Datatilsynet

Årsberetning

2022

DATATILSYNET

Datatilsynet

Årsberetning

2022

DATATILSYNET

Indhold

Til Folketinget

Datatilsynet har i 2022 brugt betydelige ressourcer på at rådgive og vejlede om EU's data-beskyttelsesforordning og databeskyttelsesloven, der har fundet anvendelse siden 25. maj 2018, samt retshåndhævelsesloven, der blev gennemført i dansk ret ved lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

Datatilsynet har samlet set en særdeles omfattende og alsidig opgaveportefølje. Tilsynets vejledningsopgaver retter sig mod meget forskelligartede aktører: Folketinget, borgerne, private organisationer og virksomheder samt statslige, regionale og kommunale myndigheder. Datatilsynet arbejder 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 klagesager og generelle tilsynssager, der kan tjene som vejledning for andre. Datatilsynet offentliggør endvidere hvert år forskellige former for vejledende tekster, ligesom tilsynet producerer videoer, podcastepisoder mv.

I 2022 har Datatilsynet offentliggjort 14 nationale vejledninger, hjemmesidetekster mv. Datatilsynet yder også en aktiv indsats på vejledningsområdet i europæiske sammenhænge i regi af Det Europæiske Databeskyttelsesråd, hvor tilsynet i 2022 har medvirket til offentliggørelse af 7 fælleseuropæiske vejledninger. Sammen med en række praktisk anvendelige skabeloner – f.eks. til opfyldelse af oplysningspligten – kan alle de nævnte vejledningsmaterialer mv. findes på Datatilsynets hjemmeside.

Større sagskomplekser og internationale opgaver

Året 2022 har generelt været præget af et højt aktivitetsniveau med mange vigtige vejledningsinitiativer, større sagskomplekser og opgaver af international karakter. Datatilsynet har behandlet flere større og ganske principielle sager om behandling af personoplysninger hos såvel offentlige myndigheder som private virksomheder.

Endvidere har Datatilsynet deltaget aktivt i bl.a. Det Europæiske Databeskyttelsesråds håndtering af flere større grænseoverskridende sager i forbindelse med den såkaldte One Stop Shop-mekanisme. Her skulle rådet træffe endelig bindende afgørelse som følge af, at de europæiske tilsynsmyndigheder, der var involveret i sagen som berørte tilsynsmyndigheder, ikke kunne blive enige om den ledende tilsynsmyndigheds udkast til en afgørelse i hver af sagerne.

Lancering af kampagne inkl. onlinespillet "Datadysten"

Endvidere markerede Datatilsynet i 2022 den internationale databeskyttelsesdag den 28. januar med lanceringen af en kampagne rettet mod 10-12-årige børn på skolernes mellemtrin (4.-6. klasse), der satte fokus på børns behandling af personoplysninger og anvendelse af digitale medier. Formålet med kampagnen var at kaste lys over de helt almindelige udfordringer, der kan opstå ved børns behandling af personoplysninger. En del af kampagnen var et nyt digitalt spil – Datadysten – der på en sjov og uformel måde formidler viden om databeskyttelse. Spillet, der er udviklet i samarbejde med lærere og elever og er gratis, er tilgængeligt for alle på datadysten.dk. Spillet indgår i en undervisningspakke, som kan bruges i fag som Dansk og Teknologiforståelse. Pakken kan også bruges i en temauge, hvor der sættes fokus på et specifikt emne.

Datatilsynet vandt i øvrigt senere på året under den internationale databeskyttelseskonference i Istanbul, hvor databeskyttelsesmyndigheder fra hele verden deltager, to priser for spillet Datadysten, og tilsynet har på den baggrund efterfølgende fået spillet oversat til engelsk.

Brugen af cloudservices

I 2022 har Datatilsynet offentliggjort en vejledning om brugen af cloudservices sammen med en kort oversigt over spørgsmål og svar om brug af cloud. Endvidere udgav tilsynet en episode om vejledningen til Datatilsynets podcast om databeskyttelsesforordningen, ligesom Datatilsynet efterfølgende har afholdt flere møder og oplæg om cloudservices.

Samtidig med offentliggørelsen af vejledningen tog Datatilsynet initiativ til nedsættelsen af en ekspertarbejdsgruppe, der bl.a. skal se på udfordringerne ved de nuværende cloudservices i lyset af den seneste retlige udvikling – og på mulige tiltag og foranstaltninger, der kan sikre en ansvarlig og lovlig brug af cloudservices.

Ekspertgruppens arbejde forventes i 2023 at udmønte sig i konkrete anbefalinger og praktisk vejledning, der kan sikre anvendelse af cloudservices inden for rammerne af databeskyttelsesreglerne.

Ny projektgruppe om kunstig intelligens og databeskyttelse

I efteråret 2021 udsendte Institut for Menneskerettigheder rapporten "Når algoritmer sagsbehandler – Rettigheder og retssikkerhed i offentlige myndigheders brug af profileringsmodeller", som undersøger de rettigheds- og retssikkerhedsmæssige udfordringer, som brugen af kunstig intelligens i sagsbehandlingen rejser. Rapporten indeholder en række anbefalinger, som i et vist omfang forudsætter inddragelse af Datatilsynet.

Datatilsynet nedsatte på den baggrund i maj 2022 en intern projektgruppe på tværs af tilsynets fagenheder, der har fået til opgave at se nærmere på kunstig intelligens og databeskyttelse i en bred kontekst.

Projektgruppens arbejde vil konkret udmønte sig i vejledning, herunder skabeloner og paradigmer, der kan benyttes ved udvikling og brug af kunstig intelligens-løsninger. Datatilsynet vil på den måde forsøge at italesætte, hvordan en lang række af de krav, der allerede i dag gælder for behandling af personoplysninger, skal anvendes i forbindelse med brug af kunstig intelligens.

Derudover har projektgruppen til opgave at foretage en kortlægning af brugen af kunstig intelligens-løsninger på tværs af den offentlige sektor. Det sker med henblik på, at Datatilsynet på længere sigt – og i forlængelse af vejledningen – kan følge op på, at kravene til databeskyttelse bliver overholdt i forbindelse med kunstig intelligens.

Projektgruppen vil som en del af sit arbejde drage nytte af de erfaringer, som Datatilsynets europæiske kollegaer i bl.a. Norge, Storbritannien og senest Frankrig allerede har gjort sig, samt inddrage en lang række relevante interessenter i Danmark.

Specialudvalg om forskning

Siden Datatilsynet lancerede sit strategiske grundlag tilbage i 2020, har tilsynet arbejdet på at skabe en endnu tættere dialog med omverdenen og styrke interessentinddragelsen. Dette er blandt andet gjort for at opnå større indsigt i udfordringerne med efterlevelsen af de databeskyttelsesretlige regler og sikre klarhed om databeskyttelsesreglerne hos de dataansvarlige.

Da forskning reguleres af et komplekst regelsæt og samtidig er af væsentlig samfundsmæssig betydning, besluttede Datatilsynet i 2022 at nedsætte et specialudvalg med fokus på behandling af personoplysninger i forbindelse med forskning.

Udvalget er bredt sammensat med inddragelse af både offentlige og private aktører på området.

Med etableringen af specialudvalget vil Datatilsynet orientere om tilsynets aktuelle arbejde på forskningsområdet, og interessenterne vil have mulighed for at komme med input til det. Første møde blev afholdt den 29. september 2022, og udvalget vil fremover mødes to gange årligt.

Indledningsvis er udvalgets fokus særligt at afklare behov og indhente bidrag til Datatilsynets vejledende tekster på forskningsområdet. Forskning forstås – i lighed med definitionen i databeskyttelsesforordningen – bredt, og specialudvalget beskæftiger sig således ikke kun med forskning inden for sundhedssektoren.

I tillæg til specialudvalget om behandling af personoplysninger i forbindelse med forskning har tilsynet et specialudvalg om det internationale databeskyttelsessamarbejde og to generelle kontaktudvalg, ét for kommuner og regioner og ét for erhvervslivet. I alle udvalgene afholdes der møder to gange årligt.

Schengen-evaluering af Danmark

Der er i oktober 2022 gennemført en Schengen-evaluering af Danmark i forhold til data-beskyttelses-reglerne, hvor Datatilsynet deltog. Opfølgningen på evalueringen er endnu ikke afsluttet.

Opfølgning på den nationale cyber- og informationssikkerhedsstrategi

Den tidligere regering offentliggjorde i december 2021 en ny national cyber- og informationssikker-heds-strategi, som indeholder en lang række initiativer.

Datatilsynet fik som led i opfølgningen på strategien midler til at etablere et datavarehus til brug for ud-stilling af oplysninger om anmeldte brud på persondatasikkerheden. Datavarehuset er et led i styrket videndeling om cyber- og informationssikkerhedshændelser og trusler på tværs af offentlige og private aktører og mellem sektorer, og den udgør dermed et bidrag til den fælles indsats mod den aktuelle og høje cybertrussel, som også udgør en trussel for persondatasikkerheden.

Datatilsynet modtog alene i 2022 ca. 8.800 anmeldelser om brud på persondatasikkerheden. Data fra Datatilsynets screening af anmeldelserne kan bidrage til at skabe et mere nuanceret billede af, hvilke ri-sici mod persondatasikkerheden danske virksomheder og myndigheder bør have blik for. Øget indsigt i baggrunden for, hvornår det går galt, kan føre til flere og mere målrettede forebyggende og vejledende tiltag, der kan sikre bedre viden og opmærksomhed på de foranstaltninger, der er relevante for at imø-degå trusselsbilledet.

I Datatilsynets arbejde i 2022 med etableringen af datavarehuset og valg af udstillingsparametre har det været væsentligt at sikre basale databeskyttelsesmæssige krav, men også at der ikke ved udstilling af data utilsigtet blev afdækket aktuelle informationssikkerhedsmæssige sårbarheder i specifikke sek-torer, som cyberkriminelle eller andre ville kunne udnytte.

Udviklingen af databasen er derfor sket med inddragelse af de øvrige myndigheder, som er en del af den nationale cyber- og informationssikkerhedsstrategi, herunder navnlig Center for Cybersikkerhed.

Lanceringen af datavarehuset sker i begyndelsen af 2023, som samtidig er et år, hvor opfølgningen på strategiens øvrige initiativer fortsætter.

Valby, april 2022

Kristian Korfits Nielsen
Formand, Datarådet

Cristina Angela Gulisano
Direktør, Datatilsynet

Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2022 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 2022, 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 Data-beskyttelsesråd (EDPB), 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 2022 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 data-ansvarlige 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 – primært 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.

Endelig har der siden den 17. december 2021, hvor lov nr. 1436 af 29. juni 2021 om beskyttelse af whistleblowere trådte i kraft, været etableret en ekstern whistleblowerordning i Datatilsynet.

Ordningen har siden skiftet navn til Den Nationale Whistleblowerordning for tydeligere at signalere til omverdenen, at selv om ordningen er etableret i Datatilsynet, så kan den bruges til at indberette om alle forhold omfattet af whistleblowerloven – ikke kun forhold vedrørende databeskyttelse. Den Nationale Whistleblowerordning er uafhængig og selvstændig, hvilket indebærer, at arbejdet med whistleblower-indberetninger holdes adskilt fra Datatilsynets øvrige opgaver og funktioner og fungerer uafhængig af tilsynets øvrige virksomhed.

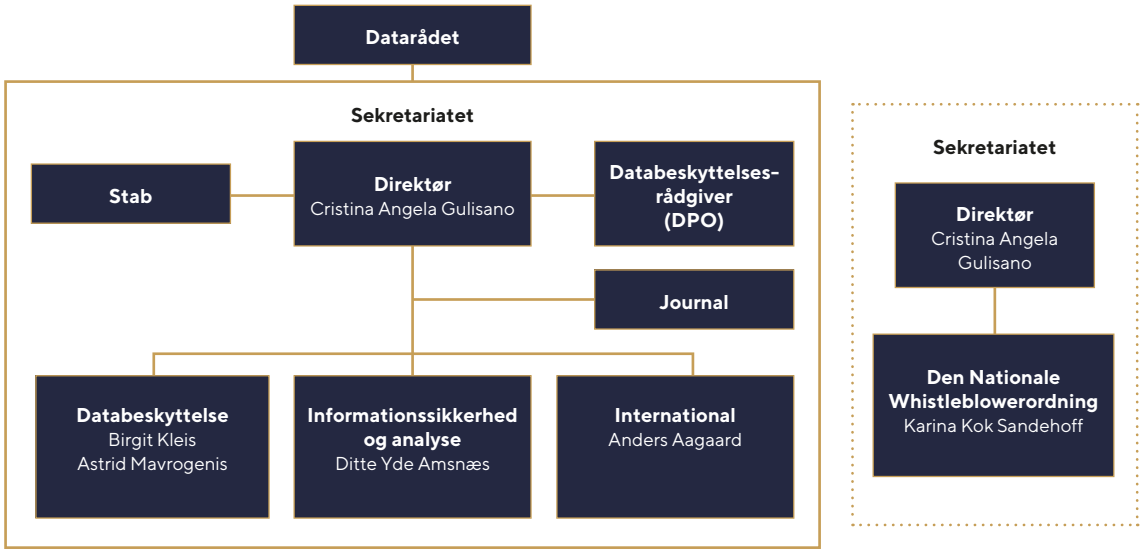
Datatilsynet har etableret hjemmesiden www.whistleblower.dk, hvor man kan læse mere om Den Nationale Whistleblowerordning.

Datatilsynets organisation

Datatilsynet består af et råd – Datarådet – og et sekretariat. Som myndighed har tilsynet en finanslovsmæssig og en 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 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 2022



Datarådet

Justitsministeren nedsætter Datarådet, der består af en formand, der skal være højesteretsdommer eller landsdommer, og syv andre medlemmer.

Datarådet udnævnes for fire år, og der kan ske genudpegning to gange. Udpegelsen sker på baggrund af medlemmernes faglige kvalifikationer.

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

Datarådets medlemmer (pr. 31. december 2022)

Formand
Højesteretsdommer Kristian Korfits Nielsen.

Medlemmer
Næstformand, professor, dr.jur., Henrik Udsen.
Advokat, Pia Kirstine Voldmester.
Formand for Rådet for Digital Sikkerhed, Henning Mortensen.
Politisk chef i Forbrugerrådet Tænk, Uffe Rabe Krag.
Juridisk chef i KL, Pernille Christensen.

