeksamen nærmere.

ITU var som følge af COVID-19-situationen blevet pålagt at afholde undervisning og eksaminer online. ITU vurderede, at det i et enkelt fag var nødvendigt at føre tilsyn med de studerende ved hjælp af et tilsynsprogram, der under den tre timer lange eksamen foretog video-, lyd- og skærmoptagelser og registrering af browsersøgehistorik fra de studerendes computere.

Datatilsynet fandt konkret i sagen, at ITU's brug af tilsynsprogrammet var foretaget inden for rammerne af de databeskyttelsesretlige regler.

Datatilsynet lagde i sin afgørelse blandt andet vægt på, at ITU havde foretaget en konkret nødvendighedsvurdering af behovet for eksamenstilsyn i forhold til de fag, ITU udbød, og ITU havde vurderet det nødvendigt i et enkelt fag. Endvidere lagde Datatilsynet vægt på, at ITU ved udvælgelsen af overvågningsprogrammet havde valgt et program, der i forhold til de konkrete omstændigheder var det mindst indgribende, at ITU havde orienteret de studerende om den ekstraordinære behandling af personoplysninger, og at ITU havde truffet en række sikkerhedsmæssige foranstaltninger i forbindelse med tilsynsprogrammets behandling af oplysninger om de studerende

Tilsyn med oplysningspligt hos testudbydere

Datatilsynet valgte i marts 2021 at føre tilsyn med tre udbydere, som tilbød COVID-19-test uden forudgående tidsbestilling. Datatilsynet førte tilsyn med SOS International A/S og Carelink A/S, som i januar 2021 vandt udbuddet af hurtigtest i regionerne. Datatilsynet førte endvidere tilsyn med Statens Serum Institut, som tilbød PCR-test uden forudgående tidsbestilling på TestCenter Danmarks mobile teststeder.

Tilsynene fokuserede på udbydernes efterlevelse af databeskyttelsesforordningens regler om oplysningspligt, herunder om testudbyderne levede op til reglerne om, at underretning skal gives til den registrerede i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog.

Datatilsynet fandt, at testudbydernes iagttagelse af oplysningspligten var i overensstemmelse med reglerne. Over for en enkelt udbyder henstillede tilsynet dog, at udbyderen supplerede underretningen af borgeren, som skete i forbindelse med modtagelse af testresultatet, med overordnede informationer på selve teststedet.

I forlængelse af ovenstående tilsyn valgte Datatilsynet i juni 2021 endvidere at føre tilsyn med Falck Danmark A/S' iagttagelse af oplysningspligten ved behandling af personoplysninger i forbindelse med COVID-19-hurtigtest af elever over 12 år i grundskolen.

Datatilsynet fandt også i denne sag, at oplysningspligten blev iagttaget i overensstemmelse med reglerne, men tilsynet bemærkede, at det ville være hensigtsmæssigt, at der blev udarbejdet en pjece eller planche, som i form og indhold var rettet mod børn.

Tilsyn med SSI's Covid-19-modelleringsprojekt

I forbindelse med Covid-19-situationens eskalering i Danmark (februar-marts 2020) og den derpå følgende nedlukning af samfundet skulle Statens Serum Institut (SSI) stille persondata – i form af blandt andet helbredsoplysninger – til rådighed for en ekspertgruppe, der skulle regne på mulige scenarier for genåbning.

SSI havde på forhånd vurderet, at risikoen for de registrerede var moderat til høj, ligesom SSI havde konstateret, at der ved behandlingens start ikke var foretaget en fuldstændig kortlægning og vurdering af de risici, som behandlingen indebar. SSI vurderede sidenhen, at den mangelfulde kortlægning og vurdering i sig selv medførte en høj risiko for de registreredes rettigheder.

Den oprindeligt tiltænkte it-løsning for dataudvekslingen kunne dog ikke være klar hurtigt nok, hvorfor dataadgangen i uge 12 blev etableret på SSI's SFTP server, der var placeret bag en ydre firewall i en zone, der kunne tilgås af eksperterne udefra (også benævnt DMZ). Oplysningerne var placeret i dedikerede mapper, hvor eksperterne, der skulle have adgang, benyttede brugernavn og kendeord.

Risikovurderingen blev ifølge SSI grundet manglende interne ressourcer og situationen på tidspunktet først påbegyndt i uge 16, og første version af en konsekvensanalyse forelå i uge 17. Databehandleraftaler med ekspertgruppens medlemmer blev ligeledes først underskrevet i uge 17.

Datatilsynet fandt, at SSI allerede på det tidspunkt, hvor de – inden behandlingens påbegyndelse – havde indset, at denne indebar en høj risiko for de registreredes rettigheder, skulle have påbegyndt arbejdet med konsekvensanalysen. Dette særligt når det stod klart, at det hastede med at komme i gang med behandlingen. Tilsynet konstaterede endvidere, at det – når der er en indbygget høj risiko for de registreredes rettigheder – og denne risiko ikke er nedbragt gennem de initiativer, som egentlig skulle udspringe af en konsekvensanalyse, alene er muligt at påbegynde behandlingen, når Datatilsynet er blevet hørt.

Datatilsynet konstaterede, at der først fem uger efter behandlingens påbegyndelse blev indgået de fornødne databehandleraftaler.

Datatilsynet konstaterede herudover, at der ved valget af den midlertidige løsning på SSI's SFTP server ikke var taget fornødent højde for risikoen for uautoriseret adgang til oplysningerne, særligt vurderet i forhold til oplysningernes karakter, interesse og evner hos de aktører, der måtte interessere sig for dem, og den valgte løsnings tekniske karakter. Tilsynet fandt derfor, at løsningen ikke havde det fornødne niveau af sikkerhed.

Datatilsynet fandt, at det var formildende omstændigheder, at behandlingen skulle etableres under en international krisesituation, at der forelå en væsentlig samfundsinteresse i den hurtige effektuering af behandlingen, og at SSI – dog – havde gjort sig overvejelser om den foreløbige fravigelse af de databeskyttelsesretlige regler og – i et vist omfang – havde forsøgt at afhjælpe disse. På den baggrund blev sanktionen alene fastsat til alvorlig kritik.

Tilsyn med kommunernes databeskyttelsesrådgivere

I 2021 afsluttede Datatilsynet 17 planlagte tilsyn med fokus på kommunernes databeskyttelsesrådgivere. Datatilsynet fandt i alle 17 tilsyn, at kommunernes løsninger var i overensstemmelse med reglerne for databeskyttelse.

Datatilsynet førte tilsyn med forskellige temaer omkring kommunernes databeskyttelsesrådgivere, herunder databeskyttelsesrådgiverens opgaver, ressourcer, faglige kvalifikationer og de registreredes adgang til databeskyttelsesrådgiveren. Den ene gruppe af tilsyn fokuserede på kommuner, som delte databeskyttelsesrådgiver med andre kommuner. Den anden gruppe af tilsyn fokuserede på kommuner, som havde tilkøbt sig ydelsen hos et advokatselskab.

I den første gruppe af tilsyn var en række kommuner tilknyttet to personer hos det Nordsjællandske Digitaliseringsarbejde. De to personer fungerede som databeskyttelsesrådgivere for alle de pågældende kommuner. De omhandlede kommuner var Fredensborg Kommune, Gribskov Kommune, Frederikssund Kommune, Helsingør Kommune, Hillerød Kommune, Hørsholm Kommune og Halsnæs Kommu-

ne. Andre kommuner havde udpeget en databeskyttelsesrådgiver, som var tilknyttet den Storkøbenhavnske Digitaliseringsforening. Det var tilfældet for Høje-Taastrup Kommune, Hvidovre Kommune, Dragør Kommune og Albertslund Kommune.

I den anden gruppe af tilsyn var en række kommuner tilknyttet forskellige advokatselskaber. Det drejede sig om Vejle Kommune, Næstved Kommune, Roskilde Kommune, Vordingborg Kommune, Mariagerfjord Kommune og Hjørring Kommune.

På baggrund af tilsynene var det Datatilsynets vurdering, at kommunernes løsninger om brug af databeskyttelsesrådgivere lå inden for rammerne af databeskyttelsesforordningen.

Det er Datatilsynets opfattelse, at den dataansvarlige og databehandleren selv er nærmest til at vurdere, hvordan den praktiske del af samarbejdet med databeskyttelsesrådgiveren skal implementeres, så samarbejdet kan foregå mest effektivt og hensigtsmæssigt i organisationen. Den dataansvarlige og databehandleren kan derfor i vidt omfang selv organisere den praktiske del af samarbejdet med databeskyttelsesrådgiveren, så længe dette sker inden for rammerne af databeskyttelsesforordningens kapitel 4.

Tilsyn med opbevaring og sletning af oplysninger om ansøgere, der ikke blev ansat

I 2021 afsluttede Datatilsynet to tilsyn med henholdsvis Kræftens Bekæmpelse og Fødevarestyrelsen, som tilsynet havde startet op i sommeren 2019. Datatilsynet havde i maj 2020 afsluttet et lignende tilsyn med Carlsberg Danmark A/S.

De to tilsyn fokuserede på Kræftens Bekæmpelses og Fødevarestyrelsens opbevaring og sletning af personoplysninger om ansøgere (efter endt rekrutteringsforløb), og hvor ansøgerne ikke var blevet ansat.

Tilsynene gav ikke Datatilsynet anledning til at udtale kritik af hverken Kræftens Bekæmpelse eller Fødevarestyrelsens behandling.

I forbindelse med tilsynene blev Datatilsynet opmærksom på, at Kræftens Bekæmpelse brugte samtykke som behandlingsgrundlag, når virksomheden gemte oplysninger om ansøgere med det formål at dokumentere, at der ikke var sket diskrimination eller lignende under ansøgningsprocessen. Herudover anvendte både Kræftens Bekæmpelse og Fødevarestyrelsen samtykke som behandlingsgrundlag under selve rekrutteringsprocessen.

Datatilsynet henstillede i den forbindelse til, at Kræftens Bekæmpelse skulle stoppe med at bruge samtykke til at opbevare oplysningerne til dokumentationsformål, hvis organisationen i stedet kunne basere behandlingen på andre relevante bestemmelser som f.eks. overholdelse af en retlig forpligtelse. Herudover henstillede Datatilsynet også til, at både Kræftens Bekæmpelse og Fødevarestyrelsen skulle stoppe med at anvende samtykke til behandling af oplysninger under selve rekrutteringsprocessen, når organisationerne kunne basere behandlingen på andre relevante bestemmelser i databeskyttelsesreglerne, som f.eks. overholdelse af en retlig forpligtelse, interesseafvejningsreglen eller i forbindelse med myndighedsudøvelse.

Det var endvidere Datatilsynets opfattelse, at både Kræftens Bekæmpelse og Fødevarestyrelsen havde etableret passende sletteprocedurer og opbevaringsperioder for oplysningerne.

Tilsyn med datingstjenestes behandling af personoplysninger

Datatilsynets tilsyn med Dating.dk ApS (Dating.dk) var rettet mod datingtjenestens behandling af personoplysninger i forbindelse med, at brugere opretter og benytter sig af tjenesten. Tilsynet fokuserede på datingtjenestens behandlingsgrundlag og behandlingssikkerhed.

På baggrund af tilsynet fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at Dating.dks behandling af personoplysninger om brugerne ikke skete i overensstemmelse med databeskyttelsesreglerne, idet Dating.dk ikke havde et gyldigt behandlingsgrundlag.

Det var Datatilsynets vurdering, at Dating.dk ikke havde opnået en utvetydig viljestilkendegivelse fra brugerne af datingtjenesten til behandling af personoplysninger om dem, hvorfor Dating.dk ikke havde indhentet et gyldigt samtykke til behandling af personoplysninger.