Endvidere har fhv. sundhedsdirektør, Svend Hartling og advokat, Martin von Haller Grønbæk frem til udløbet af deres udnævnelsesperiode den 15. oktober 2022 deltaget i Datarådets arbejde. En nærmere stillingtagen til deres eventuelle genudpegning eller udpegningen af to nye medlemmer til rådet forventes i 1. halvår af 2023.

Sekretariatet

Tilsynets sekretariat består af ca. 85 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 2022, der kan findes på undersiden "Årsberetninger og årsrapporter" på Datatilsynets hjemmeside.

Sekretariatets medarbejdere (pr. 31. december 2022)

(Oversigten viser antallet af medarbejdere og ikke antallet af årsværk. Der kan derfor være visse afvigelser i forhold til den økonomiske årsrapport for 2022).

Direktør, cand.jur. Cristina Angela Gulisano
Kommitteret, cand.jur. Birgit Kleis
Kontorchef, cand.jur. Anders Aagaard
Kontorchef, cand.jur. Astrid Mavrogenis
Kontorchef, cand.jur. Ditte Yde Amsnæs
Kontorchef, cand.jur. Karina Kok Sanderhoff
Chefkonsulent, cand.jur. Kenni Elm Olsen
Chefkonsulent, cand.jur., Makar Juhl Holst
Chefkonsulent, cand.jur., Marianne Halkjær Ebbesen
Chefkonsulent, cand.jur. Morten Juul Gjermundbo
Chefkonsulent, cand.jur. Susanne Richter (orlov)
Chefkonsulent, cand.jur., Vibeke Dyssemark Thomsen
Specialkonsulent, cand.jur. Andreas Droob Kristensen
Specialkonsulent, cand.jur., Diana Ismail
Specialkonsulent, cand.soc. Gry Wad
Specialkonsulent, cand.jur. Louise Ellemann Christensen
Specialkonsulent, cand.jur. Maria Freja Reffeldt Bircherod Calundan

Specialkonsulent, cand.jur., Marie Louise Buch-Lassen
Specialkonsulent, cand.jur. Pernille Ørum Walther
Specialkonsulent, cand.jur., Sacha Lena Kiming Faltum
Specialkonsulent, cand.jur. Sarah Hersom Kublitz (orlov)
Specialkonsulent, cand.jur., Signe Vestergård Spring
Fuldmægtig, cand.jur. Alberte Kylén Pedersen
Fuldmægtig, cand. merc.jur. Nicolai Philip van Hauen
Fuldmægtig, cand.jur. Ajla Catovic
Fuldmægtig, cand.jur. Amalie Pilgaard Stubdrup
Fuldmægtig, cand.jur. Anja Bondrup Grunth Hansen
Fuldmægtig, cand.jur. Anna Carolina Jensen
Fuldmægtig, cand.jur. Anna Schmidt Obdrup
Fuldmægtig, cand.jur. Anne Elisabeth Tinten
Fuldmægtig, cand.jur. Anne-Sofie Bruunsgaard Secher
Fuldmægtig, cand.jur. Camilla von Köller
Fuldmægtig, cand.jur. Caroline Rasmussen
Fuldmægtig, cand.jur. Ditte Hector Dalhoff
Fuldmægtig, cand.jur. Delaram Ostadian Lam
Fuldmægtig, cand.jur. Janani Parameswaran
Fuldmægtig, cand.jur. Jane Mindstrup Hagelin
Fuldmægtig, cand.jur. Jonatan Aarkrogh Ubbesen
Fuldmægtig, cand.jur. Josefine Grue
Fuldmægtig, cand.jur. Kamille Frølund Thomsen
Fuldmægtig, cand.jur. Karen Helena Bloch Lindehammer
Fuldmægtig, cand.jur. Kasper Folmar
Fuldmægtig, cand.jur. Line Sørensen
Fuldmægtig, cand.jur. Louise Lunddahl Nielsen
Fuldmægtig, cand.jur. Mads Nordstrøm Kjær
Fuldmægtig, cand.jur. Majbrit Marie Hansen
Fuldmægtig, cand.jur. Malene Højbjerg (orlov)
Fuldmægtig, cand.jur. Matthias Leonhardt Christensen
Fuldmægtig, cand. merc. jur. Miriem Naima Johansson
Fuldmægtig, cand.jur. Rasha Suhiela Said Eleish
Fuldmægtig, cand.jur. Sara Samanlu
Fuldmægtig, cand.jur. Signe Adler-Nissen
It-sikkerhedsspecialist, cand.jur. Allan Frank
It-sikkerhedskonsulent, BSc. dat., Anders Chemnitz
It-sikkerhedskonsulent, diplomingeniør, Benjamin Damore
It-sikkerhedskonsulent, it-supporter, Daniel Lykke Kondrup Bitsch
It-sikkerhedskonsulent, cand.polyt., Ph.d., Martin Mehl Lauridsen Schadegg
It-sikkerhedskonsulent, politiassistent Poul Erik Høj Weidick
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
Dataspecialist, cand.mag. Morten Engberg Helmstedt
Stabsmedarbejder, cand.soc. Anne Bech (orlov)
Stabsmedarbejder, cand.polit., Ph.d., Lea Sell
HR-jurist, cand.jur. Mette Odel Spliid
Kommunikationskonsulent, cand.mag. Anders Due
Kommunikationsfuldmægtig, cand.mag. Natascha Helverskov Jørgensen
Kommunikationsfuldmægtig, cand.mag. Hisar Sindi (orlov)

Controller, cand.merc.aud. Yimin Huang Nielsen
Kontorfunktionær Anette Sørensen
Kontorfuldmægtig Anne-Marie Müller
Kontorfunktionær Camilla Knutsdotter Hallingby
Kontorfunktionær Cathrine Bartels Thing
Kontorfuldmægtig Mette-Maj Aner Leilund
Kontorfuldmægtig Pernille Jensen
Kontorelev, Philip Aguilar Larsen
Informationssikkerhedskoordinator, Jan Hjelvang
Informationssikkerhedskoordinator, Susanne Lynge Lehmann
It-supporter, Poul Hansen
Stud.jur. Amalie Overkær Lund Jensen
Stud.jur. Laura Offenbach Larsen Voss
Stud.jur. Laura Tranekær Krebs
Stud.jur. Oskar Magnus Høgedal
Stud.it. Bjørn Alexander Wade Patterson
Stud.it. Lars Brogaard Kaiser
Stud.it. Daniel Joketovic
Stud.scient.soc. Emily Christine Reither

Den interne whistleblowerordning i Datatilsynet

Den 17. december 2021 blev en intern whistleblowerordning etableret i Datatilsynet. Datatilsynets interne whistleblowerordning er forbeholdt tilsynets medarbejdere. Ved medarbejdere forstås både fuldtids- og deltidsansatte (f.eks. studentermedarbejdere), fastansatte, tidsbegrænset ansatte og vikarer, som er direkte ansat eller tjenestegørende i tilsynet. Det er en betingelse for at bruge den interne ordning, at medarbejderen er ansat på det tidspunkt, hvor oplysningerne indgives. Medarbejderne kan til ordningen indberette oplysninger om forhold, som har fundet eller vil finde sted, og som vedrører overtrædelser af EU-retten, som er omfattet af anvendelsesområdet for whistleblowerdirektivet, alvorlige lovovertrædelser eller øvrige alvorlige forhold.

Indberetninger til Datatilsynets interne whistleblowerordning modtages og behandles af Datatilsynets databeskyttelsesrådgiver (DPO). Efter at have forestået en undersøgelse af den konkrete sag afrapporterer DPO'en direkte til Datatilsynets direktør, som også er autoriseret til at modtage og behandle indberetninger. Datatilsynets direktør har – på baggrund af DPO'ens rapport og indstilling – kompetencen med hensyn til at beslutte, hvilken reaktion (f.eks. politianmeldelse af forhold eller ansættelsesretlig konsekvens) som sagen skal afstedkomme.

Datatilsynets interne whistleblowerordning har siden sin oprettelse i december 2021 og i hele 2022 ikke modtaget nogle indberetninger.

Året i tal

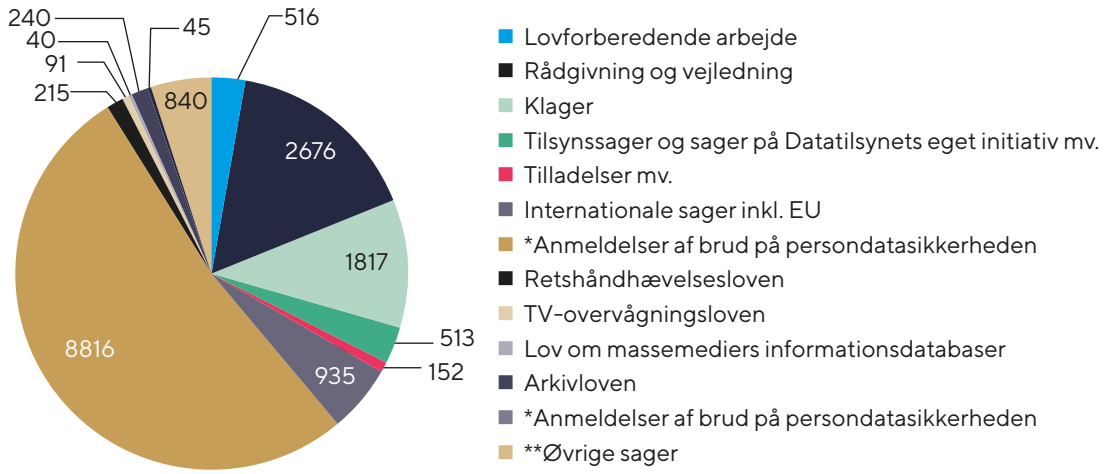
I det følgende afsnit findes oplysninger om antallet af nye sager, som er oprettet i Datatilsynets journalsystem i 2022.

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 **16.896** nye sager i 2022.

Fordeling af oprettede sager i 2022	
Lovforberedende arbejde	516
Rådgivning og vejledning	2676
Klager	1817
Tilsynssager og sager på Datatilsynets eget initiativ mv.	513
Tilladelser mv.	152
Internationale sager inkl. EU	935
Anmeldelser af brud på persondatasikkerheden*	8816
Retshåndhævelsesloven	215
TV-overvågningsloven	91
Lov om massemediers informationsdatabaser	40
Arkivloven	240
Sager om Grønland og Færøerne	45
Øvrige sager**	840
Sager i alt	**16896**

Oprettede sager i 2022



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.)

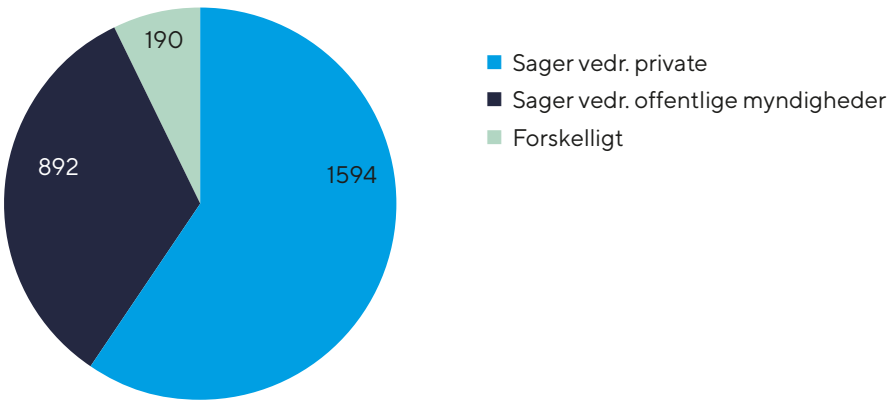
Fordeling af sager vedr. lovforberedende arbejde	
Høringer over bekendtgørelser, cirkulærer, vejledninger, anordninger mv.	318
Høringer over betænkninger, lovforslag, EU-retsakter, konventioner mv.	158
Folketingsspørgsmål, private lovforslag, folketingsbeslutninger, høringer mv.	21
Forskelligt	19
Sager i alt	**516**

Sager vedrørende lovforberedende arbejde

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

Fordeling af sager vedr. rådgivning og vejledning	
Sager vedr. private	1594
Sager vedr. offentlige myndigheder	892
Forskelligt	190
Sager i alt	**2676**

Fordeling af sager vedr. rådgivning og vejledning

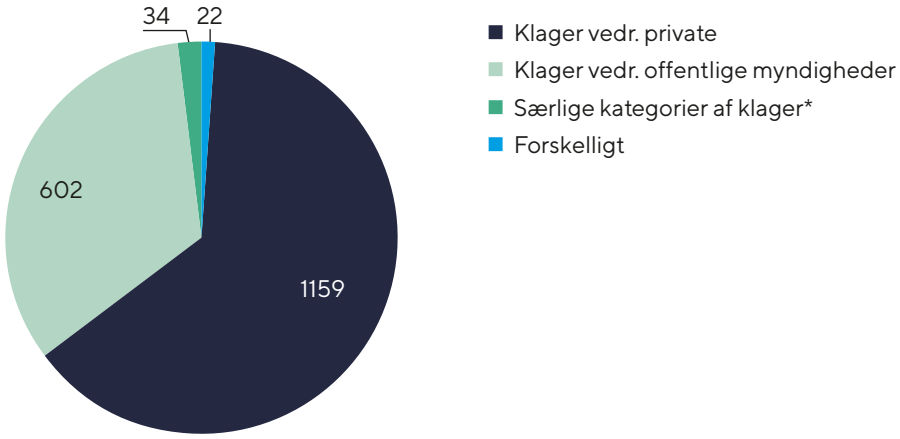


Tilsyn
(Klager)

Fordeling af klagesager	
Klager vedr. private	1159
Klager vedr. offentlige myndigheder	602
Særlige kategorier af klager*	34
Forskelligt	22
Sager i alt	**1817**

*Klager over kreditoplysningsbureauer

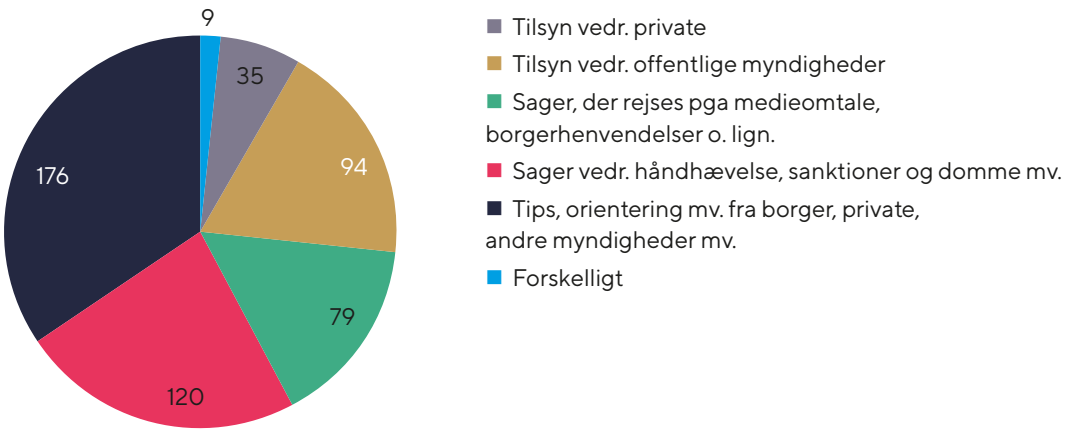
Klagesager



Tilsyn
(Sager på Datatilsynets eget initiativ)

Fordeling af sager på Datatilsynets eget initiativ	
Sager vedr. private	35
Sager vedr. offentlige myndigheder	94
Sager, der rejses pga. medieomtale, borgerhenvendelse o. lign.	79
Sager vedr. håndhævelse, sanktioner og domme mv.	120
Tips, orientering mv. fra borgere, private, andre myndigheder mv.	176
Forskelligt	9
Sager i alt	**513**

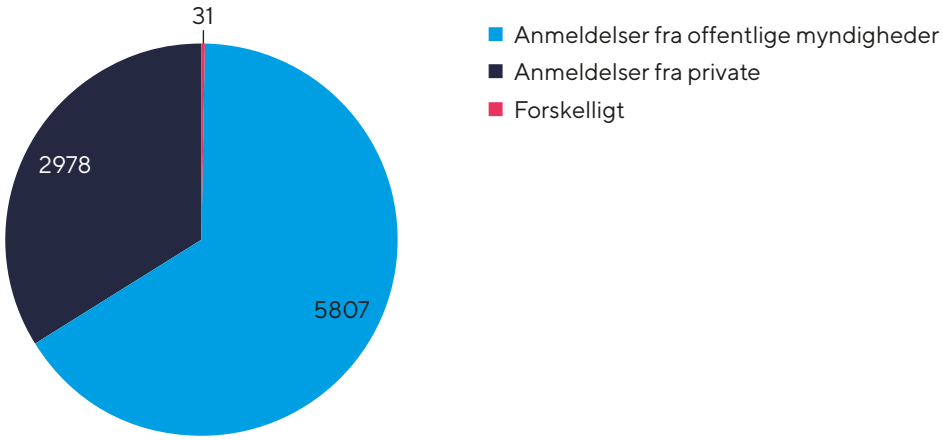
Sager på Datatilsynets eget initiativ



Anmeldelser af brud på persondatasikkerheden

Fordeling af anmeldelser af brud på persondatasikkerheden	
Anmeldelser fra offentlige myndigheder	5807
Anmeldelser fra private	2978
Forskelligt	31
Sager i alt	**8816**

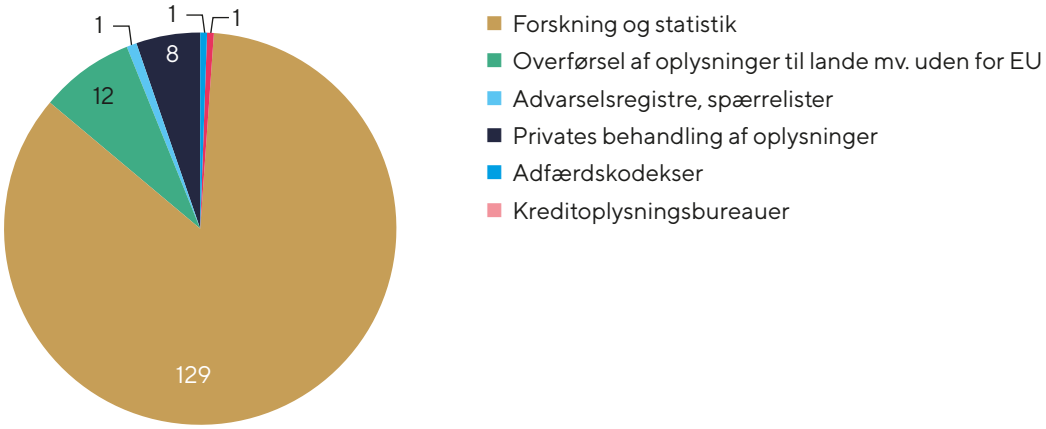
Fordelingen af anmeldelser af brud på persondatasikkerheden



Tilladelser mv.

Fordeling af tilladelser mv.	
Forskning og statistik	129
Overførsel af oplysninger til lande mv. uden for EU	12
Advarselsregistre, spærrelister	1
Privates behandling af oplysninger	8
Adfærdskodekser	1
Kreditoplysningsbureauer	1
Sager i alt	**152**

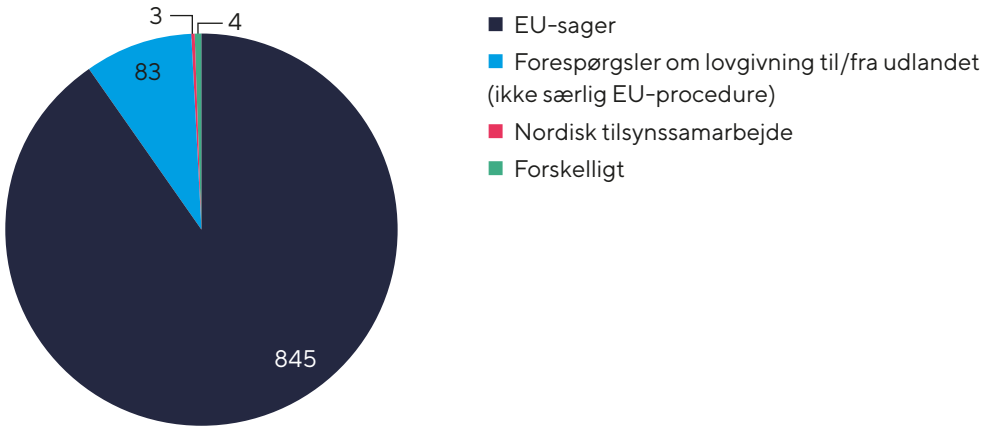
Fordeling af tilladelser mv.



Internationale sager

Fordeling af internationale sager	
EU-sager	845
Forespørgsler om lovgivning til/fra udlandet (ikke særlig EU-procedure)	83
Nordisk tilsynssamarbejde	3
Forskelligt	4
Sager i alt	**935**

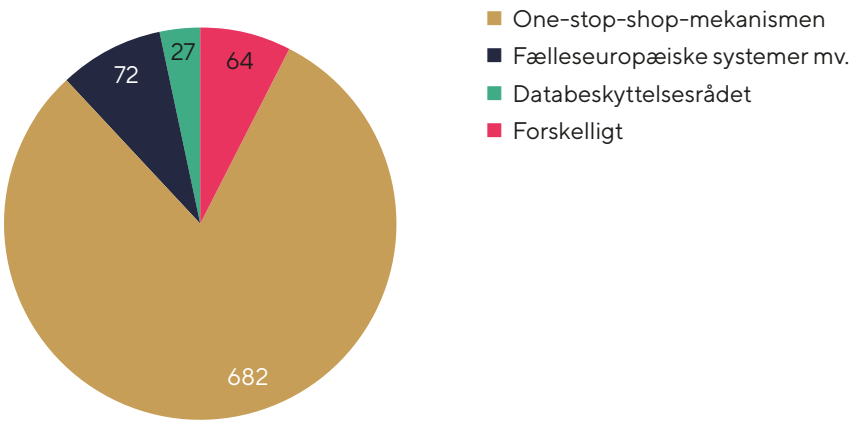
Fordelingen af internationale sager



Fordeling af EU-sager

Fordeling af EU-sager	
One-stop-shop-mekanismen	682
Fælleseuropæiske systemer mv.	72
Databeskyttelsesrådet	27
Forskelligt	64
Sager i alt	**845**

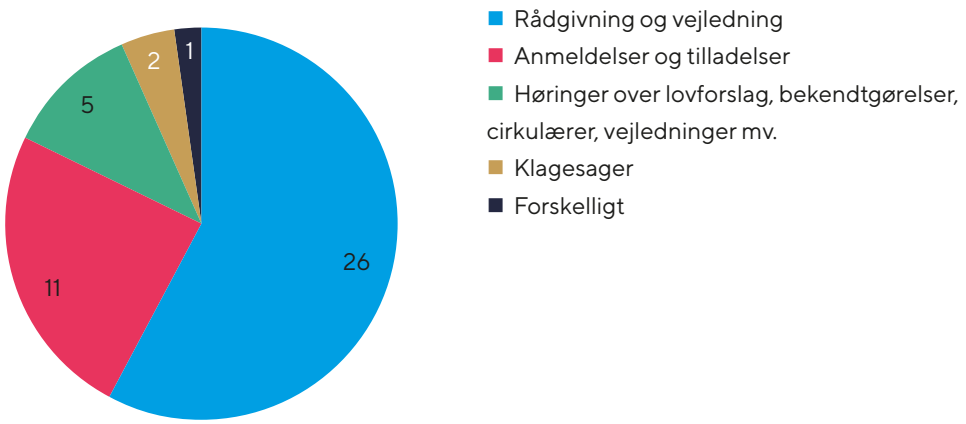
Fordelingen af EU-sager



Grønland og Færøerne

Fordeling af sager vedr. Grønland og Færøerne	
Rådgivning og vejledning	26
Anmeldelser og tilladelser	11
Høringer over lovforslag, bekendtgørelser, cirkulærer, vejledninger mv.	5
Klagesager	2
Forskelligt	1
Sager i alt	**45**

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 2022 offentliggjort 14 nye eller opdaterede nationale vejledninger og vejledende tekster mv. om databeskyttelsesreglerne, som supplerer de 32 nationale vejledninger og vejledende tekster mv., som tilsynet har offentliggjort fra 2017 til 2021. Datatilsynet yder også en aktiv indsats på vejledningsområdet i europæiske sammenhænge og har i regi af Det Europæiske Databeskyttelsesråd bidraget til udarbejdelsen af 7 nye fælleseuropæiske vejledninger om databeskyttelsesforordningen og retshåndhævelsesdirektivet. Alle de nævnte vejledninger og vejledende tekster mv. kan findes på Datatilsynets hjemmeside.

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. Datatilsynet deltog i 2022 f.eks. med en rådgivningsbod på Børsen i forbindelse med et arrangement, som Dansk Erhverv stod bag, ligesom tilsynet var tilstede med en stand på Digitaliseringsmessen i Odense. Endvidere benyttede Datatilsynet i forbindelse med to fysiske tilsyn i Aalborg lejligheden til at svare på spørgsmål fra borgere på byens hovedbibliotek.

Datatilsynets podcast – "Bliv klogere på GDPR"

Siden lanceringen i september 2019 har Datatilsynet produceret 23 tilgængelige episoder af tilsynets podcast "Bliv klogere på GDPR". I 2022 opnåede podcasten 64.967 afspilninger, hvilket totalt set udgør 201.061 afspilninger (pr. 31. december 2022).

Podcastepisoderne tager fat i et afgrænset emne inden for databeskyttelsesforordningen (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 nye vejledning om brugen af cloudservices, udgav tilsynet i marts 2022 en podcast-episode med overskriften: Cloud - hvad siger GDPR og Schrems II, og kan man gøre det lovligt? Episoden ligger samtidig i forlængelse af tidligere episoder i podcasten om cloud og tredjelandsoverførsler efter Schrems II-dommen. Endvidere udgav Datatilsynet i august 2022 en podcast-episode om deling af billeder på forældreintranet. Det skete i forlængelse af, at tilsynet havde meldt ud, at skoler i udgangspunktet godt kan dele relevante billeder af elever på forældreintranet o.l. uden at indhente samtykke.

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.

Kategorisering af afgørelser på Datatilsynets hjemmeside

Datatilsynet offentliggør løbende udvalgte afgørelser på sin hjemmeside. Afgørelserne er en vigtig del af tilsynets vejledning, fordi de viser den konkrete udmøntning af, hvordan reglerne i databeskyttelses-forordningen skal forstås. Der er nu offentliggjort knap 300 afgørelser, siden forordningen fik virkning i 2018.

Men i takt med, at flere afgørelser er kommet til, er det blevet sværere at finde frem til relevante sager på forskellige områder. Derfor har Datatilsynet i 2022 gennemgået alle de offentliggjort afgørelser og kategoriseret dem, så man kan filtrere de mange afgørelser efter forskellige parametre:

- **Virksomhedsområde** – er den dataansvarlige en privat virksomhed, en offentlig myndighed eller en retshåndhævende myndighed?
- **Sagstype** – tager sagen udgangspunkt i fx klage, tilsyn, anmeldt brud på persondatasikkerheden eller forespørgsel?
- **Sanktion** – munder afgørelsen ud i fx kritik, påbud, bødeindstilling e.l.?
- **Nøgleord** – hvilke områder inden for databeskyttelse handler afgørelsen om – fx behandlings-sikkerhed, adgangskontrol eller retten til sletning?

Ud over disse muligheder er det også muligt at filtrere efter dato og kombinere med en almindelig fritekstsøgning.

Cybersikkerhedsmåned: Hotline og daglige tips

I forbindelse med Sikker Digitals afholdelse af "national cybersikkerhedsmåned" i oktober 2022, hvor myndigheder, virksomheder mv. kunne tilmelde lokale aktiviteter, besluttede Datatilsynet at deltage med to tiltag: En hotline om behandlingssikkerhed og daglig offentliggørelse af korte sikkerhedstips på tilsynets hjemmeside. Tiltagene blev bl.a. valgt ud fra den erfaring, som Datatilsynet har gjort sig på tilsynets almindelige telefonvagt, hvor mange borgere, virksomheder og myndigheder spørger ind til netop behandlingssikkerhed.