Derudover var det Datatilsynets vurdering, at Dating.dk havde behandlet følsomme personoplysninger uden at have identificeret en undtagelse til det generelle forbud mod behandling af særlige kategorier af personoplysninger.

På den baggrund fandt Datatilsynet grundlag for at meddele Dating.dk et påbud om, at virksomheden skulle bringe behandlingen af personoplysninger om brugere af Dating.dk i overensstemmelse med databeskyttelsesforordningens bestemmelser.

Datatilsynet fandt endelig grundlag for at udtale alvorlig kritik af, at Dating.dk havde behandlet personoplysninger uden at kunne påvise, at behandlingen var sket under hensyntagen til de risici, som behandlingen udgjorde for de registrerede. Datatilsynet lagde i denne forbindelse vægt på, at Dating.dk behandlede oplysninger om lokation og særlige kategorier af personoplysninger.

Kommunes anvendelse af oplysninger om hjemmesidebesøgende til statistik

Datatilsynet iværksatte i 2020 en sag af egen drift mod Næstved Kommune om kommunens behandling af personoplysninger om hjemmesidebesøgende. Efter Datatilsynet indledte undersøgelsen af Næstved Kommune, valgte kommunen at ændre sin fremgangsmåde til behandling af personoplysninger om besøgende på kommunens hjemmeside.

Den fremgangsmåde til behandling af personoplysninger om besøgende, som Næstved Kommune benyttede i oktober 2020 præsenterede den hjemmesidebesøgende for information om, at hjemmesiden brugte cookies til bl.a. at forbedre brugeroplevelsen og til at støtte markedsføringen af kommunens services. Hjemmesidebesøgende havde herefter mulighed for at vælge "OK" eller "Vis detaljer".

Næstved Kommune oplyste, at oplysninger om hjemmesidebesøgende blev indsamlet til statistiske formål med henblik på at sikre et højt niveau af borger- og brugervenlighed.

Datatilsynet fandt – efter sagen havde været forelagt Datarådet – anledning til at udtale kritik af, at Næstved Kommune i forbindelse med behandling af personoplysninger om hjemmesidebesøgende ikke iagttog det grundlæggende behandlingsprincip om, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde. Afgørende herfor var, at teksterne på hjemmesiden foranledigede besøgende til at tro, at kommunen behandlede personoplysninger til markedsføringsformål, selvom dette ikke var tilfældet.

Datatilsynet fandt endvidere, at Næstved Kommunes behandling af personoplysninger om hjemmesidebesøgende til statistiske formål skete som led i kommunens myndighedsudøvelse og dermed inden for rammerne af databeskyttelsesreglerne. Datatilsynet lagde i den forbindelse vægt på, at Næstved Kommune har en pligt til at vejlede og hjælpe borgere, hvilket bl.a. kan ske ved brug af hjemmesiden. Datatilsynet lagde ved vurderingen til grund, at kommunens behandling af oplysninger var sat op på en måde, så datasættet fra de enkelte cookies indsamles hos en leverandør, som genererede irreversibel anonymiseret statistik til kommunen.

Anmeldelser af brud på persondatasikkerheden

Opgørelse af brud på persondatasikkerheden 2021

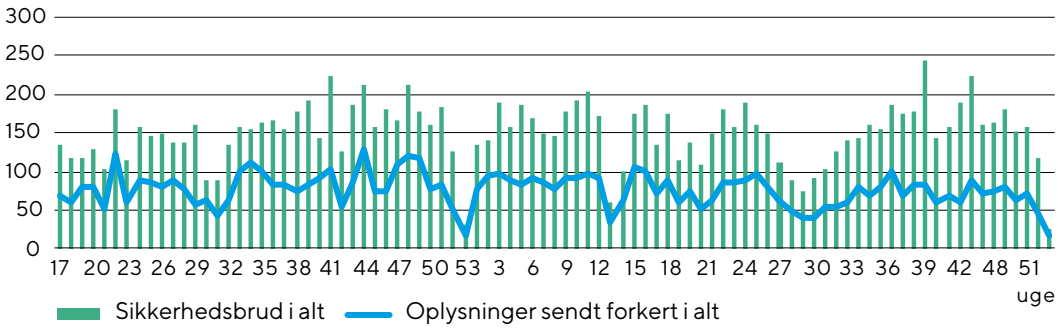
Datatilsynet modtager fortsat en stor mængde anmeldelser om brud på persondatasikkerheden. I 2021 blev der anmeldt 8.554 sikkerhedsbrud i alt. I uge 46, hvor tilsynet modtog flest anmeldelser af brud på persondatasikkerheden, blev der anmeldt 561 sikkerhedsbrud.

Som et led i en ny strategi for en mere data- og risikobaseret indsats begyndte Datatilsynet i 2020 at lave 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.

Datatilsynet ser fortsat en klar tendens til, at størstedelen af de anmeldte brud på persondatasikkerheden vedrører personoplysninger, der sendes forkert (se diagram nedenfor), enten fordi 1) oplysningerne utilsigtet sendes til en forkert modtager, eller fordi 2) det utilsigtet er de forkerte oplysninger, der bliver sendt til modtageren.

Personoplysninger, der er sendt forkert, udgør således over halvdelen af alle sikkerhedsbrud anmeldt til Datatilsynet siden uge 17 2020 (8.235 af 13.364). Størstedelen af denne type brud vedrører personoplysninger, der utilsigtet er sendt til en forkert modtager (6.991 af 8.235).

Andelen af sikkerhedsbrud der omhandler personoplysninger sendt til en forkert modtager



*Datagrundlaget for diagrammet er anmeldelser om brud på persondatasikkerheden fra uge 17 (2020) frem til uge 52 (2021). Årsagen til starttidspunktet er, at Datatilsynet fra uge 17 i 2020 begyndte at klassificere anmeldelserne i bestemte hændelsestyper.

Serie af utilsigtede videregivelser af personoplysninger

I årene 2018 til 2020 anmeldte Familieretshuset 158 brud på persondatasikkerheden til Datatilsynet. Af disse handlede mere end 130 sager om utilsigtet videregivelse af personoplysninger, og 34 af disse omhandlede beskyttede navne- og adresseoplysninger. I en række af sagerne var der tale om høj risiko for de registreredes rettigheder; så høj, at videregivelse i enkelte tilfælde kunne påvirke sikkerhed, liv og helbred.

På den baggrund indledte Datatilsynet i 2021 en sag af egen drift over for Familieretshuset med henblik på at afdække årsagen til disse bruds opståen. Familieretshuset iværksatte med hjælp fra en konsulentvirksomhed en intern undersøgelse og fremsendte denne til Datatilsynet.

Af redegørelsen fremgik det, at Familieretshuset organisatorisk bygger på det tidligere Statsforvaltningen, og at arbejdet med implementering, databeskyttelse og informationssikkerhed historisk set ikke har været tilstrækkeligt prioriteret. Dette har efterladt en betydelig organisatorisk og teknisk gæld og en generel lav modenhed.

Familieretshuset oplyste, at en række af de utilsigtede videregivelser af personoplysninger skyldtes manuelle og menneskelige behandlingsfejl. For at imødegå disse iværksatte Familieretshuset en større implementeringsplan, der skitserede en række aktiviteter og fokusområder. Bl.a. blev der udpeget en gruppe decentrale ambassadører, der i løbet af 2021 ville blive uddannet i en lang række centrale databeskyttelsesretlige spørgsmål. Familieretshuset ville også sætte fokus på procedurer og arbejdsgange, gennemgang af databehandleraftaler, udarbejdelse af en ny politik for databeskyttelse efter databeskyttelsesforordningen og uddannelse af de decentrale ambassadører.

Det fremgik endvidere af Familieretshusets redegørelse, at der ikke var indgået databehandleraftale med en af deres leverandører, og at den indgåede databehandleraftale med en anden leverandør ikke levede op til kravene i databeskyttelsesforordningen.

Familieretshuset administrerer i alt 40 it-løsninger inden for blandt andet adoption, bidrag, faderskab, forældreansvar, klager, skilsmisse, værgemål og ægteskab for internationale par, som borgere har adgang til (selvbetjeningsløsninger). For adskillige af disse løsninger havde Familieretshuset konstateret brud på persondatasikkerheden forbundet med utilsigtet videregivelse af navn på borgere med navne- og adressebeskyttelse. Årsagen var en teknisk mangel i form af en kodefejl i et CPR-kald, der anvendtes i de løsninger, der blev udbudt af leverandørerne. Løsningerne blev taget ud af drift, indtil fejlene var rettet.

Rapporten om forretningsgange og tekniske aktiviteter konkluderede, at alle de identificerede databrud i forbindelse med CPR-kald havde eksisteret i løsningerne siden deres implementering flere år tidligere og var dokumenteret til at have en teknisk karakter. Det fremgik endvidere af undersøgelsen, at Familieretshusets organisation historisk havde været vidende om fejlen og konsekvenserne for mindst én af løsningerne, hvilket dog ikke førte til effektiv afhjælpning. Konsulentvirksomheden konkluderede bl.a., at en manglende forankring i risikovurderinger, politikker og procedurer havde været medvirkende til, at organisationen og ledelsen ikke effektivt havde fået kommunikeret og afhjulpet bruddene tidligere.

Datatilsynet fandt, at Familieretshuset ikke havde udført tilstrækkelig og regelmæssig afprøvning af de udviklede selvbetjeningsløsninger, inden de blev sat i drift, og at de anvendte testmiljøer ikke var af en karakter, der gjorde dem egnede til at udføre denne afprøvning. Derved havde Familieretshuset ikke opfyldt databeskyttelsesforordningens artikel 32, stk. 3, litra d.

Det var endvidere Datatilsynets opfattelse, at løsninger, der indeholder oplysninger af den karakter, Familieretshuset behandler, ikke bør være designet til at eksponere data som standardindstilling, men i stedet være designet til – som udgangspunkt – at beskytte personoplysningerne og kun eksponere dem, når det er relevant.

Herudover fandt Datatilsynet, at Familieretshuset ikke i tilstrækkelig grad havde sikret, at medarbejderne havde den fornødne omhu ved behandling af borgernes personoplysninger, herunder beskyttede navne- og adresseoplysninger. Derved havde Familieretshuset ikke levet op til databeskyttelsesforordningens artikel 32, stk. 1, litra b.

Det var i den forbindelse Datatilsynets vurdering, at flere af de menneskelige fejl kunne være undgået under iagttagelse af fornøden omhu fra medarbejdernes side, ligesom en ekstra kontrol, der blev udført af en anden sagsbehandler, åbenbart ikke var tilstrækkelig effektiv. Datatilsynet udtalte alvorlig kritik af, at Familieretshusets behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1.

Endvidere fandt Datatilsynet, at der var grundlag for at udtale alvorlig kritik af, at Familieretshuset ikke – i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 3 – havde iagttaget kravet om skriftlig databehandleraftale og udarbejdelse af en skriftlig databehandlerinstruks.

Samlet set gav gennemgangen anledning til, at Datatilsynet udtalte alvorlig kritik af Familieretshusets overtrædelser af databeskyttelsesforordningen.

Brud på persondatasikkerheden undersøgt for sent

Datatilsynet udtalte i 2021 alvorlig kritik af, at Justitsministeriets departement (herefter Justitsministeriet) ikke havde passende sikkerhed i overensstemmelse med databeskyttelsesforordningens artikel 32 i forbindelse med afsendelse af e-mails. Datatilsynet udtalte ligeledes alvorlig kritik af Justitsministeriets håndtering af bruddet. Endelig gav tilsynet Justitsministeriet et påbud om at foretage underretning af de berørte registrerede i overensstemmelse med forordningens artikel 34.