En dedikeret hotline til spørgsmål om behandlingssikkerhed gav en direkte linje til specialister, der kunne svare mere udførligt på sådanne spørgsmål. Hotlinen var åben alle hverdage i oktober måned fra kl. 10-12, og den blev i hele perioden betjent af alle Datatilsynets it-sikkerhedskonsulenter.

De daglige sikkerhedstips på tilsynets hjemmeside tjente til at imødekomme en efterspørgsel fra borgere, myndigheder og virksomheder om gode råd til f.eks. behandlingssikkerhed, som flere har savnet, efter at Datatilsynet ophørte med at bringe "mandagsmyten", der indeholdt korte råd eller vejledende tekster om forskellige databeskyttelsesretlige spørgsmål.

Spørgsmål om kommuners hjemmel til AI-profileringsværktøjet Asta

Styrelsen for Arbejdsmarked og Rekruttering (STAR) anmodede i 2022 Datatilsynet om en vurdering af spørgsmålet om kommunernes hjemmel til at anvende AI-profileringsværktøjet Asta.

Asta er et værktøj, der – på grundlag af en flerhed af informationer – har til formål at foretage en maskinel analyse af, hvad en nyledig dagpengemodtagers risiko er, for at kontaktforløb med jobcenteret bliver langvarigt. Analysen foretages ved at sammenligne en konkret dagpengemodtagers informationer (værdier) med en række konstruerede (generelle) persontypers værdier. Risikoen for at ende med et langt kontaktforløb skønnes så ud fra, i hvor høj grad den konkrete borgers værdier mest ligner persontyper, der ender med kort eller langt kontaktforløb.

Datatilsynet vurderede i første række, at borgerens samtykke ikke kunne danne grundlag for behandling i henhold til databeskyttelsesforordningen, eftersom borgerens samtykke i den pågældende kontekst ikke kunne anses for frivilligt. Dette gjaldt også, selvom det i praksis var muligt for borgeren at frasige sig behandlingen, dvs. undgå profileringen, uden at dette havde en negativ indvirkning for den pågældende – f.eks. stop af ydelse – idet der forelå en ikke ubetydelig risiko for, at den registrerede, uagtet denne mulighed, ville kunne føle sig presset til at samtykke til behandlingen, f.eks. for at undgå at fremstå besværlig eller lignende.

Datatilsynet vurderede herefter, at databeskyttelsesforordningens artikel 6, stk. 1, litra e (offentlig myndighedsudøvelse) var eneste mulige behandlingshjemmel.

Nødvendigt med national lovgivning på området

I den forbindelse udtalte Datatilsynet, at anvendelsen af artikel 6, stk. 1, litra e, kræver, at behandlingen er forudsat i EU-retten eller national ret, men ikke nødvendigvis, at der er en national implementerende hjemmelslovgivning om selve behandlingen. Hvilke krav, der stilles til klarheden af dette nationale hjemmelsgrundlag, afhænger af, hvor indgribende den pågældende behandling er for den registrerede. Er der tale om en helt harmløs behandling, vil kravene ikke være særlig store. Er der derimod tale om en indgribende behandling, som det er tilfældet i den pågældende situation, stilles der større krav til klarheden af hjemmelsgrundlaget.

På baggrund af dette, var det Datatilsynets opfattelse, at der skulle være hjemmel hertil i national lovgivning, som det f.eks. kendes fra § 8, stk. 2, i lov om en aktiv beskæftigelsesindsats, for at Asta-værktøjet kunne anvendes af kommunerne.

Datatilsynet udtalte samtidig, at den omstændighed, at det var nødvendigt med national lovgivning på området, ikke i sig selv betød, at kommunerne af den grund ville kunne foretage profilering af den registrerede, uden at denne har indvilliget heri, idet det i et nationalt hjemmelsgrundlag ville være muligt at fastsætte nærmere krav til, under hvilke betingelser kommunerne kunne anvende værktøjet.

Ny vejledning og ekspertgruppe om brug af cloud

Cloud er en af de teknologier, som de seneste år har givet anledning til mange spørgsmål til Datatilsynet. I marts 2022 udgav Datatilsynet derfor en vejledning om brug af cloudservices.

Vejledningen er målrettet myndigheder og virksomheder, der ønsker at bruge cloudservices, og gennemgår de overvejelser, som virksomheder og myndigheder skal gøre sig, hvis de ønsker at benytte en cloudservice. Vejledningen giver blandt andet anvisninger på, hvordan man vurderer sine cloudleverandører, hvilke krav man skal stille til dem, hvordan man dokumenterer sine valg, og hvordan man kontrollerer, at personoplysninger behandles i tråd med instruksen. Vejledningen indeholder herudover afsnit, der handler om overførsel af personoplysninger til tredjelande, herunder en gennemgang af det mest benyttede tredjeland, USA, og de særlige problemstillinger, som EU-Domstolens afgørelse i den såkaldte Schrems II-sag har affødt.

Cloudservices leveres ofte som standardiserede ydelser, hvor den enkelte virksomhed og myndighed som kunde har begrænsede muligheder for at tilpasse servicen til sine individuelle behov og krav. Dele af vejledningen henvender sig derfor også til cloudleverandører, der kan læse mere om, hvordan de kan levere services i overensstemmelse med databeskyttelsesreglerne. Af samme årsag har Datatilsynet som noget nyt samtidig udgivet en engelsk udgave af vejledningen med henblik på at nå ud til flest mulige aktører, der arbejder med udvikling og brug af cloudservices.

For at formidle de centrale budskaber i Datatilsynets vejledning afholdt tilsynet i forlængelse af udgivelsen af vejledningen to gå-hjem-møder i henholdsvis København og Aarhus med sammenlagt over 300 deltagere.

Samtidig med udgivelsen af vejledningen tog Datatilsynet endvidere initiativ til nedsættelsen af en ekspertarbejdsgruppe. Gruppen fik til opdrag at se på udfordringerne ved de nuværende cloudservices i lyset af den seneste retlige udvikling og på mulige tiltag og foranstaltninger, der kan sikre en ansvarlig og lovlig brug af cloudservices.

Ekspertgruppens arbejde skal i løbet af 2023 udmønte sig i konkrete anbefalinger og praktisk vejledning, der kan sikre anvendelse af cloudservices inden for rammerne af databeskyttelsesreglerne.

Endelig iværksatte Datatilsynet – som opfølgning på den udgivne vejledning – fire tilsynssager, der skal se nærmere på to virksomheders og to myndigheds brug af cloudservices. I den forbindelse offentliggjorde Datatilsynet også det spørgeskema, som blev fremsendt til de fire organisationer. Spørgeskemaet omfatter de fleste punkter, man som dataansvarlig skal være opmærksom på, hvis man benytter sig af cloud. Skemaet kan således hjælpe dataansvarlige, der benytter sig af cloudservices, med at undersøge, om deres brug af cloud lever op til reglerne for databeskyttelse.

Google Analytics

I løbet af 2022 traf flere europæiske datatilsynsmyndigheder, heriblandt myndighederne i Østrig, Frankrig og Italien, afgørelser om europæiske organisationers brug af værktøjet Google Analytics. I alle sagerne fandt tilsynsmyndighederne, at brugen af Google Analytics under de givne omstændigheder ikke var lovlig.

Selvom de enkelte sager blev afgjort individuelt af de respektive tilsynsmyndigheder, som modtog de oprindelige klager, var afgørelserne udtryk for en fælleseuropæisk holdning blandt tilsynsmyndighederne. Genstanden for de indgivne klager har været ens, og sagerne blev derfor behandlet samlet i en arbejdsgruppe i regi af Det Europæiske Databeskyttelsesråd, herunder med deltagelse af Datatilsynet. Her blev de juridiske problemstillinger – og besvarelsen heraf ¬– drøftet.

I kølvandet på afgørelserne så Datatilsynet nærmere på værktøjet Google Analytics og de konkrete indstillinger, som Google stiller til rådighed. På baggrund af denne gennemgang konkluderede Datatilsynet, at værktøjet ikke kan benyttes lovligt uden videre. En lovlig brug forudsætter implementering af en række supplerende foranstaltninger ud over de indstillinger, Google stiller til rådighed. I tilknytning til denne gennemgang udarbejdede Datatilsynet også en vejledende tekst om konsekvenserne for danske myndigheder og virksomheder samt en række spørgsmål og svar om brug af værktøjet.

Nye vejledende tekster om tredjelandsoverførsler mv.

Det er Datatilsynets erfaring, at problemstillinger vedrørende overførsel af personoplysninger til tredjelande har fyldt meget hos danske myndigheder og virksomheder siden EU-Domstolens afgørelse i den såkaldte Schrems II-sag i juli 2020. Det var også tilfældet i 2022.

Datatilsynet prioriterede derfor i løbet af 2022 at udarbejde flere vejledende tekster og besvare konkrete forespørgsler fra myndigheder og virksomheder om, hvordan reglerne om overførsel af personoplysninger til tredjelande kan overholdes.

Står det i databehandleraftalen, er det ikke utilsigtet

I marts 2022 henvendte KOMBIT sig til Datatilsynet med et konkret spørgsmål om udlevering af personoplysninger til myndigheder i tredjelande. Konkret drejede det sig om, at KOMBIT – der leverer systemet Aula til de danske kommuner – benyttede Netcompany som underleverandør, som igen benyttede Amazon Web Services ("AWS") som underleverandør.

Ifølge KOMBIT behandledes oplysningerne som udgangspunkt inden for EU/EØS, men det fremgik samtidig af databehandleraftalen mellem Netcompany og AWS, at dette kunne fraviges, hvis det var nødvendigt for at leve op til lovgivningen eller en bindende afgørelse fra en offentlig myndighed. Spørgsmålet fra KOMBIT bestod i, om der – hvis AWS bragte undtagelsen i spil – var tale om en tilsigtet eller utilsigtet overførsel til tredjelande.

Datatilsynet udtalte, at der efter tilsynets opfattelse vil være tale om en tilsigtet tredjelandsoverførsel. Derfor skal kommunerne som de dataansvarlige sikre sig, at reglerne om overførsler til tredjelande overholdes, når eller hvis AWS foretager sådanne overførsler i henhold til den instruks, der fremgår af databehandleraftalen.

Om begrebet "dataeksportør"

Datatilsynet udgav endvidere i juni 2022 en vejledende tekst om begrebet "dataeksportør". Teksten var foranlediget af en række spørgsmål om, hvem der i praksis er ansvarlig for at sikre, at overførsel af personoplysninger til tredjelande er lovlig, når overførslen sker på baggrund af den såkaldte standardkontrakt, som Europa-Kommissionen har vedtaget.

Datatilsynets udtalte, at databeskyttelsesforordningens artikel 44, som fastsætter det generelle princip for overførsel af personoplysninger til tredjelande, er en forpligtelse for både den dataansvarlige og databehandleren. Begge parter er derfor forpligtede til at sørge for, at der tilvejebringes et overførselsgrundlag, der er effektivt i lyset af alle omstændighederne ved overførslen. Det gælder også i de tilfælde, hvor det i praksis er databehandleren, der indgår Europa-Kommissionens standardkontrakt med eventuelle underdatabehandlere i tredjelande. I så fald består forpligtelsen for den dataansvarlige i praksis i at sikre sig – og kunne påvise over for Datatilsynet – at databehandleren har etableret det fornødne overførselsgrundlag, og at dette overførselsgrundlag er effektivt i lyset af alle omstændighederne ved overførslen, herunder ved implementeringen af supplerende foranstaltninger om nødvendigt.

Ny vejledning om valgkampagner

I efteråret 2022 blev der afholdt valg til Folketinget. Umiddelbart inden valgudskrivelsen udgav Datatilsynet i oktober 2022 en vejledning, som beskriver, hvordan politiske aktører overholder databeskyttelsesreglerne i forbindelse med valgkampagner.

Vejledningen beskriver, hvilke overvejelser politiske aktører skal gøre sig fra start, når de indsamler personoplysninger til brug for en valgkampagne, til slut, når kampagnen er overstået. Vejledningen beskriver særligt en række forskellige relevante scenarier og sætter især fokus på målretnings- og forstærkningsteknikker, der anvendes til at sprede budskaber på internettet. Disse værktøjer er ofte baseret på avanceret profilering og omfattende behandling af vælgernes oplysninger.

Datatilsynet har tilstræbt at gøre vejledningen så konkret og praktisk anvendelig som muligt. Vejledningen indeholder derfor bl.a. også en lang række konkrete eksempler.

Lokalarkivers behandling af personoplysninger

Et lokalarkiv er et arkiv, der indsamler, registrerer, opbevarer og i visse tilfælde offentliggør privat arkivmateriale, som typisk er skabt af virksomheder, foreninger eller privatpersoner fra et afgrænset lokalområde. Lokalarkiverne er ikke omfattet af reglerne i arkivloven og reguleres dermed af de almindelige databeskyttelsesregler, som findes i databeskyttelsesforordningen og databeskyttelsesloven.

Datatilsynet udgav i 2022 – efter inddragelse af foreningen Sammenslutningen af Lokalarkiver - retningslinjer for lokalarkivers behandling af personoplysninger, som skal bidrage til, at tvivl om databeskyttelsesreglerne ikke står i vejen for det arbejde, som lokalarkiverne foretager. På baggrund af en vurdering af de behandlinger, som oftest foretages af lokalarkiver, anbefalede Datatilsynet, at lokalarkiverne følger nedenstående retningslinjer:

- Materiale, som alene indeholder "almindelige" personoplysninger (lav-risiko materiale), kan uden videre behandles (indsamles), men offentliggøres som det klare udgangspunkt først, når materialet er mindst 20 år gammelt. Det betyder bl.a., at det vil være i orden at publicere navne på personer i forbindelse med publicering af billeder, der er ældre end 20 år.
- Lokalarkivet behandler (indsamler) ikke følsomme personoplysninger eller andre særligt beskyttelsesværdige personoplysninger, herunder oplysninger om enkeltpersoners rent private forhold, i

digital form eller systematiserer sådanne oplysninger i et register, førend vedkommende, hvis oplysninger det drejer sig om, har været død i mindst 10 år, eller oplysningerne er 75 år gamle. Det betyder, at materiale, der indeholder sådanne oplysninger, alene kan opbevares analogt og uden at der registreres metadata, som gør det muligt for arkivet at fremfinde arkivalier relateret til en bestemt person, f.eks. fordi det er muligt at søge på vedkommendes navn.

- Lokalarkivets offentliggjorte materiale, der indeholder personoplysninger, og registrerede metadata, indekseres ikke af søgemaskiner.
- Lokalarkiverne sletter personoplysninger fra internettet, hvis den registrerede anmoder om dette.

Hvis lokalarkivet ønsker at behandle, herunder indsamle og offentliggøre, følsomme personoplysninger eller andre særligt beskyttelsesværdige personoplysninger digitalt eller systematisere sådanne oplysninger i et register, herunder ved anvendelse af metadata, som gør det muligt at fremsøge personoplysninger, f.eks. ved anvendelse af navn, kan dette kun ske med den registreredes samtykke, medmindre der er tale om oplysninger, der tydeligvis er offentliggjort af den registrerede selv, eller den, hvis oplysninger det drejer sig om, har været død i mindst 10 år eller oplysningerne er mindst 75 år gamle.

Nye fælleseuropæiske vejledninger

Det Europæiske Databeskyttelsesråd (EDPB) har i 2022 vedtaget en række vejledninger mv. om aktuelle databeskyttelsesretlige emner,

Vejledning om retten til indsigt

EDPB vedtog i januar 2022 en omfattende vejledning om retten til indsigt, som bl.a. kommer ind på formålet med og rækkevidden af retten til indsigt, de supplerende informationer, den dataansvarlige skal give om behandlingen, hvordan de dataansvarlige kan give indsigt og undtagelser til indsigtsretten. Vejledningen indeholder endvidere en række eksempler og et flowchart over, hvordan en anmodning om indsigt bør håndteres.

Vejledningen har været i offentlig høring, som blev afsluttet i marts 2022. EDPB forventes i 2023 at afslutte arbejdet med vejledningen i lyset af de indkomne bemærkninger.

Vejledning om vildledende designmønstre i grænseflader på sociale medier

I marts 2022 vedtog EDPB endvidere en vejledning om vildledende designmønstre (*deceptive design patterns)* på sociale medier. Vejledningen omhandler designelementer og brugergrænseflader designet til at påvirke brugerens handlinger. Deceptive design patterns kendes eksempelvis fra nogle cookie-bannere, hvor der anvendes kontrastfarver, som søger at påvirke brugeren til at samtykke til brugen af cookies.

Vedledningen fokuserer bl.a. på, hvordan man som dataansvarlig kan undgå at anvende deceptive design patterns i strid med de databeskyttelsesretlige regler, når man behandler oplysninger om personer, der opretter sig som brugere på et socialt medie. Den nye vejledning er også relevant i en række andre databeskyttelsesretlige sammenhænge – f.eks. ved brug af samtykkeløsninger til behandling af personoplysninger om hjemmesidebesøgende.

Vejledningen har efter vedtagelsen været i offentlig høring, og den forventes endeligt vedtaget i 2023.

Vejledning om udmåling af bøder til virksomheder

EDPB vedtog i maj 2022 en vejledning om udmåling af bøder til virksomheder. Vejledningen er udarbejdet i arbejdsgruppen Task Force Fining under EDPB, og Datatilsynet har deltaget i den gruppe af tilsynsmyndig-heder, som udarbejdede udkastet til vejledningen.

Vejledningen indeholder en detaljeret angivelse af bødeberegningsmetoden, og den giver nogle indikationer på et bødeudgangspunkt for overtrædelser af forskellig grovhed. Det overordnede formål med vejledningen er at sikre ensartethed i udmålingen af bødeniveauet på tværs af EU-landene.

Efter vedtagelsen har vejledningen været i offentlig høring, og den forventes endeligt vedtaget i 2023.

Datatilsynet vil samtidig vurdere, om det giver anledning til at revidere tilsynets nationale vejledning om udmåling af bøder til virksomheder, som blev offentliggjort i januar 2021.

Vejledning om brug af certificeringer som overførselsgrundlag

Certificeringsordninger kan benyttes af virksomheder og myndigheder som et værktøj til at demonstrere overholdelse af databeskyttelsesforordningens generelle regler. Dertil kan de under visse betingelser udgøre et gyldigt grundlag for overførsel af personoplysninger til tredjelande.

EDPB har tidligere udgivet en generel vejledning om certificeringer. Som supplement hertil har EDPB i juni 2022 vedtaget en vejledning særligt rettet mod brugen af certificeringer som overførselsgrundlag. Vejledningen beskriver bl.a. de specifikke indholdsmæssige krav, forpligtelserne for de involverede parter samt proceduren, når en certificeringsordning skal godkendes som et gyldigt overførselsgrundlag i henhold til databeskyttelsesforordningens kapitel V.

Efter vedtagelsen har vejledningen været i offentlig høring, og den forventes endeligt vedtaget i 2023.

EDPB har i 2021 endvidere udarbejdet en lignende vejledning om adfærdskodekser som overførselsgrundlag, der efter at have været i offentlig høring blev endelig godkendt i februar 2022.

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 **516** sager i 2022 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.

Lov om Det Centrale Dna-profilregister og Det Centrale Fingeraftryksregister

I marts 2022 sendte Justitsministeriet et lovforslag i høring om Det Centrale DNA-profilregister og Det Centrale Fingeraftryksregister, der havde til formål at skabe en samlet og mere enkel regulering af de to registre.

Der blev med lovforslaget bl.a. lagt op til at indføre differentierede frister på henholdsvis 15, 25 og 40 år for sletning af dna-profiler og fingeraftryk fra personer, der er dømt for en lovovertrædelse. Derudover blev der lagt op til differentierede slettefrister på henholdsvis 10, 15 og 20 år for dna-profiler og fingeraftryk fra personer, der er sigtet, men ikke dømt, for en lovovertrædelse. I begge tilfælde ville slettefristen som følge af lovforslaget blive fastsat ud fra strafferammen for den overtrædelse, der er rejst sigtelse for.

Lovforslaget lagde endvidere op til at videregivelse af oplysninger fra henholdsvis dna-profilregisteret og fingeraftryksregisteret fremover skulle være reguleret af de almindelige databeskyttelsesretlige regler. Endelig blev der lagt op til at forbedre den registreredes adgang til indsigt i oplysninger om sig selv, således at vedkommende ville kunne få adgang til oplysningerne på skriftligt grundlag.

I sit høringssvar bemærkede Datatilsynet generelt, at det var positivt, at lovforslaget forsøgte at indføre en samlet og mere enkel regulering af de to registre, og at dette måtte forventes at skabe en større klarhed over retsgrundlaget for de registrerede.

Datatilsynet bemærkede endvidere, at der med slettefristerne på henholdsvis 10, 15 og 20 år for dna-profiler og fingeraftryk fra personer, der er sigtet, men ikke dømt for en lovovertrædelse, ville ske en udvidelse af opbevaringsperioden for dna-profiler og fingeraftryk fra sigtede, men ikke dømte personer. Datatilsynet henstillede derfor til, at der i lovforslaget nærmere blev redegjort for, hvordan det ville styrke politiets efterforskningsmuligheder, hvis slettefristerne blev forlænget. Derudover henstillede Datatilsynet til, at det blev uddybet, hvordan balancen mellem på den ene side hensynet til politiets arbejde og på den anden side hensynet til privatlivets fred kunne opretholdes med de nye, længere slettefrister.

For så vidt angår forslaget om at indføre differentierede slettefrister på henholdsvis 15, 25 og 40 år for dna-profiler og fingeraftryk fra dømte personer, hvor slettefristen fremover ville blive fastsat ud fra strafferammen, bemærkede Datatilsynet, at slettefrister baseret på den konkret udmålte straf i højere grad end slettefrister baseret på strafferammen for den rejste sigtelse udgør den rette balance mellem på den ene side hensynet til politiets arbejde og på den anden side hensynet til privatlivets fred. Datatilsynet bemærkede i den forbindelse, at det forhold, at det ikke teknisk er muligt at fastsætte slettefrister baseret på den udmålte straf, generelt ikke bør komme den registrerede til skade.

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 skærpet 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 2022 indgivet **11 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.

Endvidere har Datatilsynet i 2022 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 myndigheder.

Datatilsynet har herudover 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 skal bruge for at kunne behandle klagen.

Klagesagsbehandling

Datatilsynet modtager hvert år mange klager over både private og offentlige dataansvarlige. Der kan f.eks. klages over, at en dataansvarlig ikke har hjemmel til at behandle den registreredes personoplysninger, at den registreredes rettigheder ikke bliver iagttaget, eller at den dataansvarlige har utilstrækkelig IT-sikkerhed.

Datatilsynet behandler alle klagerne grundigt, og i hver enkelt sag overvejer tilsynet nøje, om der skal indledes en undersøgelse af det forhold, der er klaget over.

I en del tilfælde beslutter Datatilsynet, at der ikke skal indledes en nærmere undersøgelse af sagen. Det kan f.eks. være tilfældet, hvis der med stor sandsynlighed ikke er foregået noget i strid med databeskyttelsesreglerne, eller hvis der i øvrigt ikke er udsigt til, at tilsynet vil kunne hjælpe klageren til at opnå en bedre retsstilling.

I andre tilfælde foretager Datatilsynet en undersøgelse af sagen. En undersøgelse kan have forskelligt omfang og udfald, alt efter hvad sagen handler om, eller hvad det er mest hensigtsmæssigt, at tilsynet gør ved sagen. En undersøgelse kan munde ud i, at Datatilsynet hjælper borgeren videre med sagen, f.eks. ved at klagen sendes til den dataansvarlige, som så får lejlighed til at forholde sig til det, der er klaget over – i mange tilfælde løser det faktisk problemet. En undersøgelse kan også være mere dybdegående og indebære, at Datatilsynet beder den dataansvarlige om en skriftlig redegørelse, hvor den dataansvarlige skal forklare, f.eks. hvilken hjemmel der har dannet grundlag for behandlingen af personoplysningerne, og hvad formålet med behandlingen har været. Derefter kan Datatilsynet forholde sig til, om databeskyttelsesreglerne har været overholdt.

En sådan nærmere undersøgelse kan ende med, at tilsynet konkluderer, at alt har været i orden. Det kan også ende med det modsatte, og at tilsynet f.eks. udtaler kritik, meddeler et påbud eller politianmelder den dataansvarlige. Det kommer an på sagens karakter og alvor.

Selvom Datatilsynet ikke indleder nærmere undersøgelser i alle klagesager, følger tilsynet nøje med i, hvor der kan være problemer eller udfordringer med databeskyttelsen. Tilsynet følger f.eks. internt op på de klager, som tilsynet modtager, når der skal udvælges tilsynssubjekter, og Datatilsynet indleder også i øvrigt løbende sager på eget initiativ. Så selv om Datatilsynet ikke iværksætter nærmere undersøgelser i alle enkeltsager, forsøger tilsynet at skabe et større overblik over, hvilke områder der er særlig god grund til at undersøge i dybden – f.eks. fordi området berører mange mennesker, eller fordi der sker behandling af følsomme oplysninger.

Selvom en klage til Datatilsynet måske ikke i sig selv fører til, at tilsynet indleder en undersøgelse af den dataansvarlige, der er klaget over, vil klagen altså alligevel indgå i det grundlag, som Datatilsynets mere overordnede tilsynsaktiviteter baseres på.

One-Stop-Shop-mekanismen

Datatilsynet vurderer i forbindelse med sin behandling af klagesager, om klagen omhandler grænse-overskridende behandling af personoplysninger.

En behandling af personoplysninger anses for at være grænseoverskridende, bl.a. hvis behandlingen finder sted som led i aktiviteter, der udføres for en dataansvarlig i flere medlemsstater, eller hvor den dataansvarlige samtidig er etableret i flere medlemsstater, jf. databeskyttelsesforordningens artikel 4, nr. 23, litra a.

Hvis Datatilsynet vurderer, at en behandling 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 nedenfor følger en række eksempler på klagesager, som Datatilsynet i 2022 traf afgørelse i.

Brugen af Chromebooks i folkeskolens undervisning

En af de mest omtalte sager i 2022 omhandlede brugen af Google-produkter i folkeskolen. Den konkrete sag udsprang af et brud på persondatasikkerheden konstateret i Helsingør Kommune tilbage i januar 2020, men endte i løbet af 2022 med at involvere halvdelen af landets kommuner i et forsøg på at lovliggøre brugen af softwaren i skolerne.

Sagen rummer indtil flere databeskyttelsesretlige problemstillinger, hvor de mest centrale vedrører kommunernes retlige grundlag for, at leverandøren (Google) behandler elevernes oplysninger til egne formål, da dette ikke er hjemlet i folkeskoleloven - og at kommunerne ikke havde formået at tilpasse kontrakter og softwarens virkemåde, så elevernes oplysninger ikke blev videregivet. I den forbindel-

se havde Helsingør Kommune ikke foretaget risikovurdering og konsekvensanalyse, hvilket allerede i 2021 fik tilsynet til at udstede påbud, meddele en advarsel og en midlertidig begrænsning samt udtale alvorlig kritik af kommunen.

I sommeren 2022 nedlagde Datatilsynet et behandlingsforbud mod behandling af Helsingør Kommunes folkeskoleelevers personoplysninger i Google Workspace, hvilket reelt betød, at eleverne efter sommerferien ikke kunne anvende de computere, kommunerne havde udleveret til dem. Helsingør Kommune leverede i løbet af nogle uger et materiale, men tilsynets vurdering var, at det ikke levede op til indholdskravene for en konsekvensanalyse, og tilsynet fastholdt derfor forbuddet.

Herefter blev der indledt et samarbejde mellem KL, Helsingør Kommune og de andre kommuner, der benyttede denne software, om at indgå dialog med leverandøren om at få lovliggjort brugen af Google Workspace.

Datatilsynet suspenderede på den baggrund i september 2022 behandlingsforbuddet og meddelte Helsingør Kommune og de øvrige involverede kommuner et påbud om lovliggørelse.

Sagerne forventes afklaret i løbet af 2023.

Advokatundersøgelser vedrørende seksuelle krænkelser mv.

Datatilsynet traf i 2022 afgørelse i flere sager om iværksættelse og gennemførelse af advokatundersøgelser vedrørende seksuelle krænkelser mv.

TV2 og Norrbom Vinding

Efter behandling af sagen i Datarådet udtalte Datatilsynet alvorlig kritik af TV2 Danmark A/S (TV2) og Norrbom Vinding I/S i en sag, hvor en person havde klaget over behandlingen af oplysninger om ham i forbindelse med en advokatundersøgelse. Undersøgelsen blev gennemført af Norrbom Vinding på vegne af TV2 med henblik på at afdække og undersøge sager om mulige krænkende handlinger.