Justitsministeriet blev informeret om et muligt brud den 18. november 2019. Bruddet angik Justitsministeriets afsendelse af en e-mail med oplysninger om 35 personers navne, personnumre og oplysninger om gæld, hvor det ikke kunne dokumenteres, at transmissionen over internettet skete med anvendelse af kryptering. Det var Datatilsynets opfattelse, at kravet i databeskyttelsesforordningens artikel 32 om passende sikkerhed normalt vil indebære, at det vil være en passende sikkerhedsforanstaltning at anvende kryptering ved transmission af fortrolige og følsomme personoplysninger med e-mail via internettet, og at håndtering af mange personers personoplysninger i én og samme forsendelse stiller større krav til medarbejdernes omhyggelighed i forbindelse med fremsendelse.

IT-leverandøren blev først involveret i undersøgelsen den 3. februar 2020. Ved den slags undersøgelser kan det gøre en forskel, hvor hurtigt der reageres, idet logs forsvinder med tiden, og en tidlig henvendelse til en it-leverandør kan dermed give flere og mere præcise svar. Det var Datatilsynets opfattelse, at de mere end 3 måneder, der gik inden anmeldelsen til Datatilsynet den 28. februar 2020, var en unødig forsinkelse, idet de faktuelle oplysninger kunne og burde have været opklaret tidligere.

Af anmeldelsen fremgik det, at Justitsministeriet ikke havde og ikke agtede at underrette de berørte registrerede. Ved vurderingen af mulige konsekvenser – og dermed risici – for de berørte registrerede og begrundelsen for at undlade underretning af de registrerede om bruddet, havde Justitsministeriet lagt vægt på, at der ikke ministeriet bekendt var indikationer på, at uvedkommende rent faktisk har fået adgang til oplysningerne.

Datatilsynet fandt imidlertid, at ikke-krypterede transmissioner over internettet indebærer muligheden for "skjult" adgang til oplysningerne, som den dataansvarlige ingen kontrol har over. Det forhold, at Justitsministeriet ikke var bekendt med uvedkommendes adgang til data, ændrede derfor ikke på den risiko, som bruddet udgjorde for de registrerede.

Et misbrug af personoplysninger kan endvidere ske lang tid efter, at bruddet er sket, og konsekvenserne kan dermed være fremtidige. Dette er endnu en grund til, at man i denne sag ikke kunne tillægge manglende *aktuel* viden om realiserede konsekvenser nogen større betydning i sin vurdering af risici. Det var derfor Datatilsynets opfattelse, at Justitsministeriet ikke havde foretaget en reel vurdering af de risici, som bruddet har udgjort og stadig kan udgøre for de registreredes rettigheder.

Forkert ikke at foretage underretning

Datatilsynet har i 2021 udtalt alvorlig kritik af, at Skatteforvaltningen ikke underrettede en berørt borger om et brud på persondatasikkerheden i tide.

Skatteforvaltningen havde anmeldt et brud på persondatasikkerheden til tilsynet. Af anmeldelsen fremgik det, at Skatteforvaltningen havde underrettet den borger, der var berørt af bruddet, to dage før, at styrelsen havde anmeldt bruddet til Datatilsynet.

Datatilsynet modtog imidlertid en opfølgning på anmeldelsen fra Skatteforvaltningen over en måned senere, hvori Skatteforvaltningen informerede tilsynet om, at der ikke var sket underretning af den registrerede, som beskrevet i den første anmeldelse - men først ca. 40 dage senere.

Det var i den forbindelse Datatilsynets opfattelse, at et helt grundlæggende formål med pligten til at underrette registrerede er, at de registrerede skal være i stand til at varetage sine interesser, hvis de er berørt af et sikkerhedsbrud.

Det var i forlængelse heraf Datatilsynets opfattelse, at tilsynet skal være i stand til at varetage de registreredes rettigheder, hvis der ikke er sket (korrekt) underretning af de registrerede - f.eks. ved at påbyde den dataansvarlige at underrette de(n) registrerede.

Datatilsynet lagde derfor særlig vægt på, at hverken den registrerede eller tilsynet var i stand til at varetage den registreredes rettigheder, når den registrerede ikke var blevet underrettet om bruddet på persondatasikkerheden, og når Datatilsynet var givet forkerte informationer i anmeldelsen, som gav Datatilsynet anledning til at tro, at den registrerede *var* blevet underrettet om hændelsen. Datatilsynet bemærkede i den forbindelse, at det er af afgørende betydning for beskyttelsen af de registrerede, deres rettigheder og deres frihedsrettigheder, at informationer i en anmeldelse af brud på persondatasikkerheden om, at der er sket underretning af berørte registrerede, er korrekte.

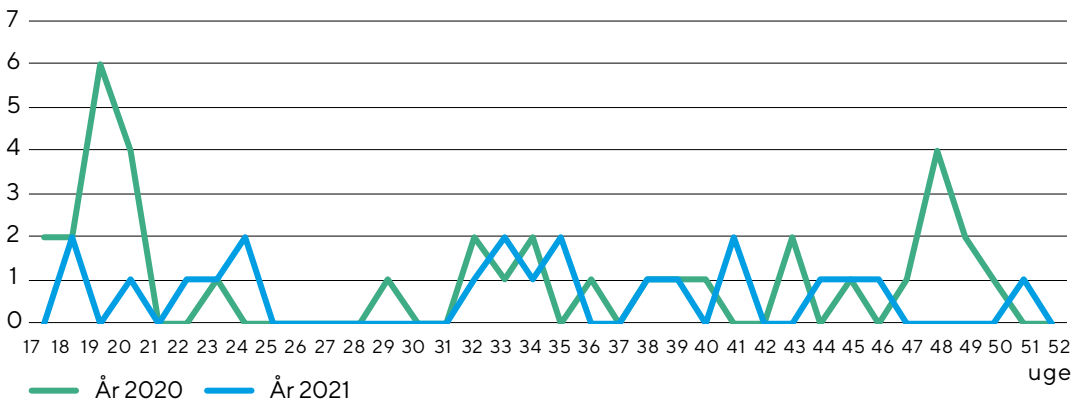
Sikkerhedstips om ransomware

Datatilsynet får løbende anmeldelser om brud på persondatasikkerheden, der bunder i ransomware-angreb. Et ransomware-angreb eller anden cyberkriminalitet skal på linje med andre brud på persondatasikkerheden anmeldes til Datatilsynet, medmindre det er usandsynligt, at bruddet har medført en risiko for personers rettigheder eller frihedsrettigheder

Et ransomware-angreb er en situation, hvor uvedkommende skaffer sig adgang til et it-system, krypterer filerne og kræver et beløb for at frigive dem. Ifølge Center for Cybersikkerhed ses en nyere tendens i ransomware-angrebene - såkaldt 'dobbelt-afpresning' - hvor ofrene udover at risikere at miste tilgængeligheden af vigtige it-systemer også risikerer, at følsomme person- eller forretningsoplysninger bliver offentliggjort eller solgt videre. For yderligere oplysninger om denne udvikling, henviser Datatilsynet til Center for Cybersikkerhed.

Datatilsynet har i 2021 ikke som forventet iagttaget en generel stigning i antallet af anmeldte ransomware-angreb, jf. diagrammet nedenfor. Dette på trods af, at Center for Cybersikkerhed i 2021 vurderede trusselsniveauet til det højst mulige (Center for Cybersikkerhed 2021). Der kan være mange forklaringer på, at anmeldelsestallet ikke er steget. Det kan skyldes højt sikkerhedsniveau hos de dataansvarlige; at angrebene ikke omfatter personoplysninger og/eller at angrebene ikke bliver anmeldt. Overordnet set, er det Datatilsynets vurdering, at der givetvis er et mørketal på området, og at det reelle tal for danskrettede ransomware-angreb, der omfatter personoplysninger, er større, end hvad anmeldelsestallene viser.

Antal anmeldte ransomware-angreb. Sammenlignelige periodeudsnit i 2020 og 2021



*Datagrundlaget for diagrammet er anmeldelser om brud på persondatasikkerheden fra uge 17 (2020) frem til uge 52 (2021). Årsagen til starttidspunktet er, at Datatilsynet fra uge 17 i 2020 begyndte at klassificere anmeldelserne i bestemte hændelsestyper.

Logningsfejl i it-system tilknyttet Udrejsecenter Kærshovedgård

Datatilsynet politianmeldte Udlændingestyrelsen i august 2021 på baggrund af en sag, som Datatilsynet indledte i august 2020 af egen drift over for Udlændinge- og Integrationsministeriet.

Datatilsynet var gennem medieomtale blevet bekendt med, at en mulig logningsfejl i et it-system tilknyttet Udrejsecenter Kærshovedgård kunne have haft konsekvenser for beboernes rettigheder og frihedsrettigheder. Efter en undersøgelse af sagen stod det klart, at Udlændingestyrelsen var dataansvarlig for behandlingen af personoplysninger i forbindelse med kontrol af beboernes opholds- og underretningspligt på Udrejsecenter Kærshovedgård og Udrejsecenter Sjælsmark.

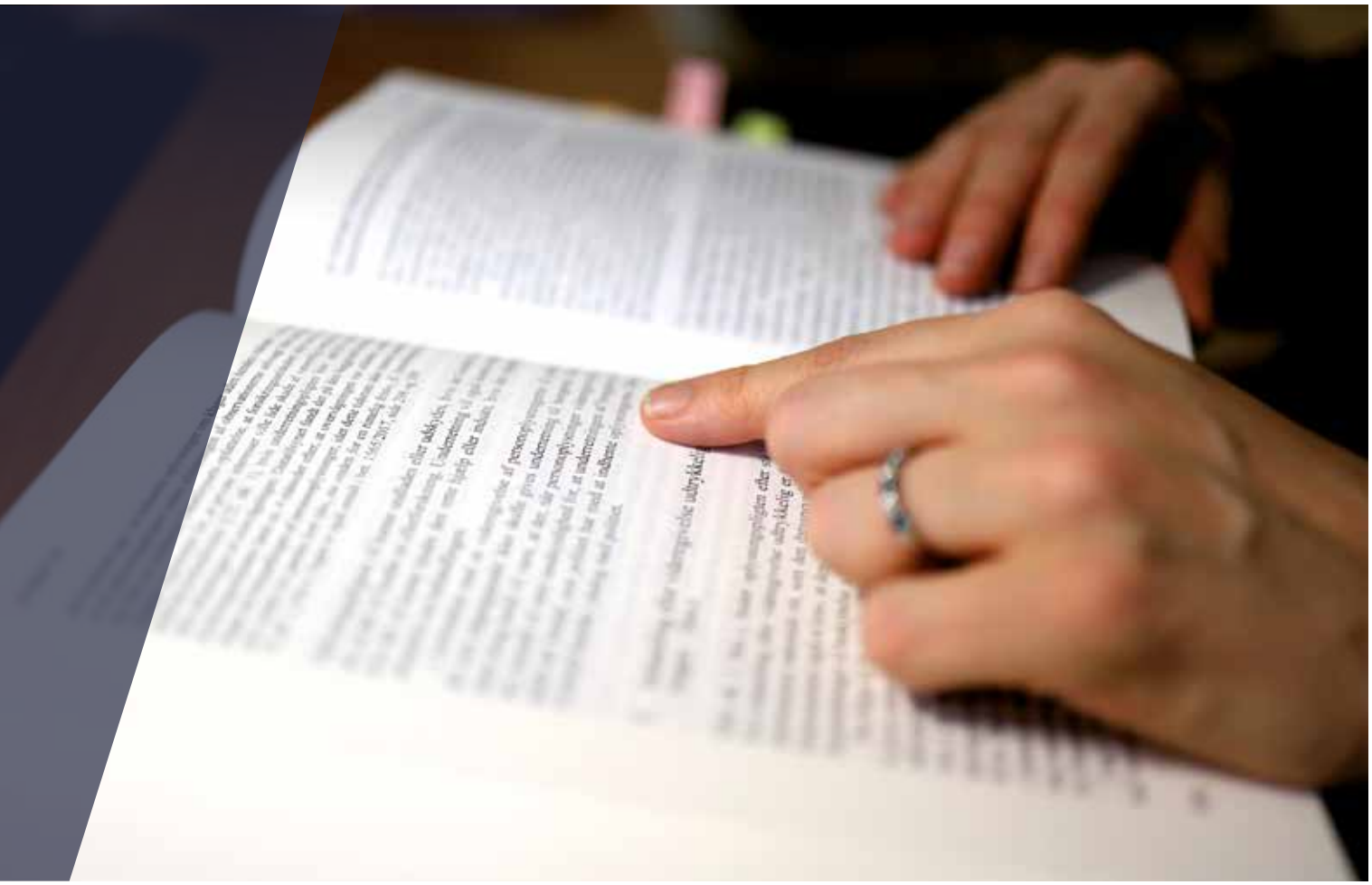
I foråret og sommeren 2020 skete en række sikkerhedshændelser vedrørende manglende registreringer i det system, som registrerer, at beboere på Udrejsecenter Kærshovedgård og Udrejsecenter Sjælsmark overholder deres opholds-, underretnings- og meldepligt (SALTO-systemet). De manglende registreringer førte til, at der blev påbegyndt sagsbehandling vedrørende nedsættelse af en række beboeres kontante ydelser samt politianmeldelse af en række beboere for manglende overholdelse af regler i udlændingeloven. Efter Datatilsynets henvendelse til Udlændinge- og Integrationsministeriet om sagen, anmeldte Udlændingestyrelsen den 10. september 2020 et sikkerhedsbrud vedrørende sagen til Datatilsynet.