Datatilsynet fandt, at TV2 forfulgte en legitim interesse i forbindelse med den iværksatte undersøgelse, og at TV2 og Norrbom Vinding derfor kunne indsamle oplysninger med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Datatilsynet fandt ikke grundlag for at tilsidesætte TV2's og Norrbom Vindings vurdering af, at det var nødvendigt at indsamle oplysninger om en bred personkreds for at undersøge (udviklingen af) kulturen på TV2, og at TV2's legitime interesse heri gik forud for de registreredes, herunder klagers, interesser.

Under hensyn til, at klager fortsat havde tilknytning til TV2, fandt Datatilsynet endvidere ikke grundlag for at tilsidesætte TV2's og Norrbom Vindings vurdering af nødvendigheden af at behandle oplysninger om klagers seksuelle forhold for at kunne fastlægge et retskrav, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra f.

Det var imidlertid Datatilsynets opfattelse, at TV2 og Norrbom Vinding ikke havde begrænset indsamlingen af oplysninger på en sådan måde, at de havde den fornødne sikkerhed for at have hjemmel i databeskyttelsesforordningens artikel 9 til at behandle de indsamlede personoplysninger, herunder oplysninger om seksuelle forhold. På den baggrund fandt Datatilsynet, at TV2's og Norrbom Vindings fremgangsmåde ved indsamlingen af personoplysninger ikke var i overensstemmelse med databeskyttelses-forordningens artikel 25, jf. også forordningens artikel 5.

Uanset at Datatilsynet generelt fandt tilrettelæggelsen af undersøgelsen og den deraf følgende indsamling af personoplysninger kritisabel, fandt tilsynet ikke grundlag for at kritisere TV2's og Norrbom Vindings behandling af oplysninger om klagers seksuelle forhold.

Endelig fandt Datatilsynet, at TV2 og Norrbom Vinding ikke havde underrettet klager i overensstemmelse med databeskyttelsesforordningens artikel 12 og artikel 14.

Det Konservative Folkeparti og Plesner

I en anden sag klagede en person til Datatilsynet over, at det Konservative Folkeparti og Plesner Advokatpartnerselskab havde behandlet oplysninger om ham i en advokatundersøgelse. Undersøgelsen blev gennemført af Plesner på vegne af det Konservative Folkeparti og havde til formål at afdække forløbet vedrørende flere anklager om påståede seksuelle krænkelser og overgreb, som var fremsat mod klager i dagspressen.

Datatilsynet fandt i sagen, at det Konservative Folkepartis og Plesners behandling af oplysninger om klager, herunder oplysninger om muligt strafbare forhold og om seksuelle forhold, skete inden for rammerne af reglerne i databeskyttelsesforordningen, jf. dennes artikel 6 og 9, samt databeskyttelseslovens § 8.

Imidlertid fandt Datatilsynet grundlag for at kritisere, at hverken det Konservative Folkeparti eller Plesner i tilstrækkelig grad havde opfyldt deres oplysningspligt efter databeskyttelsesforordningens artikel 14 over for klager i forbindelse med undersøgelsens gennemførelse.

Københavns Kommune og Bech-Bruun

Endelig traf Datatilsynet i 2022 afgørelse i to sager, hvor en person havde klaget over, at henholdsvis Københavns Kommune og Bech-Bruun Advokatpartnerselskab behandlede oplysninger om ham i forbindelse med en advokatundersøgelse. Undersøgelsen blev gennemført af Bech-Bruun på vegne af Københavns Kommune med det formål at afdække, om der havde været udvist krænkende adfærd på uddannelsesinstitutionen Sankt Annæ Gymnasium, samt hvordan sådan adfærd var blevet håndteret.

I den ene sag, som vedrørte Københavns Kommunes behandling af oplysninger om klager i forbindelse med advokatundersøgelsens iværksættelse, fandt Datatilsynet, at kommunens behandling af oplysninger om klager var sket inden for rammerne af databeskyttelsesforordningens artikel 6, stk. 1, litra e. Imidlertid fandt Datatilsynet grundlag for at kritisere, at Københavns Kommune ikke i tilstrækkelig grad havde opfyldt oplysningspligten efter databeskyttelsesforordningens artikel 14, jf. artikel 12, stk. 1.

I den anden sag, som vedrørte Bech-Bruuns behandling af oplysninger om klager i forbindelse med advokatundersøgelsens gennemførelse, fandt Datatilsynet, at Bech-Bruuns behandling af oplysninger om klager, herunder oplysninger om seksuelle forhold, var sket inden for rammerne af databeskyttelses-forordningens artikel 6, stk. 1, litra e, og artikel 9, stk. 2, litra f, samt databeskyttelseslovens § 8, stk. 3 og 4. Imidlertid fandt Datatilsynet grundlag for at kritisere, at Bech-Bruun havde undladt at opfylde oplysningspligten efter databeskyttelsesforordningens artikel 14. Herudover fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at Bech-Bruuns håndtering af en anmodning fra klager om indsigt ikke var sket i overensstemmelse med databeskyttelsesforordningens artikel 15, stk. 3.

Datatilsynet meddelte i den forbindelse et påbud til Bech-Bruun om på ny at tage stilling til klagers indsigtsanmodning. Efterfølgende bekræftede Bech-Bruun at have imødekommet Datatilsynets påbud.

Videregivelse af personoplysninger i forbindelse med regressag

Datatilsynet traf i 2022 afgørelse i en sag, hvor Civilstyrelsen i forbindelse med behandlingen af en regressag havde videregivet oplysninger om skadelidte til skadevolderen.

Civilstyrelsen havde over for Datatilsynet anført, at styrelsen har behov for at kunne godtgøre over for skadevolder, at der er et erstatningsretligt krav mod denne, og at der er årsagssammenhæng mellem den strafbare handling, skadevolderen har begået, og den erstatning, der er udbetalt til den skadelidte, herunder størrelsen af erstatningen. Civilstyrelsen fandt derfor, at det var nødvendigt at videregive oplysninger om skadelidte til skadevolder.

Civilstyrelsen anførte dog samtidig, at visse oplysninger ikke havde været nødvendige at videregive, for at skadevolder kunne forholde sig til kravet, og derfor burde have været undtaget.

Datatilsynet var enig i Civilstyrelsens vurdering og bemærkede, at det i en sag som denne er særligt vigtigt at være opmærksom på, at der kun bliver videregivet oplysninger om skadelidte til skadevolder, som er nødvendige for behandlingen af regressagen.

Datatilsynet fandt på den baggrund – efter at sagen havde været behandlet i Datarådet – anledning til at udtale alvorlig kritik af, at Civilstyrelsen havde videregivet oplysninger om skadelidte til skadevolder, som ikke var nødvendige at videregive.

For så vidt angik de øvrige oplysninger om skadelidte, som var blevet videregivet til skadevolder, fandt Datatilsynet ikke tilstrækkeligt grundlag for at tilsidesætte Civilstyrelsens vurdering af, at oplysningerne var nødvendige at videregive, for at skadevolder kunne forholde sig til regreskravet.

Skolers indhentelse og videregivelse af referencer fra tidligere praktiksted uden samtykke

Datatilsynet har i 2022 behandlet to sager, som udsprang af samme forhold, idet en folkeskole (skole A) – i forlængelse af en samtale med klager om en mulig praktikplads – havde indhentet reference fra klagerens tidligere praktiksted (skole B).

Klageren klagede både over, at skole A indhentede en reference om klager fra skole B, og at skole B videregav en reference om klager til skole A.

Skole A oplyste til sagen, at skolen anså samtalen som uforpligtende, da der var tale om en stilling, som endnu ikke var slået op. Af den grund journaliserede Skole A ikke noget i forbindelse med samtalen – heller ikke den indhentede reference fra skole B.

Datatilsynet fandt, at skole A's indhentelse af oplysninger om klager ikke var omfattet af databeskyttelsesreglerne, da de indsamlede oplysninger ikke blev – eller var bestemt til at blive – behandlet elektronisk eller indgå i et register. Tilsynet tog ikke herved stilling til, om journal- og notatpligten var overholdt.

Derudover fandt Datatilsynet, at skole B's videregivelse af referencen i det konkrete tilfælde kunne rummes inden for myndighedens snævre rum for at benytte sig af interesseafvejningsreglen.

Datatilsynet lagde i den forbindelse vægt på, at skole B var af den opfattelse, at klager havde indvilget i, at referencen kunne videregives, da skole A havde oplyst dette. Grundet karakteren af oplysningerne havde skole B ikke en særlig pligt til at tage yderligere skridt for at sikre sig klagers accept.

Gennemgang af omfattende materiale i forbindelse med en anmodning om indsigt

Datatilsynet behandlede i 2022 en sag, hvor det væsentligste spørgsmål var, i hvilket omfang man som dataansvarlig er forpligtet til at gennemgå materiale for at imødekomme en anmodning om indsigt, når der er tale om et meget stort antal dokumenter, som i al væsentlighed er udarbejdet i forbindelse med den indsigtssøgendes arbejdsopgaver. Sagen handlede om en person, der havde anmodet om indsigt i forbindelse med en verserende retssag.

Anmodningen om indsigt ville gøre det nødvendigt at identificere, indsamle, gennemgå og vurdere mere end en mio. dokumenter fordelt på forskellige selskaber for at afgøre, hvorvidt personoplysninger om klager, der måtte fremgå af disse dokumenter, skulle udleveres.

Den store mængde dokumenter, som kunne indeholde oplysninger om klager, relaterede sig i al væsentlighed til virksomheden Q, hvor klager var bestyrelsesmedlem, og virksomheden Z, hvor klager var administrerende partner, samt til igangværende retssager, herunder mod klager, i forlængelse af en virksomhedsoverdragelse.

Under disse omstændigheder fandt Datatilsynet – efter at sagen havde været behandlet i Datarådet –

at de dataansvarlige ikke var forpligtet til at fremsøge og gennemgå dokumenterne for at identificere og udlevere oplysninger om klager. På den baggrund fandt Datatilsynet ikke grundlag for at kritisere de dataansvarliges håndtering af klagers anmodning om indsigt.

Datatilsynet lagde vægt på, at klager ikke nærmere havde specificeret sin anmodning sådan, at omfanget af materiale, som skulle gennemgås for at identificere eventuelle oplysninger om ham, blev nedbragt.

Datatilsynet lagde herefter vægt på, at der var tale om et større antal dokumenter, som kunne indeholde oplysninger om klager, men hvor man måtte antage, at eventuelle oplysninger om klager kun ville optræde "accessorisk" i forhold til formålet med dokumenterne (i denne sammenhæng virksomhedsdrift).

Afgørelsen ligger således i forlængelse af tidligere afgørelser om samme emne, herunder om arbejdsgiveres mulighed for at afvise anmodninger om indsigt.

Afslag på indsigt i tv-overvågningsoptagelser fra stadion var berettiget

Datatilsynet traf i 2022 afgørelse i en sag, hvor DBU og Divisionsforeningen afviste at give en registreret indsigt i tv-overvågningsoptagelser foretaget i forbindelse med en fodboldkamp på Blue Water Arena i Esbjerg, hvor han var tilskuer.

I sagen havde tilskueren anmodet om indsigt i en række tv-overvågningsoptagelser fra kampen, som han skulle bruge i forbindelse med en erstatningssag mod politiet.

DBU og Divisionsforeningen afviste at udlevere overvågningsmaterialet under generel henvisning til, at indsigt ville kunne kompromittere sikkerheden på det pågældende stadion, idet bl.a. kameraernes placering og blinde vinkler derved kunne blive afsløret.

Datatilsynet fandt ikke grundlag for at tilsidesætte DBU og Divisionsforeningens vurdering af, at klagers konkrete interesse i at få indsigt burde vige for afgørende hensyn til den offentlige sikkerhed, idet der var tale om et større stadion, hvor mange mennesker er samlet på begrænset plads, og hvor uroligheder kan opstå, hvorved bl.a. tilskuere vil kunne blive udsat for væsentlig fare. Derfor fandt tilsynet, at DBU og Divisionsforeningen var berettiget til at afvise klagers anmodning om indsigt, jf. databeskyttelseslovens § 22, stk. 1 og 2.

Datatilsynet bemærkede dog, at en dataansvarlig ved modtagelse af en indsigtsanmodning er forpligtet til at foretage en konkret vurdering af den registreredes interesse i at modtage oplysningerne over for de afgørende hensyn, som eventuelt kan begrunde, at indsigtsanmodningen ikke imødekommes. Datatilsynet henstillede, at DBU og Divisionsforeningen fremadrettet foretager en sådan konkret vurdering af modtagne indsigtsanmodninger, herunder af den registreredes konkrete interesse i helt eller delvist at modtage oplysningerne.

Underdatabehandler afviste at udlevere oplysninger til den dataansvarlige

Datatilsynet traf i 2022 afgørelse i en sag, hvor en dataansvarlig havde klaget over, at deres tidligere underleverandør af et it-system ikke ville tilbagelevere den dataansvarliges kundeoplysninger.

Det fremgik af sagen, at databehandleren havde indgået en databehandleraftale med en underdatabehandler, hvori databehandleren (og ikke den oprindelige dataansvarlige) var anført som dataansvarlig over for underdatabehandleren.

Underdatabehandleren afviste at have handlet i strid med databeskyttelsesforordningen ved ikke at imødekomme den dataansvarliges krav om udlevering af data med henvisning til denne aftale. De anførte, at de som forhandlerens underdatabehandler ikke var underlagt den dataansvarliges direkte instruktionsbeføjelse, hvorfor den oprindelige dataansvarlige ikke kunne instruere dem i at tilbagelevere kundeoplysningerne.

Datatilsynet fandt i sagen frem til, at de nævnte kundeoplysninger både af databehandleren og underdatabehandleren de facto blev behandlet på vegne af den oprindelige dataansvarlige. Derfor kunne det forhold, at underdatabehandleren og databehandleren havde indgået en databehandleraftale, hvori databehandleren var anført som værende dataansvarlig, ikke føre et andet resultat. Datatilsynet fandt altså, at det afgørende for vurderingen af, hvem der er dataansvarlig eller databehandler, er de faktiske omstændigheder, og ikke hvad der måtte være aftalt kontraktuelt mellem to databehandlere.

I den sammenhæng bemærkede Datatilsynet, at underdatabehandleren selv havde fastlagt formålet med opbevaringen ved ikke at imødekomme den dataansvarliges anmodning om tilbagelevering af de omtalte kundedata og derved også blev selvstændig dataansvarlig for den fortsatte opbevaring af kunde-oplysningerne.

Datatilsynet udtalte på den baggrund alvorlig kritik, ligesom tilsynet udstedte et påbud om tilbagelevering af kundeoplysningerne og et forbud mod at behandle de omtalte kundeoplysninger, medmindre behandlingen skete efter den dataansvarliges instruks.

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 2022

Datatilsynet offentliggjorde i januar 2022 en oversigt over, hvilke områder tilsynet særligt vil 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 2022

Arkivloven
Regler om beskyttelse af personoplysninger er først og fremmest fastsat i databeskyttelsesforordningen og databeskyttelsesloven, men er også indeholdt i anden lovgivning, herunder i arkivlovgivningen.

Ifølge arkivloven har bl.a. kommunerne i en række tilfælde mulighed for at oprette egne arkiver. Det følger endvidere af loven, at arkivalier hos de offentlige arkiver som udgangspunkt bliver umiddelbart tilgængelige efter 20 år, og borgere kan dermed få adgang til at se disse arkivalier uden yderligere tilladelse fra det offentlige arkiv. For visse typer af arkivalier gælder der dog længere tilgængelighedsfrister end 20 år. Hvis der f.eks. er tale om arkivalier, der indeholder oplysninger om enkeltpersoners private, herunder økonomiske forhold, er de først tilgængelige efter 75 år.

Hvis tilgængelighedsfristen endnu ikke er udløbet, kan der søges om tilladelse til at benytte arkivalierne. Den, der søger om tilladelse, skal oplyse om formålet med den tilsigtede benyttelse af de oplysninger, der søges adgang til. Er der tale om arkivalier, som er afleveret af en offentlig myndighed og som indeholder oplysninger om enkeltpersoners rent private forhold, og har den tidligere behandling være omfattet af databeskyttelsesforordningen, skal det offentlige arkiv indhente samtykke fra Datatilsynet, inden der gives tilladelse til benyttelse af arkivalierne.

Datatilsynet har i 2022 valgt at føre tilsyn med en række kommuners håndtering af arkivalier, herunder kommunernes overholdelse af de særlige regler om adgang til arkivalier inden tilgængelighedsfristernes udløb.

Tilladelser til at behandle følsomme personoplysninger i den private sektor
Private virksomheder mv. kan på nærmere fastsatte vilkår i helt særlige tilfælde få tilladelse fra Datatilsynet til at behandle følsomme oplysninger i databeskyttelsesforordningens forstand, hvis behandling af oplysninger er nødvendig af hensyn til væsentlige samfundsinteresser.

Datatilsynet har besluttet i 2022 at føre tilsyn med, om de vilkår, som Datatilsynet har fastsat i forbindelse med en række tilladelser, bliver overholdt.

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

Datatilsynet har i 2022 valgt at føre tilsyn med en række private aktørers iagttagelse af oplysningspligten, når disse dataansvarlige henvender sig uanmodet over for de registrerede.

Forsyningsselskabers håndtering af anmodninger om indsigt og sletning
Datatilsynet modtager jævnligt henvendelser fra borgere, der klager over forsyningsselskabers besvarelse af anmodninger om indsigt i eller sletning af personoplysninger, som selskaberne behandler.

I 2022 retter Datatilsynet derfor fokus mod forsyningsselskabers håndtering af anmodninger fra de registrerede om indsigt og sletning.

Behandling af personoplysninger om hjemmesidebesøgende
Som opfølgning på Datatilsynets vejledning fra februar 2020 om behandling af personoplysninger om hjemmesidebesøgende og de tilsynssager, som tilsynet behandlede på dette område i 2021, har Datatilsynet for at fastholde fokus på området besluttet også i 2022 at iværksætte tilsyn inden for dette felt.

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.

Databeskyttelsesforordningens regler om databeskyttelse gennem design og udarbejdelse af konsekvensanalyser skal sikre, at de fornødne garantier i behandlingen integreres fra starten, når it-løsninger designes, udvikles, indkøbes eller tilpasses med henblik på at opfylde forordningens krav og beskytte de registreredes rettigheder.

En konsekvensanalyse vedrørende databeskyttelse er en proces, der bl.a. har til formål at vurdere behandlingens nødvendighed og proportionalitet samt at bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger medfører.

Vurdering af risici er også en del af kravene til behandlingssikkerhed generelt, men konsekvensanalysen går et skridt videre ved at inkludere en proces, der blandt andet kan omfatte høring hos Datatilsynet og indhentning af de registreredes synspunkter vedrørende den planlagte behandling. Det er endvidere en proces, hvor der stilles specifikke krav til dokumentation.

Til gengæld er det kun i visse situationer, at den dataansvarlige skal lave en konsekvensanalyse. Der er databehandlinger, hvor det navnlig er påkrævet at udføre en konsekvensanalyse, jf. i den forbindelse også den liste, som Datatilsynet offentliggjorde i januar 2019 over de typer af behandlingsaktiviteter, der altid er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse. Ved andre behandlinger beror det på en konkret vurdering, hvorvidt en konsekvensanalyse er påkrævet. Det er i første omgang den dataansvarlige selv, der skal foretage denne vurdering.

Datatilsynet har i 2022 besluttet at føre tilsyn med persondatasikkerheden mv. inden for følgende områder:

- fællesoffentlige it-løsninger,
- fællesstatslige it-løsninger,
- om brud på persondatasikkerheden håndteres og anmeldes i overensstemmelse med reglerne herom,
- om der i de tilfælde, hvor der foreligger en høj risiko for de registrerede som følge af et brud på persondatasikkerheden, sker den fornødne underretning af de berørte registrerede og
- om de dataansvarlige i forbindelse med, at it-løsninger designes, udvikles, indkøbes eller tilpasses, overholder reglerne om databeskyttelse gennem design og udarbejdelse af konsekvensanalyser.

Alt efter karakteren af de pågældende områder, vil tilsynene i varierende grad rette sig mod forskellige dataansvarlige i den private og i den offentlige sektor, og Datatilsynet vil i forbindelse med disse tilsyn også gøre brug af mere generelle screeningsmetoder hos et større antal dataansvarlige.

Kontrol med databehandlere
Virksomheder kan som dataansvarlige overlade personoplysninger til andre aktører, der som databehandlere herefter står for behandlingen af oplysningerne. Når man gør brug af databehandlere, skal man – foruden at indgå en databehandleraftale – føre en passende kontrol (tilsyn) med databehandleren. De enkelte dataansvarlige har med andre ord en selvstændig forpligtelse til at føre kontrol med, om en databehandler overholder den dataansvarliges instrukser for behandlingen.

Datatilsynet har siden 2016 løbende haft fokus på kontrol med databehandlere, og tilsynet har besluttet i 2022 at føre tilsyn med, om private virksomheder fører passende kontrol med sine databehandlere.

Tv-overvågning
Datatilsynet besluttede i 2021 at føre tilsyn med en række private og offentlige myndigheders behandling af personoplysninger i forbindelse med tv-overvågning, navnlig i lyset af den ændring af tv-overvågningsloven, som trådte i i kraft den 1. juli 2020.

Datatilsynet har valgt fortsat at fokusere en række af sine tilsynsaktiviteter på tv-overvågningsområdet, hvorfor Datatilsynet i 2022 vil udføre flere tilsyn med private og offentlige myndigheders behandling af personoplysninger i forbindelse med tv-overvågning.

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 har besluttet i 2022 at føre tilsyn med en række myndigheders behandling af personoplysninger i forbindelse med anvendelsen af nogle af de nævnte informationssystemer.

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 har i 2022 valgt at føre tilsyn med de retshåndhævende myndigheders overholdelse af en række af lovens bestemmelser, herunder sletning af personoplysninger og behandlingssikkerhed.

Oversigt over udførte tilsyn i 2022

Offentlige myndigheder:
Billund Kommune
Digitaliseringsstyrelsen
Faxe Kommune
Gentofte Kommune
Gladsaxe Kommune
Greve Kommune
Gribskov Kommune
Ishøj Kommune
Københavns Kommune
Norddjurs Kommune
Næstved Kommune
Odense Kommune
Region Hovedstaden
Region Sjælland
Region Syddanmark
Rigsarkivet
Ringsted Kommune
Roskilde Kommune
Rudersdal Kommune
Sønderborg Kommune
Tårnby Kommune
Udlændingestyrelsen
Økonomistyrelsen
Aabenraa Kommune
Aalborg Kommune
Aarhus Kommune

Private virksomheder:
Alm. Brand Forsikring A/S
Andel Energi A/S
Andy's
b.energy A/S
Børns Vilkår
Danica Pension Livsforsikringsaktieselskab
Det Faglige Hus
Falck A/S
Falck Healthcare A/S
Familieretshuset
Folkekirkens Nødhjælp
GHP Gildhøj Privathospital ApS
Hjerteforeningen
HK/Danmark A/S
Ingrid Jespersens Gymnasieskole
Jehovas Vidner (Sjælsø Menighed)
LB Forsikring A/S
Moderaterne

Modstrøm Danmark A/S
Norlys Energi A/S
Old Irish Pub Denmark A/S
RED Center mod æresrelaterede konflikter
RedenUng
Røde Kors
S/I Arbejdsmarkedets Erhvervssikring
Sex & Samfund
Skattestyrelsen
Strømtid ApS
Topdanmark Forsikring A/S
Tryg Forsikring A/S
Tuba Aarhus
Ullits Winther Statsautoriseret Revisionspartnerselskab
Veganerpartiet
Ældre Sagen

Fælleseuropæiske systemer

Rigspolitiet
Udlændinge- og Integrationsministeriet
Udenrigsministeriet

Tilsyn baseret på digital screening

Offentlige myndigheder:
Albertslund Kommune
Assens Kommune
Bornholms Regionskommune
Brøndby Kommune
Brønderslev Kommune
Dragør Kommune
Fanø Kommune
Fredensborg Kommune
Fredericia Kommune
Frederiksberg Kommune
Frederikssund Kommune
Faaborg-Midtfyn Kommune
Haderslev Kommune
Halsnæs Kommune
Herlev Kommune
Herning Kommune
Holstebro Kommune
Horsens Kommune
Høje-Taastrup Kommune
Ikast-Brande Kommune
Kerteminde Kommune
Kolding Kommune
Køge Kommune

Lejre Kommune
Lemvig Kommune
Lyngby-Taarbæk Kommune
Læsø Kommune
Middelfart Kommune
Morsø Kommune
Nordfyns Kommune
Nyborg Kommune
Odsherred Kommune
Rebild Kommune
Region Hovedstaden
Region Midtjylland
Region Nordjylland
Region Sjælland
Region Syddanmark
Rødovre Kommune
Samsø Kommune
Silkeborg Kommune
Skive Kommune
Slagelse Kommune
Stevns Kommune
Struer Kommune
Svendborg Kommune
Thisted Kommune
Tønder Kommune
Vallensbæk Kommune
Vejen Kommune
Vejle Kommune
Vesthimmerlands Kommune
Viborg Kommune
Vordingborg Kommune
Ærø Kommune

Tilsyn med en række kommuner og regionernes modenhed på databeskyttelsesområdet

Som led i Datatilsynets strategi om en mere data- og risikobaseret tilgang til vejledning og kontrol har Datatilsynet i forlængelse af lignende tilsyn foretaget i 2020 og 2021 også i 2022 gennemført tilsyn baseret på egen-evaluering hos de dataansvarlige for at belyse den generelle modenhed på udvalgte sikkerhedsområder. Der blev i 2022 gennemført tilsyn hos 50 kommuner og alle 5 regioner.

Formålet med egen-evalueringen er både at give Datatilsynet blik for bestemte emneområder med behov for øget indsats, men også at understøtte en mere forebyggende tilgang. Det er tanken, at den dataansvarlige gennem den interne proces med besvarelse af de stillede spørgsmål bliver mere bevidst om relevante databeskyttelsesretlige overvejelser og forhold.

2022-tilsynet indikerede, at der hos de udvalgte dataansvarlige generelt var behov for større fokus på:

- stillingtagen til, hvilke procedurer der skal følges, når personoplysninger skal slettes fra behandlingssystemer
- styring af brugeres adgangsrettigheder og kontrol med adgangsrettigheder
- foranstaltninger ved udsendelse af mails med personoplysninger
- implementering af foranstaltninger, der reducerer risikoen for, at personoplysninger sendes forkert.

Derudover indikerede 2022-tilsynet, at arbejdet med konsekvensanalyser og test af beredskab i mindre grad er i fokus, særligt i kommunerne. Det kan betyde, at der sker behandling af personoplysninger i kommunerne, hvor risikoen for de registrerede ikke er tilstrækkeligt adresseret. Ligeledes er det Datatilsynets holdning, at test af beredskab udgør grundlæggende sikkerhed til at retablere drift under angreb og til at håndtere hændelser.

I 2022-tilsynet valgte Datatilsynet at lade de 20 tekniske minimumskrav til it-sikkerheden i statslige myndigheder danne baggrund for en række af spørgsmålene. Kravene skal beskytte offentlige arbejdspladser mod ondsindede cyber- og informationssikkerhedshændelser, og de vedrører generelle tekniske og organisatoriske foranstaltninger, som i vidt omfang overlapper med de databeskyttelsesretlige krav til persondatasikkerheden. Flere af disse foranstaltninger har længe været anbefalet generelt – og altså ikke kun overfor statslige myndigheder.

Alle organisationer, der deltog i 2022-tilsynet, modtog som afslutning på tilsynene en rapport med en række konkrete anbefalinger for det videre arbejde med databeskyttelse, herunder i forhold til foranstaltninger til sikring af informationssikkerheden.

Datatilsynet valgte endvidere på baggrund af svarene at gennemføre et fysisk tilsynsbesøg hos en af de kommuner, der deltog. Formålet med tilsynet var bl.a. at foretage en overordnet vurdering af Mariager Kommunes modenhed i forhold til databeskyttelse, herunder navnlig på sikkerhedsområdet.