Efter en gennemgang af sagen fandt Datatilsynet, at Udlændingestyrelsens behandling af personoplysninger ikke har været i overensstemmelse med reglerne om passende sikkerhed.

Datatilsynet lagde vægt på, at Udlændingestyrelsen ikke havde indført procedurer for systematisk at anvende oplysningerne i den hændelseslog, som registrerer beboernes færden inde på Udrejsecenter Kærshovedgård og Udrejsecenter Sjælsmark i forbindelse med behandlingen af anmeldelsessager som led i kontrollen med opholds- og underretningspligten.

Herudover lagde Datatilsynet vægt på, at Udlændingestyrelsen ikke havde identificeret og forholdt sig til risici for de registrerede i forbindelse med behandlingsaktiviteterne i SALTO-systemet.

Endelig lagde Datatilsynet vægt på, at Udlændingestyrelsen – henset til retsvirkningerne for beboerne forbundet med de pågældende registreringer – ikke havde foretaget tilstrækkelig backup af de oplysninger, som behandles i SALTO-systemet. Det var derfor ikke muligt for styrelsen at genskabe en række af de data, som gik tabt under en sikkerhedshændelse den 9.-10. juni 2020.



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 2021:

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 har i 2021 kun behandlet få nye sager 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.

Advarselsregister – fra gamle til nye vilkår

Det er efter databeskyttelseslovens § 26, stk. 1, nr. 1, et krav, at der skal indhentes en tilladelse fra Datatilsynet, hvis behandling af personoplysninger, der foretages for en privat dataansvarlig, sker med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret – et såkaldt advarselsregister.

En særlig form for advarselsregistre er spærrelister, der specifikt angår spærring af betalingskort og andre betalingsinstrumenter, og som har til formål at undgå bl.a. misbrug af et stjålet eller på anden vis bortkommet betalingskort.

Kravet om indhentelse af Datatilsynets forudgående tilladelse til behandling af oplysninger i forbindelse med førelse af et advarselsregister eller en spærreliste fulgte også af den tidligere gældende persondatalovs § 50, stk. 1, nr. 2.

I november 2019 vedtog Datatilsynet – som følge af overgangen til databeskyttelsesforordningen og databeskyttelsesloven – nye opdaterede standardvilkår for privates behandling af oplysninger i forbindelse med førelse af advarselsregistre og spærrelister. Vilkårene præciserer og supplerer reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

Datatilsynet har i forlængelse af vedtagelsen af de nye standardvilkår for advarselsregistre og spærrelister arbejdet på at flytte alle eksisterende tilladelser meddelt efter persondatalovens § 50, stk. 1, nr. 2, over på nye vilkår efter databeskyttelseslovens § 26, stk. 1, nr. 1.

I 2021 færdiggjorde Datatilsynet sit arbejde med at flytte alle 115 eksisterende tilladelser til advarselsregistre og spærrelister udstedt efter de tidligere gældende regler over på nye vilkår, som nu er blevet meddelt de enkelte dataansvarlige for behandlingerne.

Tilladelse til at oprette advarselsregister inden for den maritime sektor

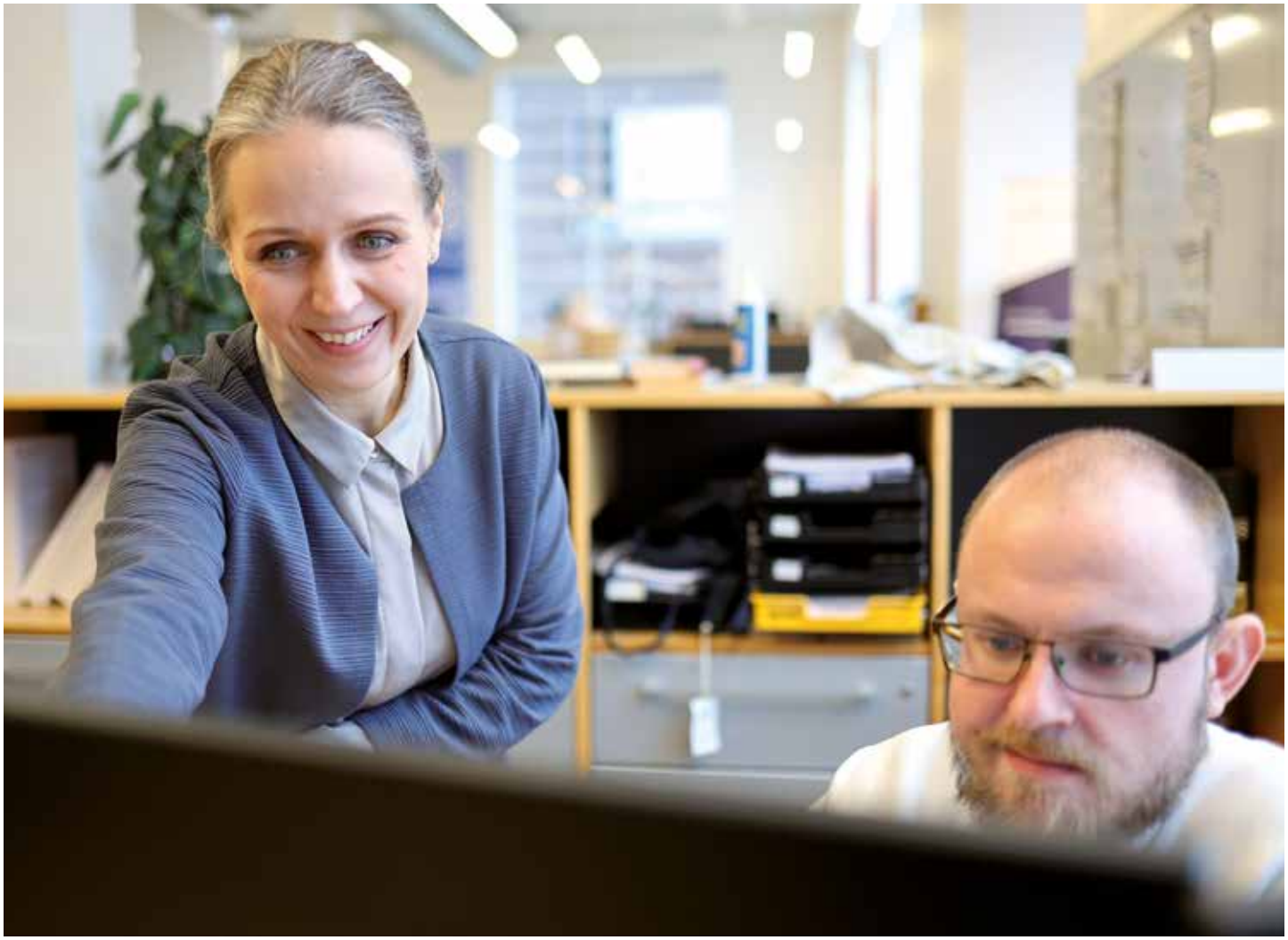
The Baltic and International Maritime Council (BIMCO) ansøgte om Datatilsynets tilladelse til førelse af et advarselsregister over virksomheders status og omdømme inden for den maritime sektor.

BIMCO oplyste, at formålet med advarselsregistret er at kunne give BIMCO's medlemmer oplysninger om andre virksomheders status og omdømme med henblik på at hjælpe medlemmerne med at vurdere, om de ønsker at indgå i et samarbejds-/kontraktforhold med en given virksomhed.

Efter ansøgningen havde været forelagt Datarådet, meddelte Datatilsynet i 2021 BIMCO tilladelse til behandling af oplysninger i forbindelse med førelse af et advarselsregister over virksomheders status og omdømme. Tilladelsen blev meddelt på en række nærmere angivne vilkår, herunder en række vilkår for optagelse i advarselsregistret med henblik på at sikre, at optagelse i registret ikke beror på subjektive vurderinger.

Af disse vilkår fremgår bl.a., at der kun må ske registrering og videregivelse af offentligt tilgængelige oplysninger om en person og/eller virksomhed under forudsætning af, at oplysningerne er objektivt konstaterbare eller fremstår tilstrækkeligt underbyggede.

Datatilsynet fastsatte også et vilkår om, at der ikke må ske registrering eller videregivelse af oplysninger om strafbare forhold eller oplysninger omfattet af databeskyttelsesforordningens artikel 9.



Tilladelse til at drive kreditoplysningsbureau

Datatilsynet behandlede i 2021 en ansøgning fra virksomheden Coface Norden Services A/S.

Coface er et internationalt kreditforsikringsselskab med filialer og koncernselskaber i mere end 60 lande. Kreditforsikring indebærer, at forsikringstager forsikrer sig mod tab på debitorer som følge af debitorernes manglende evne til at opfylde sine betalingsforpligtelser.

Da Coface påtænkte at lancere en række kreditvurderingsprodukter og kreditoplysningsprodukter på det danske marked, ansøgte selskabet i henhold til databeskyttelseslovens §§ 19 og 26, stk. 1, nr. 2, Datatilsynet om tilladelse til at drive virksomhed med behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse (kreditoplysningsbureau).

Coface oplyste i den forbindelse, at virksomheden ønskede at tilbyde kreditvurderingsprodukter til forsikringstagerne samt formidling af kreditoplysningsprodukter, der ligeledes indeholdt en kreditbedømmelse.

Oplysninger til brug for den enkelte kreditvurdering ville blive indhentet hos eksterne kilder og suppleret med egne oplysninger, herunder oplysninger fra forsikringstagerne.

Datatilsynet vurderede, at den påtænkte behandling ville have karakter af et kreditoplysningsbureau og gav virksomheden tilladelse til at drive kreditoplysningsbureau.

Datatilsynet fastsætte i den forbindelse nærmere vilkår for behandlingen, jf. databeskyttelseslovens § 26, stk. 4.

Godkendelse af adfærdskodeks

Datatilsynet godkendte i sommeren 2021 en adfærdskodeks om behandling af personoplysninger som led i sognepleje for menighedsråd i Danmark. Adfærdskodeksen, der er udarbejdet af Kirkeministeriet i samarbejde med Landsforeningen af Menighedsråd, er den første af sin art herhjemme.

Adfærdskodeksen opstiller konkrete retningslinjer og procedurer med henblik på at sikre en lovlig behandling af personoplysninger for menighedsrådet som dataansvarlig. Særligt indgår emner som dataansvar, de generelle behandlingsprincipper, behandlingsgrundlag, oplysningspligten, sikker opbevaring og sikker kommunikation mv.

Målet med adfærdskodeksen er at lette overholdelsen af de databeskyttelsesretlige regler for de menighedsråd, der tilslutter sig kodeksen.

Det er frivilligt at tilslutte sig kodeksen, og det er kun de menighedsråd, som formelt vælger at tilslutte sig kodeksen, som skal overholde de indeholdte retningslinjer og procedurer.

Konsekvensanalyser af Coronapas-appen

I 2021 foretog Datatilsynet en vurdering af to konsekvensanalyser fra SSI vedrørende forskellige versioner af Coronapas-appen. På baggrund af sagens hastende karakter rådgav Datatilsynet – fortløbende – SSI om indholdet af den første version af analysen, ligesom tilsynet stillede en række supplerende spørgsmål til behandlingen.

Datatilsynet fik undervejs adgang til yderligere relevant dokumentation af løsningen og rapporter fra den eksterne sikkerhedstest. En opdateret version af konsekvensanalysen gav også anledning til, at Datatilsynet stillede en række uddybende spørgsmål til SSI, Sundhedsdatastyrelsen(SDS) (som databehandler for SSI) og BDO (som reviewer af systemet).

Datatilsynet påpegede mangler bl.a. ved behandlingssikkerheden og mindre uhensigtsmæssigheder, der symptomatisk fremgik af eksterne reviews og rapporter. Datatilsynet indskærpede, at der for disse blev udarbejdet en plan for udbedring.

På baggrund af det samlede fremsendte materiale, de afhjælpende foranstaltninger i konsekvensanalysen og de anbefalinger, Sundhedsministeriets databeskyttelsesrådgiver (DPO) havde anført, konkluderede Datatilsynet i slutningen af maj 2021, at SSI som dataansvarlig i tilstrækkeligt omfang havde identificeret og begrænset risikoen ved den pågældende behandling.

Datatilsynet behandlede i perioden frem til begyndelsen af juli 2021 yderligere konsekvensanalyser for version 1.1 og 1.2 af Coronapas-appen.

Datatilsynet påpegede generelt, at det ikke må blive det normale modus, at komplekse behandlingssituationer skal gennemføres med en sådan hast, at både it-udviklingen og de juridiske vurderinger, der skal foretages af den dataansvarlige, ikke til fulde får behandlet og nedbragt de risici, der er for de regi-

strerede. Tilsynet indskærpede på den baggrund, at der ved disse komplekse behandlingssituationer, hvor der typisk vil være en høj risiko for de registreredes rettigheder, skal skabes fornødent tidsmæssigt rum i projektforløb, beslutningsprocesser med videre. Dette skal også inkludere en forventet – normal – sagsbehandlingstid i Datatilsynet.

På baggrund af undersøgelsen, og hvis de anbefalinger, der fremgik af konsekvensanalysen og i risikovurderingen – som afhjælpende foranstaltninger – blev implementeret inden behandlingens opstart, var det Datatilsynets opfattelse, at SSI som dataansvarlig i tilstrækkeligt omfang havde identificeret og begrænset risikoen ved den pågældende behandling.

Internationalt arbejde

Med databeskyttelsesforordningen har det internationale samarbejde fået en ny og større betydning. Databeskyttelsesområdet er nu i langt højere omfang reguleret på EU-niveau, ligesom der med forordningen er etableret et mere formaliseret samarbejde mellem de europæiske tilsynsmyndigheder.

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 fastsat en række strategiske målsætninger for det internationale arbejde, som skal være med til at 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 2021 har det internationale samarbejde fortsat i høj grad været præget af COVID-19-udbruddet i form af fysiske møder, som enten er blevet afholdt online eller er blevet udskudt. I EDPB-regi har der navnlig været fokus på at klarlægge 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 ca. en gang om måneden. Som følge af COVID 19-situationen blev der dog i 2021 kun afholdt et enkelt fysisk møde, mens 13 møder blev afholdt online.

Arbejdet med forberedelsen af vejledninger, udtalelser, afgørelser mv., som EDPB skal godkende, foreståsprimært af 12 ekspertarbejdsgrupper, som normalt mødes med 1-2 måneders intervaller i Bruxelles. Som følge af COVID 19-situationen er arbejdsgruppemøderne dog i 2021 alle blevet afholdt online.

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

I 2021 vedtog EDPB en række vejledninger mv. om aktuelle databeskyttelsesretlige emner, herunder en vejledning om dataansvarlige og databehandlere.

EDPB havde fortsat fokus på at vejlede om de praktiske konsekvenser af EU-Domstolens dom i den såkaldte Schrems II-sag om overførsel af personoplysninger til tredjelande, herunder gennem vedtagelsen af anbefalinger om iværksættelse af supplerende foranstaltninger, når beskyttelsesniveauet i tredjelandet ikke er tilstrækkeligt. Endelig traf EDPB afgørelse i en sag om grænseoverskridende behandling af personoplysninger omfattet af den særlige tvistbilæggelsesprocedure i databeskyttelsesforordningen.

Bindende afgørelse – WhatsApp

I slutningen af juli 2021 vedtog EDPB en bindende afgørelse efter reglerne i databeskyttelsesforordningen om tvistbilæggelse.

I sager om grænseoverskridende behandling af personoplysninger skal der i overensstemmelse med samarbejdsmekanismen efter databeskyttelsesforordningen ("One-Stop-Shop") 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 tilsynsmyndigheder, 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.

I den konkrete sag, som vedrørte WhatsApp Irland havde det irske datatilsyn som ledende tilsynsmyndighed udarbejdet et udkast til en afgørelse. Afgørelsen omhandlede primært WhatsApp Irlands manglende opfyldelse af gennemsigtighedsforpligtelserne efter databeskyttelsesforordningen. En række berørte tilsynsmyndigheder gjorde indsigelser mod afgørelsen, som det irske datatilsyn ikke var enig i. Sagen blev derfor forelagt EDPB, der traf en bindende afgørelse.

I sin afgørelse anmodede EDPB det irske datatilsyn om at ændre sin afgørelse og følge en række af de fremsatte indsigelser, som navnlig drejede sig om overtrædelse af yderligere bestemmelser end dem, det irske datatilsyn i første omgang havde identificeret, udregningen af bødestørrelsen samt fristen for, at WhatsApp Irland skulle bringe sine behandlingsaktiviteter i overensstemmelse med databeskyttelsesforordningen.

For så vidt angår udregningen af bødestørrelsen slog EDPB i sin afgørelse fast, at virksomhedens omsætning ikke alene er relevant ved udregningen af det maksimale bødeloft, men også ved udregningen af selve bødestørrelsen for at sikre, at denne er effektiv, proportional og har afskrækkende virkning. Herudover fandt EDPB, at også moderselskabets omsætning skal tages i betragtning ved udregningen af bøden. EDPB fandt endvidere anledning til at præcisere, at hvis der er tale om flere overtrædelser for

den samme behandlingsaktivitet, skal alle overtrædelser hver især tages i betragtning ved udregning af bøden.

EDPB fandt endvidere i overensstemmelse med flere af de fremsatte indsigelser, at WhatsApp Irlands frist for at bringe sin behandling af personoplysninger i overensstemmelse med databeskyttelsesforordningen skulle nedsættes fra 6 måneder, som det irske datatilsyn havde fastsat, til 3 måneder.

Det irske datatilsyn traf – på baggrund af EDPB's afgørelse – endelig afgørelse i sagen den 20. august 2021. Afgørelsen indeholdt kritik af WhatsApp Irland, et påbud om at bringe behandlingsaktiviteterne i overensstemmelse med reglerne inden for en periode på 3 måneder samt en bøde på samlet 225 millioner euro.

WhatsApp Irland har efterfølgende den 1. november 2021 indbragt sagen for EU-Domstolen med henblik på at få EDPBs afgørelse annulleret. EU-Domstolen har endnu ikke taget stilling til sagen

Schrems II-sagen – endelige supplerende foranstaltninger

Den 16. 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 af 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 standardkontraktbestemmelser, som er et generelt retsgrundlag for overførsel af personoplysninger til lande uden for EU/EØS (såkaldte tredjelande). EU-Domstolen fastslog dog, at standardkontraktbestemmelserne fortsat er gyldige, men at der efter omstændighederne kan være behov for at iværksætte supplerende foranstaltninger, hvis beskyttelsesniveauet i tredjelandet ikke er tilstrækkeligt.

Datatilsynet iværksatte sammen med de andre europæiske tilsynsmyndigheder i regi af EDPB en nærmere analyse af dommen og dens praktiske konsekvenser. EDPB nedsatte i den forbindelse en task force, som fik til opgave at udarbejde anbefalinger om, hvordan behovet for iværksættelse af supplerende foranstaltninger – når databeskyttelsesniveauet i tredjelandet ikke er tilstrækkeligt – kan imødekommes i praksis.

Datatilsynet deltog i task forcens arbejde, som den 10. november 2020 resulterede i et udkast til anbefalinger, som efterfølgende blev sendt i offentlig høring. På baggrund af de modtagne høringssvar arbejdede task forcen i 2021 videre med udkastet til anbefalingerne, som blev endeligt vedtaget den 18. juni 2021.

Nye standardbestemmelser – tredjelandsoverførsler

Den 4. juni 2021 vedtog Europa-Kommissionen nye standardbestemmelser, som kan anvendes som et såkaldt overførselsgrundlag ved overførsel af personoplysninger til tredjelande.

Europa-Kommissionen har med de nye standardbestemmelser forsøgt at modernisere dem, så de i højere grad tager højde for den måde, behandling af personoplysninger finder sted i dag.

Forud for vedtagelsen af standardbestemmelserne vedtog EDPB den 14. januar 2021 – sammen med Den Europæiske Tilsynsførende for Databeskyttelse – en udtalelse, som kan findes på EDPB's hjemmeside.

Brexit

Med udtrædelsen af EU blev Storbritannien et tredjeland i databeskyttelsesforordningens og retshåndhævelseslovens forstand, hvilket indebærer, at man ved overførsel af personoplysninger til Storbritannien som udgangspunkt skal tilvejebringe et såkaldt overførselsgrundlag.

Som led i udtrædelsesaftalen vedtog man dog i første omgang en overgangsperiode, der gjaldt indtil udgangen af juni 2021, og som sikrede, at personoplysninger kunne overføres til Storbritannien uden et overførselsgrundlag.

Europa-Kommissionen har efterfølgende den 28. juni 2021 godkendt Storbritannien som et sikkert tredjeland – både i relation databeskyttelsesforordningen og retshåndhævelsesloven. Det skete ved udstedelsen af to såkaldte tilstrækkelighedsafgørelser, som betyder, at der også fremover kan overføres personoplysninger til Storbritannien uden et særligt overførselsgrundlag.

Tilstrækkelighedsafgørelse – Sydkorea

Den 24. september 2021 vedtog EDPB en udtalelse om Europa-Kommissionens udkast til en tilstrækkelighedsafgørelse vedrørende Sydkorea. Udtalelsen kan findes på EDPB's hjemmeside.

Databeskyttelsesforordningen giver mulighed for, at Europa-Kommissionen kan træffe en tilstrækkelighedsafgørelse, hvis beskyttelsesniveauet for personoplysninger i et tredjeland i det væsentlige svarer til beskyttelsesniveauet i EU/EØS. I daglig tale kaldes lande, som er omfattet af en tilstrækkelighedsafgørelse, for "sikre tredjelande".

Tilstrækkelighedsafgørelsen vedrørende Sydkorea blev godkendt den 17. december 2021. Sydkorea anses nu for at være et sikkert tredjeland, man som dataansvarlig og/eller databehandler kan overføre personoplysninger til uden et særligt overførselsgrundlag.

Særlige internationale tilsynsforpligtelser

Datatilsynet fører tilsyn med danske myndigheders behandling af personoplysninger, når de anvender en række EU-informationssystemer, som beskrives nærmere nedenfor.

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 igangsatte i 2021 to tilsyn vedrørende Rigspolitiets behandling af personoplysninger i relation til SIS II.

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 2021 afholdt to møder, hvor gruppen bl.a. har drøftet udkastet til en ny forordning for Schengenevaluerings- og overvågningsmekanismen.

Repræsentanter for Europa-Kommissionen og eu-LISA har endvidere deltaget på møderne med henblik på at drøfte aktuelle databeskyttelsesretlige spørgsmål og holde gruppen underrettet om

den aktuelle situation for SIS II. I den forbindelse har Europa-Kommissionen bl.a. informeret om implementeringen af de nye SIS-retsakter og forberedelse af oplysningskampagner om det nye SIS, som forventeligt vil idriftsættes i 2022.

Datatilsynet har også i 2021 fremsendt et spørgeskema udarbejdet af SIS II SCG til Rigspolitiet med henblik på indsamling af oplysninger vedrørende en specifik type indberetninger i SIS II.

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

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.

Toldstyrelsen er dataansvarlig for CIS i Danmark, mens Datatilsynet er tilsynsmyndighed. Datatilsynet fører således tilsyn med behandlingen af informationer i den danske del af CIS.

Datatilsynet foretog i 2021 et tilsyn med Toldstyrelsens behandling af personoplysninger i CIS.

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 2021 været afholdt et møde i Koordinationsgruppen for tilsynet med Toldinformationssystemet.

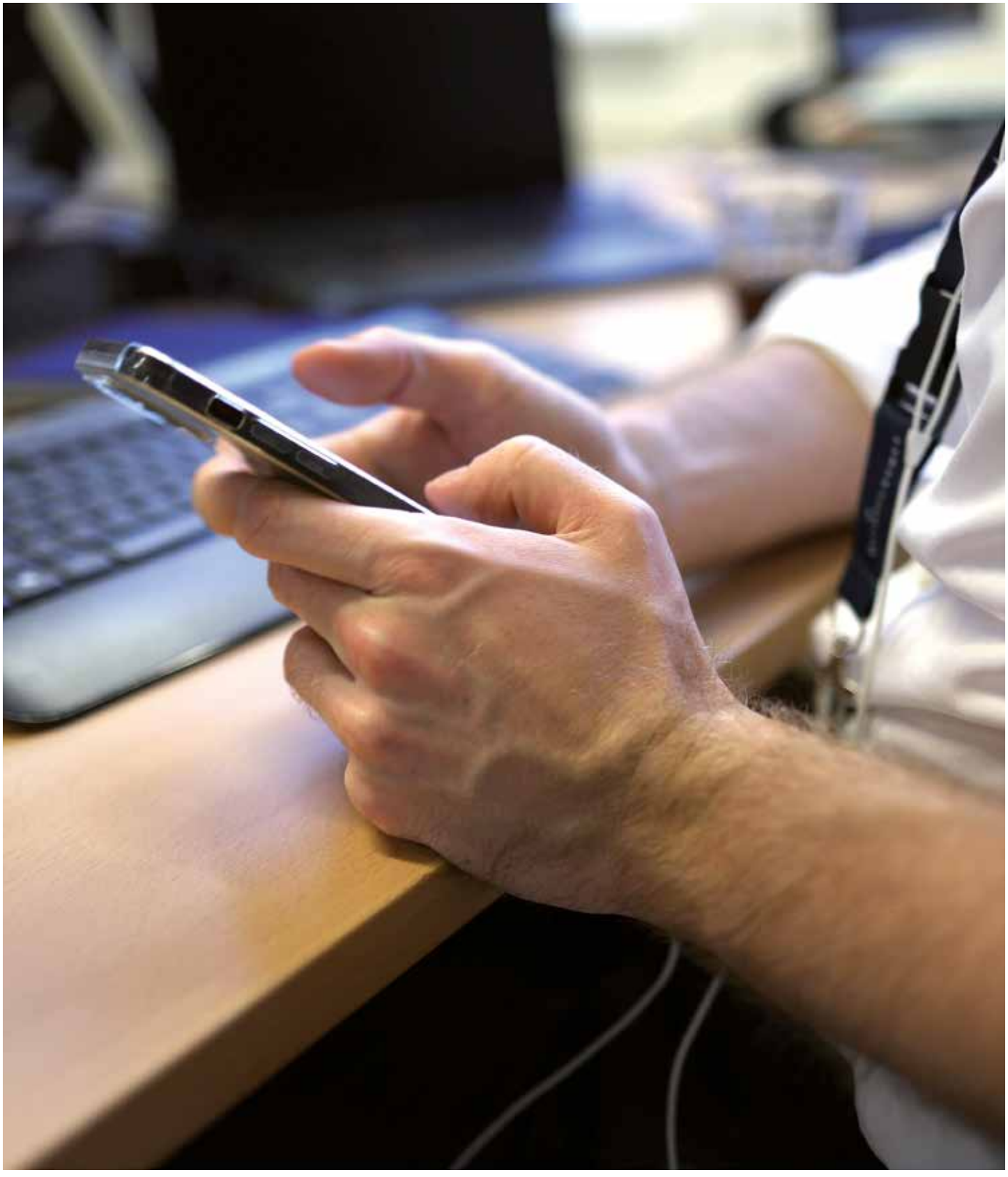
På Datatilsynets hjemmeside under punktet "Internationalt" findes generel information om CIS og Datatilsynets opgaver i relation til CIS, herunder muligheden for at klage til Datatilsynet over behandling af personoplysninger i CIS.

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. I 2021 har Datatilsynet igangsat et tilsyn med Rigspolitiets behandling af personoplysninger i relation til Eurodac.

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 2021 har der været afholdt to møder, hvor gruppen bl.a. har haft besøg af repræsentanter for Europa-Kommissionen og eu-LISA med henblik på orienteringer om den seneste udvikling på området og drøftelser af de aktuelle databeskyttelsesretlige problemstillinger, herunder Europa-Kommissionens forslag til en ny Eurodac-forordning. Herudover har gruppen bl.a. drøftet følgende emner:

- En struktureret måde for afrapportering til gruppen om nationale tilsyn.
- Færdiggørelsen af et projekt med Fundamental Rights Agency (FRA) vedrørende udøvelsen af registreredes rettigheder.
- Udarbejdelsen af en udtalelse vedrørende forslaget til en ny Eurodac-forordning.



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.

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 har i 2021 igangsat et tilsyn vedrørende behandling af personoplysninger i VIS.

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 2021 har der været afholdt to møder, hvor koordinationsgruppen bl.a. har haft besøg af repræsentanter for Europa-Kommissionen og eu-LISA, som har orienteret gruppen om den seneste udvikling på området, herunder forhandlingerne om og den efterfølgende vedtagelse af Europa-Kommissionens forslag til en revideret VIS-forordning. Der har derudover bl.a. været drøftet følgende emner:

- Arbejdet med en fælles tilsynsplan til brug for nationale tilsynsmyndigheders tilsyn med VIS.
- Udarbejdelse og vedtagelse af et spørgeskema vedrørende sletning af oplysninger i VIS før tid.

Datatilsynet har i 2021 fremsendt ovennævnte spørgeskema udarbejdet af VIS SCG til Udlændinge- og Integrationsministeriet med henblik på indsamling af oplysninger vedrørende sletning før tid i VIS.

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

IMI

Indre Markedsinformationssystemet (IMI) er et informationssystem oprettet af Europa-Kommissionen, som overordnet har til formål at lette europæiske myndigheders grænseoverskridende samarbejde og sagsbehandling.

Datatilsynet fører tilsyn med behandlingen af personoplysninger i den danske del af systemet. Fem offentlige myndigheder blev i 2020 udvalgt af Datatilsynet til skriftligt tilsyn med deres behandling af personoplysninger i IMI, og disse tilsyn blev afsluttet i løbet af 2021.

På EU-niveau deltager Datatilsynet i the Coordinated Supervision Committee (CSC), hvor de nationale datatilsyn sammen med Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) sikrer et koordineret tilsyn med behandlingen af personoplysninger i en række store EU-informationssystemer, herunder IMI. De nationale datatilsyn i EU's medlemsstater og i Island, Norge og Liechtenstein deltager i gruppens aktiviteter vedrørende IMI. Der har i 2021 været afholdt to møder i CSC.

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 2021 deltog Datatilsynet i Europarådets konvention 108-komitémøde. På mødet drøftedes en række aktuelle emner, herunder retshåndhævende myndigheders adgang til personoplysninger og digital identitet.

"Berlin-gruppen"

Den såkaldte Berlin-gruppe, der har skiftet navn til International Working Group on Data Protection in Technology, har i 2021 afholdt to virtuelle møder.

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

Berlin-gruppens fokus på privatliv og sikkerhed har i 2021 ført til vedtagelsen af et Working Paper.

Dokumentet "on the Risks emerging from the Tracking and Targeting Ecosystem in the Digital Advertising Market" omhandler de problemstillinger, der kan relateres til det såkaldte Adtech marked. Særligt databeskyttelsesretlige problemstillinger omkring tracking og målrettet reklame og mekanismerne omkring real-time bidding (salg af reklameplads i realtid, når man benytter hjemmesider mv.) er behandlet. Det er særligt brugen af samtykke, formålsglidning og profilering, der bliver behandlet. Der er i dokumentet fokus på den ugennemsigtige informationsindsamling hos den enkelte og det faktum, at den registrerede ikke har nogen- eller kun ringe sikkerhed for, hvordan oplysningerne benyttes. Gruppens mål har været at få lavet beskrivelser og oplæg til at adressere de pågældende problemstillinger.

I årets løb har Berlin-gruppen herudover arbejdet med aktuelle emner, som indeholder problemstillinger med hensyn til databeskyttelse og beskyttelse af privatliv, eksempelvis, Covid-19, ansigtsgenkendelse, blockchain, webtracking, smart dust, quantum computing, biometri i elektronisk online autentifikation, ISO-standardisering, privatlivsbeskyttelse ved ICANN's RDS (Registration Directory Services) for internettet, og forhold omkring forfølgelse og uønsket opmærksomhed i digital forstand, det såkaldte cyber bullying and stalking.

Nordisk samarbejde

Datatilsynet lægger stor vægt på at have et tæt samarbejde med de øvrige nordiske datatilsyn, da tilsynene har mange fælles interesser og synspunkter. De nordiske tilsyn er derfor i jævnlig kontakt om såvel konkrete som generelle emner.

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, som i 2021 skulle have været afholdt i Finland, blev imidlertid udskudt til 2022 som følge af COVID-19-udbruddet.

Den europæiske konference

Den Europæiske Konference for datatilsynsmyndigheder, også kaldet Forårskonferencen, afholdes en gang årligt.

Konferencen, som i 2021 skulle have været afholdt i Kroatien, blev imidlertid udskudt til 2022 som følge af COVID-19-udbruddet.

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 deltager i bl.a. den såkaldte Berlin-gruppe. Konferencen består dels af en lukket del forbeholdt de tilsynsmyndigheder, som er medlem af GPA, og en åben del tilgængelig for alle.

Konferencen, som i 2021 skulle have været afholdt fysisk i Mexico, blev på grund af COVID-19-udbruddet i stedet afholdt online.

På konferencen, som Datatilsynet deltog i, vedtog GPA en række resolutioner om bl.a. datadeling i samfundets interesse, børns digitale rettigheder og myndigheders adgang til data. Der blev endvidere vedtaget resolutioner om GPA's strategiske retning for 2021-2023

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 personoplysninger på Færøerne. For den behandling af personoplysninger på Færøerne, der foretages af færøske myndigheder og af private virksomheder, organisationer mv., gælder den færøske persondatalov. Tilsynsmyndighed i forhold til denne lov er det færøske datatilsyn Dátueftirlitið.

Datatilsynet har i lighed med tidligere år i 2021 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 har imidlertid i 2021 foretaget en række tilsynsbesøg på Færøerne og I Grønland. På Færøerne omfattede besøgene rigsmyndighederne, hvorimod besøgene i Grønland omfattede såvel offentlige myndigheder som private institutioner, der har anmeldt sin behandling af personoplysninger til Datatilsynet.

Formålet med besøgene var både at se på overholdelsen af databeskyttelsesreglerne og at være til rådighed, i det omfang der måtte være behov for vejledning.

Datatilsynets fokus var særligt på anmeldelsespligten, de registreredes rettigheder, spørgsmål om sletning af personoplysninger og en gennemgang af overordnede sikkerhedsmæssige spørgsmål, herunder vigtigheden af medarbejdernes kontinuerlige opmærksomhed på databeskyttelse.

Besøgene viste, at der er opmærksomhed på databeskyttelsesreglerne, og at der løbende arbejdes aktivt med at efterleve reglerne, men at der er problemstillinger, der fortsat skal arbejdes med.

Del 2: Retshåndhævelsesloven

Retshåndhævelsesloven gælder for politiets, anklagemyndighedens – herunder den militære anklagemyndighed – kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling, og for anden ikke-automatisk behandling af personoplysninger, der bliver 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 af oplysninger omfattet af loven – med undtagelse af de behandlinger, der foretages for domstolene. Tilsynet med domstolene foretages af henholdsvis Domstolsstyrelsen og retterne i overensstemmelse med retshåndhævelseslovens regler.

Evaluering af retshåndhævelsesdirektivet

Europa-Kommissionen er i medfør af retshåndhævelsesdirektivet forpligtet til hvert fjerde år at gennemføre en evaluering af anvendelsen af direktivet.

Det Europæiske Databeskyttelsesråd (EDPB) vedtog i december 2021 – til brug for den første evaluering af retshåndhævelsesdirektivet – en udtalelse til Europa-Kommissionen. De nationale tilsynsmyndigheder, herunder Datatilsynet, havde forinden leveret bidrag til EDPB's udtalelse. I udtalelsen konstaterede EDPB bl.a., at det på nuværende tidspunkt er for tidligt at drage konklusioner om effektiviteten af retshåndhævelsesdirektivet.

EDPB oplyste endvidere, at man ville fortsætte arbejdet med at udarbejde vejledninger og afgive udtalelser om fortolkningen af retshåndhævelsesdirektivet. Endelig henledte EDPB opmærksomheden på, at en effektiv gennemførelse af opgaverne i retshåndhævelsesdirektivet forudsætter, at de nationale tilsynsmyndigheder tilføres tilstrækkelige ressourcer. Udtalelsen er tilgængelig på EDPB's hjemmeside.

Tilsyn med retshåndhævelsesloven

I 2021 har Datatilsynet bl.a. behandlet klagesager og anmeldelser fra de retshåndhævende myndigheder om brud på persondatasikkerheden.

Manglende kryptering ved systemoverførsler hos Kriminalforsorgen

Datatilsynet har i 2021 udtalt kritik i en sag, hvor Kriminalforsorgen har anmeldt et sikkerhedsbrud. To af Kriminalforsorgens systemer havde i en længere periode transmitterede personoplysninger om indsatte ukrypteret over internettet, idet systemerne blev tilgået via en ukrypteret HTTP forbindelse.

Datatilsynet fandt, at Kriminalforsorgen – ved ikke at have krypteret transmissionen af personoplysninger – ikke havde levet op til retshåndhævelseslovens krav om passende sikkerhed.

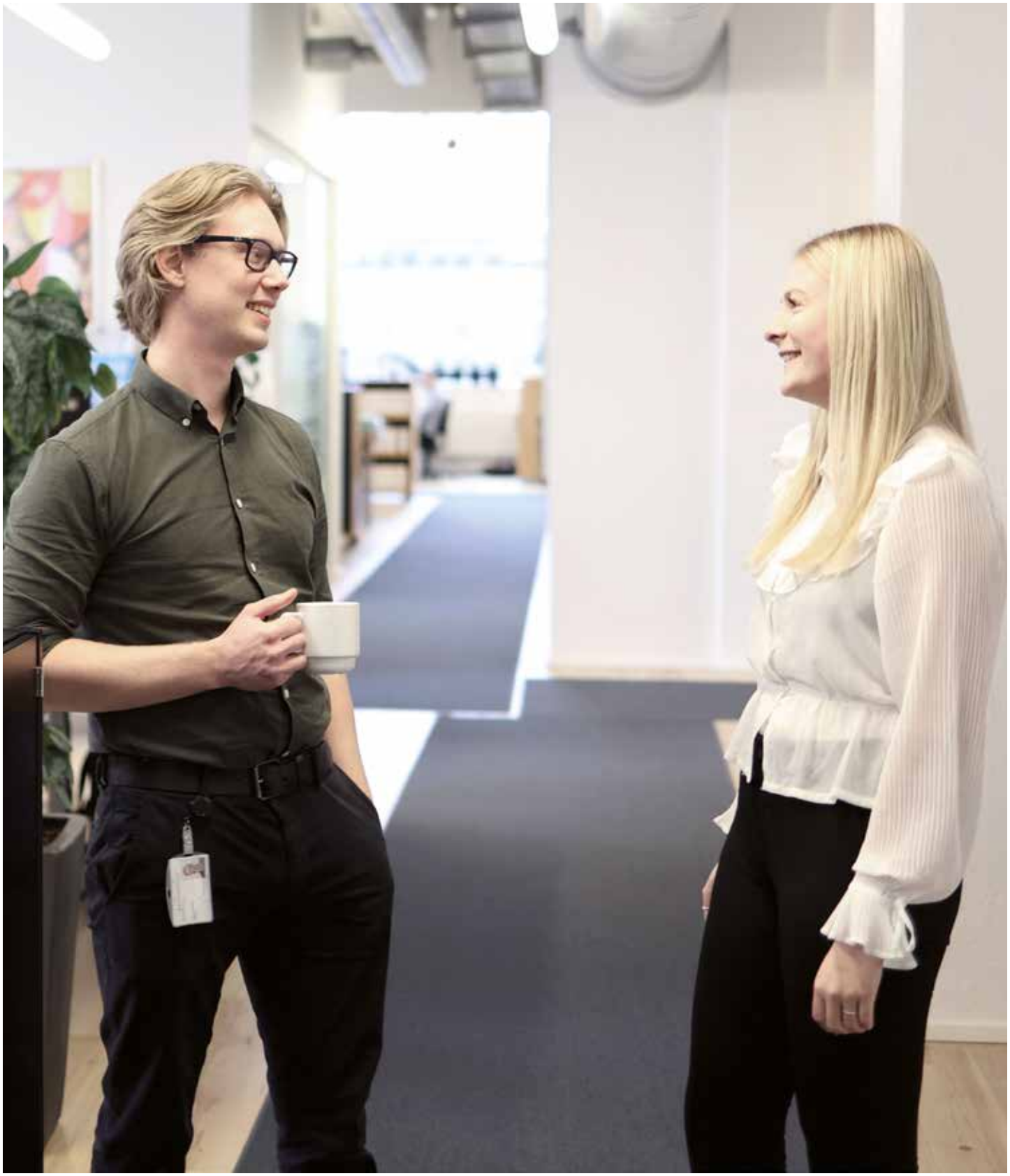
Datatilsynet udtalte i den forbindelse, at der var tale om særligt beskyttelsesværdige oplysninger om indsatte, og at krypteret transmission af sådanne oplysninger er en basal teknisk sikkerhedsforanstaltning, der i en årrække har været et krav for statslige myndigheder.

Transmissionen burde være sket via HTTPS, som er en udgave af HTTP, hvor data "pakkes ind" i en TLS-krypteret forbindelse. Med andre ord så skulle webserveren have haft et certifikat, og have understøttet HTTPS, så webbrowseren kunne validere webserveren, samt udveksle krypteringsnøgler, så personoplysningerne kunne sendes sikkert fra webserveren til browseren.

Teledata-sagen

Datatilsynet undersøgte behandlingen af personoplysninger hos Rigspolitiet på baggrund af, at tilsynet via presseomtale fik kendskab til, at et it-system til brug for behandling af oplysninger om fysiske personers geografiske placering på baggrund af masteoplysninger mv., ikke til enhver tid har leveret retvisende resultater.

Datatilsynet udtalte i afgørelsen alvorlig kritik af, at behandlingen af personoplysninger ikke var sket i overensstemmelse med en række bestemmelser i retshåndhævelsesloven, blandt andet fornøden sikkerhed, oplysningernes rigtighed og den fornødne ansvarlighed.



Samlet set fandt Datatilsynet, at Rigspolitiet havde utilstrækkelige processer og arbejdsgange i forbindelse med behandlingen af teledata. Datatilsynet udtalte endvidere, at Rigspolitiet ikke har sikret kvaliteten, rigtigheden og integriteten af de leverede teledata, eller har påset den efterfølgende sletning af oplysningerne.

Datatilsynet konkluderede, at Rigspolitiet ikke havde truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger med henblik på et sikre et passende sikkerhedsniveau, herunder ved at sikre, at myndigheden ikke behandler og videregiver urigtige personoplysninger, som herefter bruges som bevismidler ved straffesager.

Datatilsynet fandt – på baggrund af Rigspolitiets redegørelse – at der har været mangelfuld kommunikation til kredsene og videre i straffesagskæden om kendte mangler i indholdet af data. Dette har, sammenholdt med kredsenes uens praksis for kvalitetskontrol af data og et manglende ledelsesmæssigt fokus på området, medført, at der i flere tilfælde er tilvejebragt ukorrekte personoplysninger, som bruges som bevismidler ved straffesager.

Datatilsynet gav Rigspolitiet påbud om at foretage sletning af de personoplysninger, der opfylder kravene til sletning efter telecentrets egne retningslinjer, i det omfang dette ikke allerede var sket.

Afgørelsen var baseret på de faktuelle omstændigheder, der allerede var kendt gennem de redegørelser, som Rigspolitiet og Rigsadvokaten havde afleveret til Justitsministeriet, og som Rigspolitiet også havde sendt til Datatilsynet som svar på tilsynets forespørgsler.

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 2021 i alt 36 databekymringer. Datatilsynet har dermed siden lanceringen den 4. juli 2019 indtil udgangen af 2021 modtaget i alt 157 databekymringer. Datatilsynet har valgt at videresende en række af de indkomne e-mails fra databekymringspostkassen til tilsynets egen postkasse, da disse efter en konkret vurdering måtte anses for at være konkrete sager og henvendelser rettet til Datatilsynet. Disse henvendelser er ikke med i det samlede antal af databekymringer.

En generel tendens i 2021 har været, at borgere har været bekymret for den behandling, der sker af personoplysninger i forbindelse med smitteopsporing og forebyggelse af Covid-19. Bekymringerne har angået både indsamling og videregivelse af helbredsoplysninger, men også særligt de behandlinger, som sker i relation til coronapasset.

Herudover har flere borgere udtrykt bekymring for private virksomheders behandling af personoplysninger, navnlig i forhold til deres brug af personnummer (cpr.nr). Bekymringerne vedrørende de private virksomheder har dog også angået behandlingssikkerheden, herunder virksomhedernes mulighed for at modtage e-mails sikkert, da borgere oplever, at virksomhederne opfordrer deres kunder til at sende personoplysninger usikkert. Flere borgere har også henvendt sig med bekymringer vedrørende hjemmesider, hvor der bliver autoudfyldt navn og adresse/mailadresse, hvis man taster et telefonnummer, og hjemmesider, hvor man kan finde navn på ejeren af en bil ved at taste nummerpladen.

Endelig har flere borgere henvendt sig med bekymringer vedrørende databeskyttelsesrådgivernes (DPO'ernes) kompetencer og uafhængighed.

Bilag 1: Oversigt over lovgivning og vejledninger mv.

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 hen blik 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.

Whistleblowerloven

- Lov nr. 1436 af 29. juni 2021 om beskyttelse af whistleblowere.

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. 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 behand-

ling 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. 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.
- Bekendtgørelse nr. 965 af 21. maj 2021 om tilbagemelding om væsentlige helbredsmæssige fund fra anmeldelsespligtige sundhedsvidenskabelige og sundhedsdatavidenskabelige forskningsprojekter, kliniske afprøvninger af medicinsk udstyr m.v. samt visse registerforskningsprojekter.
- Bekendtgørelse nr. 1860 af 23. september 2021 om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret).

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 mv.
- Vejledning af november 2017 om dataansvarlige og databehandlere (under opdatering)
- Vejledende principper om dataansvar for vikarer og konsulenter
- Vejledning af december 2017 om databeskyttelsesrådgivere (under opdatering)
- Vejledning af januar 2018 om adfærdskodekser og certificeringsordninger (opdateret i december 2018)
- Vejledning af februar 2018 om håndtering af brud på persondatasikkerheden (under opdatering)
- Vejledning af marts 2018 om konsekvensanalyse
- Liste over behandlinger, der altid er underlagt kravet om konsekvensanalyse
- Vejledning af juni 2018 om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger
- Vejledning af juli 2018 om de registreredes rettigheder
- 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 august 2020 om fortegnelse
- Vejledning af november 2020 om optagelse af telefonsamtaler
- Vejledning af december 2020 om databeskyttelse i forbindelse med ansættelsesforhold
- Vejledning af januar 2021 om udmåling af bøder til virksomheder
- Vejledning af januar 2021 om udveksling af personoplysninger med politiet
- Vejledning af april 2021 om certificeringsordninger
- Vejledning af maj 2021 om samtykke

- Vejledende tekst af juli 2021 om kommuners offentliggørelse af personoplysninger i offentligt tilgængelige webarkiver
- Vejledning af juli 2021 om overførsel af personoplysninger til tredjelande
- Informationspjece af august 2021 – det skal du vide om databeskyttelse
- Begrebet personoplysninger af august 2021 – få et hurtigt overblik
- Vejledning af september 2021 om udmåling af bøder til fysiske personer
- Vejledning af oktober 2021 om tilsyn med databehandlere
- Vejledende tekst af november 2021 om rollefordelingen, når private er leverandører til det offentlige
- Vejledende tjekliste af december 2021 til vuggestuer og børnehaver ved brug af billeder og video

De oplistede vejledninger mv. er offentliggjort på Datatilsynets hjemmeside.

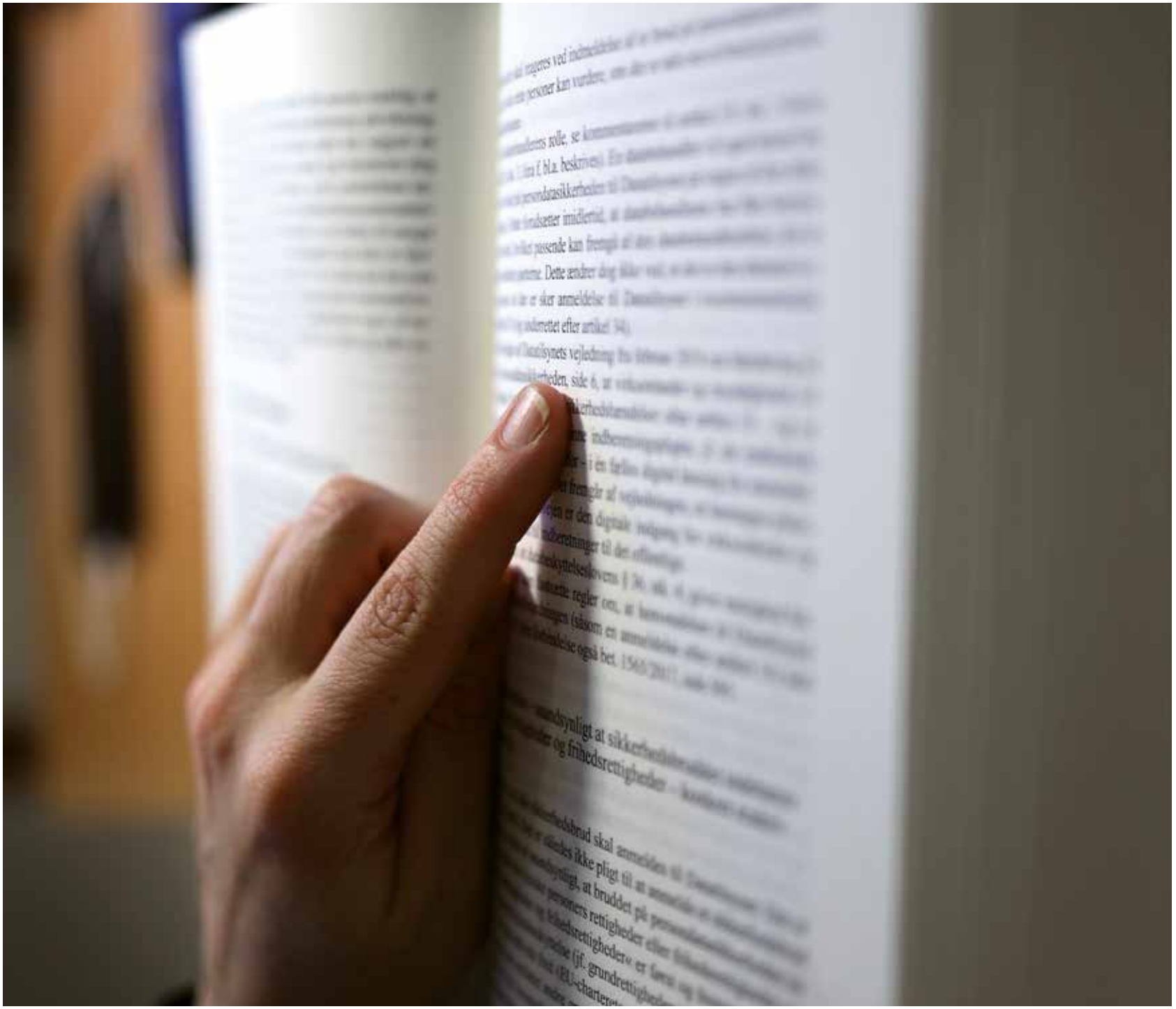
Vejledninger fra Justitsministeriet
- Vejledning af juni 2017 om udveksling af personoplysninger som led i den koordinerede myndighedsindsats over for rocker- og bandekriminalitet.
- Vejledning af december 2018 - Ofte stillede spørgsmål om frivillige foreningers behandling af personoplysninger.
- Vejledning 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.
- Retningslinjer af september 2021 for statslige myndigheders opbevaring af slettede e-mails mv.

Spørgsmål om Justitsministeriets vejledninger mv. kan rettes til Justitsministeriet.

Vejledninger mv. fra Det Europæiske Databeskyttelsesråd (EDPB)
- Adfærdskodekser som overførselsværktøj (Vejledning 4/2021)
- Adfærdskodekser (Vejledning 1/2019)
- Akkreditering (Vejledning 4/2018)
- Anvendelsen af databeskyttelsesforordningens artikel 65(1) (a) (Vejledning 3/2021)
- Art. 6(1)(b) i databeskyttelsesforordningen som behandlingshjemmel ved udbud af online tjenester (Vejledning 2/2019)
- Administrative bøder i henhold til databeskyttelsesforordningen (wp253)
- Anmeldelse af brud på persondatasikkerheden (wp250)
- Automatiske individuelle afgørelser og profilering (wp251)
- Anvendelse af lokaliseringsdata og kontaktopsporingsværktøjer i forbindelse med Covid-19-udbruddet (Vejledning 4/2020)
- Behandling af personoplysninger i forbindelse med forbundne køretøjer og mobilitetsrelaterede applikationer (Vejledning 1/2020)
- Behandling af sundhedsdata med henblik på videnskabelig forskning i forbindelse med Covid-19-udbruddet (Vejledning 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 og databehandlere, samarbejdsproceduren (wp263)
- Bindende virksomhedsregler (BCR) for dataansvarlige, standardansøgning (wp264)
- Bindende virksomhedsregler (BCR) for databehandlere, standardansøgning (wp265)
- Brug af videoudstyr til behandling af personoplysninger (Vejledning 3/2019)
- Certificering (Vejledning 1/2018)
- Dataansvarlig og databehandler (Vejledning 7/2020)

- Dataportabilitet, retten til (wp242)
- Databeskyttelsesrådgivere, DPO'ere (wp243)
- Det juridiske grundlag for lagring af kreditkortdata med det ene formål at lette yderligere online-transaktioner (Anbefaling 2/2021)
- Eksempler på meddelelse om databrud (Vejledning 1/2021)
- Foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU-niveauet for beskyttelse af personoplysninger (Anbefaling 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 (Vejledning 8/2020)
- Overførsel af personoplysninger mellem offentlige myndigheder og organer uden for EØS (Retningslinjer 2/2020)
- Relevant og begrundet indsigelse i henhold til forordningen (Vejledning 9/2020)
- Restriktioner i henhold til artikel 23 i GDPR (Vejledning 10/2020)
- Samtykke (wp259)
- Samtykke i henhold til forordningen (Vejledning 5/2020)
- Samspillet mellem det andet direktiv om betalingstjenester og GDPR (Vejledning 6/2020)
- Samspillet mellem anvendelsen af artikel 3 og bestemmelserne om overførsel til tredjelande i kapitel V i databeskyttelsesforordningen (Vejledning 5/2021)
- Supplerende foranstaltninger ved overførsel af personoplysninger til tredjelande (Anbefaling 1/2020)
- Territorialt anvendelsesområde for databeskyttelsesforordningen (Vejledning 3/2018)
- Tredjelandsoverførsler, tilstrækkeligt databeskyttelsesniveau (wp254)
- Tredjelandsoverførsler, undtagelser i særlige situationer (Vejledning 2/2018)
- Tilstrækkelighed i henhold til retshåndhævelsesdirektivet (Anbefaling 1/2021)
- Virtuelle stemmeassistenter (Vejledning 2/2021)

De nævnte vejledninger mv. er offentliggjort på EDPB's hjemmeside og kan tilgås via Datatilsynets hjemmeside, hvor der løbende offentliggøres 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. 978-87-999222-6-0

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