På baggrund af tilsynet fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at kommunen havde opbevaret personoplysninger ud over, hvad der var nødvendigt i forhold til formålet, og af at kommunen ikke havde indført retningslinjer eller tilsvarende organisatoriske foranstaltninger for sletning af personoplysningerne, hvor tekniske foranstaltninger ikke var muligt.

Datatilsynet fandt endvidere grundlag for at udtale alvorlig kritik af, at kommunen – ved ikke at udføre kontrol af logoplysninger, ved ikke at have implementeret multifaktor-autentifikation eller andet ekstra lag af verifikation, og ved ikke at begrænse medarbejdernes rettigheder til at installere programmer på deres devices – ikke havde truffet passende sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er ved kommunens behandling af personoplysninger.

Derudover fandt Datatilsynet grund for at meddele kommunen påbud om at udarbejde en liste over kommunens systemer, hvori der bliver behandlet personoplysninger, at slette personoplysninger, hvor det ikke længere er nødvendigt for kommunen at opbevare oplysningerne, og at udarbejde en plan for, hvordan kommunen i samarbejde med kommunens systemleverandører kan få slettet personoplysninger i kommunens systemer, som kommunen ikke længere har et formål med at opbevare.

Datatilsynet fandt endvidere grund til at meddele påbud om at fjerne medarbejderes rettigheder til at installere programmer og eksekvere skadelig kode mv. på de computere og devices, der kan tilsluttes kommunens netværk.

Undersøgelse af en række hjemmesiders samtykkeløsninger

Siden 2020 har behandling af oplysninger om hjemmesidebesøgende været et fokusområde for Datatilsynet, og tilsynet valgte også i 2022 at føre tilsyn med, om de betingelser der stilles til et databeskyttelsesretligt samtykke var opfyldt i forbindelse med en række hjemmesiders indhentelse af samtykke til behandling af personoplysninger.

DBA's samtykkeløsning på www.dba.dk

I 2022 afsluttede Datatilsynet et tilsyn med Den Blå Avis (DBA), som tilsynet havde indledt i juni 2020. Efter Datatilsynet indledte sin undersøgelse, valgte DBA at ændre sin samtykkeløsning på www.dba.dk. Datatilsynet tog derfor stilling til to forskellige samtykkeløsninger i afgørelsen.

DBA anførte i forbindelse med sagens behandling, at behandling af oplysninger om hjemmesidebesøgende til analytiske og statistiske formål kunne baseres på selskabets legitime interesser. I den forbindelse benyttede DBA sig af statistik- og analyseværktøjet Google Analytics.

Datatilsynet fandt – efter sagen havde været behandlet på et møde i Datarådet – anledning til at udtale alvorlig kritik af, at hverken DBA's tidligere eller efterfølgende samtykkeløsning til behandling af personoplysninger om de besøgende på www.dba.dk opfyldte databeskyttelsesforordningens betingelser for et gyldigt samtykke.

Endvidere fandt Datatilsynet, at DBA's fornyede samtykkeløsning til behandling af personoplysninger ikke opfyldte det grundlæggende princip om lovlighed, rimelighed og gennemsigtighed i databeskyttelsesforordningen.

Datatilsynet fandt herudover, at DBA's behandling af personoplysninger til statistiske formål ikke var i overensstemmelse med databeskyttelsesforordningen.

JP/Politikens samtykkeløsning på www.eb.dk

Datatilsynet afsluttede i 2022 også et tilsyn med JP/Politikens samtykkeløsning på www.eb.dk, som tilsynet havde indledt i november 2021. JP/Politiken anvendte en samtykkeløsning, der gav besøgende på www.eb.dk tre valgmuligheder (Kun nødvendige, Tilpas indstillinger og Acceptér alle).

Af samtykkeløsningens "første lag" fremgik det, at JP/Politiken behandlede personoplysninger til statistik- og markedsføringsformål. I samtykkeløsningens "andet lag", som den besøgende kunne tilgå ved at klikke på Tilpas indstillinger, kunne den besøgende tilvælge behandlingsformålene præferencer, statistik og markedsføring.

Datatilsynet vurderede, at besøgende på www.eb.dk ikke afgav et informeret samtykke, idet besøgende, som klikkede Acceptér alle, ikke modtog information om alle behandlingsformål – da information om præferenceformålet først fremgik af "andet lag".

Med afgørelsen fastslog tilsynet, at der er store frihedsgrader for brug af farvevalg og designelementer, så længe designet ikke "skubber" brugeren i retning af valg, der fører til ulovlige scenarier eller undergraver den registreredes rettigheder. I det konkrete tilfælde, hvor valgmuligheden Acceptér alle førte til et mangelfuldt samtykke, fandt tilsynet, at designet stred mod princippet om lovlighed, rimelighed og gennemsigtighed.

Datatilsynet udtalte på baggrund af ovenstående alvorlig kritik af JP/Politikens behandling af oplysninger om hjemmesidebesøgende.

Behandling af personoplysninger i forbindelse med udbud af internetkonkurrencer

Datatilsynet traf i 2022 afgørelse i en sag, hvor tilsynet på baggrund af en henvendelse fra Forbrugerombudsmanden besluttede at undersøge SmartResponse A/S' behandling af personoplysninger. Spørgsmålene om samtykkets gyldighed og behandling af oplysninger i forbindelse med spørgeskemaer blev afgjort efter forelæggelse for Datarådet.

For at deltage i en internetkonkurrence skulle deltagere samtykke til, at SmartResponse kunne behandle oplysninger om dem, og at SmartResponse kunne videregive oplysningerne til virksomhedens samarbejdspartnere. Datatilsynet fandt, at samtykket, som SmartResponse indhentede, var i overensstemmelse med databeskyttelsesreglerne.

Samtykkets opbygning gav imidlertid Datatilsynet anledning til at overveje, om kravet om frivillighed, herunder kravet om granularitet, var opfyldt, idet SmartResponse indsamlede personoplysninger til egen brug og videregav oplysningerne til brug for samarbejdspartnernes direkte markedsføring. SmartResponse tilbød deltagere i internetkonkurrencen at udfylde et spørgeskema med henblik på at tilpasse markedsføring til den enkeltes personlige behov.

Spørgeskemaoplysningerne blev videregivet til samarbejdspartnerne på baggrund af databeskyttelseslovens § 13, stk. 2. Datatilsynet fandt det tvivlsomt, om databeskyttelseslovens § 13, ligger inden for det nationale råderum, som databeskyttelsesforordningens artikel 6, stk. 2-3, tillader. Datatilsynet undlod derfor i sagen at anvende databeskyttelseslovens § 13, og vurderede i stedet videregivelsen efter interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f. Datatilsynet fandt, at spørgeskemaoplysningerne var for detaljerede til at kunne videregives efter interesseafvejningsreglen, og at oplysningernes videregivelse derfor forudsatte samtykke.

SmartResponse oplyste, at virksomheden opbevarer oplysninger for at kunne dokumentere gyldigheden af et indhentet samtykke. SmartResponse havde endvidere oplyst, at når et samtykke blev trukket tilbage, blev deltagerens telefonnummer og e-mailadresse registreret på en nej-tak-liste. Endelig havde SmartResponse oplyst, at opbevaringsperioden for oplysningerne var 5 år i henhold til forældelsesfristen i databeskyttelses-loven. Datatilsynet fandt i den forbindelse, at en opbevaringsperiode på 5 år – fastsat efter forældelsesfristen i databeskyttelsesloven – ikke er overensstemmende med princippet om opbevaringsbegrænsning.

Tilsyn med banker og sparekassers håndtering af indsigtsanmodninger fra kunder

I 2022 afsluttede Datatilsynet en række tilsyn med 5 udvalgte bankers og sparekassers håndtering af indsigtsanmodninger fra kunder. Tilsynene fokuserede på retningslinjer og procedurer for håndtering af kunders anmodninger om indsigt.

Bankerne og sparekasserne var bl.a. udvalgt baseret på antallet af klager hos Datatilsynet og bestod af Danske Bank A/S, Sparekassen Sjælland-Fyn A/S, Basisbank A/S, Sparekassen Kronjylland og Ringkjøbing Landbobank Aktieselskab.

Datatilsynet fandt, at procedurerne hos fire ud af 5 banker understøttede retten til indsigt. Datatilsynet udtalte alvorlig kritik af, at Danske Banks procedure for at håndtere anmodninger om indsigt fra kunder ikke var i overensstemmelse med databeskyttelsesreglerne. Datatilsynet fandt, at bankens procedure, som bestod i en lagdelt tilgang, hvor kunden kunne få indsigt i sine oplysninger på tre forskellige måder, ikke var i overensstemmelse med databeskyttelsesforordningen.

Datatilsynet fandt endvidere, at Sparekassen Sjælland-Fyn A/S', Basisbank A/S', Sparekassen Kronjylland og Ringkjøbing Landbobank Aktieselskabs procedurer for at håndtere anmodninger om indsigt fra kunder understøttede retten til indsigt.

Af Datatilsynets afsluttende udtalelser i de enkelte tilsyn fremgår bl.a. følgende:

- at Sparekassen Sjælland-Fyn A/S' procedure for at besvare af anmodninger om indsigt fra kunder består i at danne en indsigtsrapport suppleret med en manuel gennemgang af systemer og databaser, som den tekniske løsning ikke omfatter.
- at Basisbank A/S har udarbejdet skabeloner til at besvare anmodninger om indsigt fra kunder, og at banken vedlægger en kopi af de oplysninger, som banken behandler om den pågældende.
- at Sparekassen Kronjyllands håndtering af indsigtsanmodninger består i manuelt at danne en indsigtsrapport samt at supplere med øvrige oplysninger, der måtte være relevante i den enkelte sag. Datatilsynet henstillede til, at Sparekassen Kronjylland samler sine mange arbejdsgange for håndtering af indsigtsanmodninger for at understøtte en ensartet praksis i organisationen samt at tydeliggøre proceduren i arbejdsgangen.
- at Ringkjøbing Landbobank Aktieselskab danner en indsigtsrapport, når banken besvarer en anmodning om indsigt, og vedlægger eventuelt yderligere materiale, som kunden samtidig efterspørger. Datatilsynet henstillede til, at Ringkjøbing Landbobank Aktieselskab tydeliggør processen for håndtering af indsigtsanmodninger i bankens arbejdsgang.

Tilsyn med behandling af personoplysninger til brug for forskning

I 2022 afsluttede Datatilsynet to tilsyn med henholdsvis Region Hovedstaden og Region Syddanmark, som tilsynet havde indledt i efteråret 2020. De to tilsyn fokuserede på regionernes aktiviteter på forskningsområdet.

I forbindelse med tilsynene modtog Datatilsynet bl.a. en fortegnelse over igangværende forskningsprojekter hos de to regioner. Datatilsynet udvalgte på den baggrund tre forskningsprojekter i hver region som genstand for undersøgelsen inden for emnerne "behandlingsgrundlag" og "ansvar og roller (dataansvar)".

Datatilsynet fandt ikke grundlag for at tilsidesætte Region Hovedstadens vurdering af grundlaget for behandlingen af personoplysninger i de tre projekter. Imidlertid udtalte Datatilsynet kritik af, at Region Hovedstaden i et af projekterne ikke havde ført et tilstrækkeligt tilsyn med en databehandler inden for rammerne af det tilsynsniveau, som regionen havde fundet passende. Datatilsynet fandt det endvidere kritisabelt, at regionen i et andet projekt ikke havde fulgt regionens egen model for fastsættelse af til-synsniveau.

Datatilsynet fandt heller ikke anledning til at tilsidesætte Region Syddanmarks vurdering af grundlaget for behandlingen af personoplysninger i de tre projekter. Dog udtalte Datatilsynet kritik af, at regionen for så vidt angik to databehandleraftaler ikke havde påvist, at der var taget stilling til, på hvilket niveau regionen som dataansvarlig ville føre tilsyn med databehandleren. I den forbindelse havde regionen heller ikke påvist, at regionens retningslinje for tilsyn med databehandlere var blevet fulgt.

Datatilsynet lagde ved sine tilsyn vægt på, at en dataansvarlig skal påse behandlingssikkerheden hos sine databehandlere. Det skyldes, at den dataansvarlige skal iagttage kravet om ansvarlighed og derved skal kunne påvise, at en behandling af personoplysninger er i overensstemmelse med reglerne i databeskyttelses-forordningen. Datatilsynet udtalte, at den dataansvarlige efter tilsynets opfattelse ikke vil kunne leve op til dette krav ved blot at indgå en databehandleraftale med databehandleren. Den dataansvarlige må tillige føre et (større eller mindre) tilsyn med, at den indgåede databehandleraftale overholdes, herunder at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Oplysningspligt i forbindelse med behandling af personoplysninger til brug for forskning

I 2021 indledte Datatilsynet af egen drift en undersøgelse af Region Hovedstadens opfyldelse af oplysningspligten i forbindelse med regionens behandling af oplysninger til brug for (fremtidig) forskning.

Under sagen kom det frem, at det er generel praksis hos Region Hovedstaden, at overskydende biologisk materiale fra patientbehandling opbevares i regionens biobank med henblik på benyttelse af materialet til fremtidig forskning. Endvidere kom det frem, at Region Hovedstaden opfyldte sin oplysningspligt ved at henvise og linke til regionens privatlivspolitik i en række standardprodukter, som patienter modtog.

Datatilsynet vurderede imidlertid, at Region Hovedstadens privatlivspolitik havde en generel karakter og rettede sig mod både patienter, ansatte og borgere, og at teksten om forskning i privatlivspolitikken alene oplyste, at regionen anvendte personoplysninger i forbindelse med forskningsaktiviteter uden nærmere at oplyse om konteksten for behandlingen.

Herefter fandt Datatilsynet, at Region Hovedstaden ikke havde givet de nødvendige oplysninger i en gennemsigtig og letforståelig form, hvilket fik tilsynet til at udtale kritik af regionen. Derudover henstillede Datatilsynet til Region Hovedstaden, at regionen overvejede, hvordan den fremadrettet ville opfylde sin oplysningspligt over for patienter.

I sin afgørelse lagde Datatilsynet bl.a. vægt på, at hvis man som dataansvarlig er bekendt med, at ens tjenester er tilgængelige for sårbare medlemmer af samfundet, skal denne sårbarhed indgå i den dataansvarliges vurdering af, hvordan man overholder kravet om gennemsigtighed i relation til de registrerede.

Tilsyn med tv-overvågning af medarbejdere

Datatilsynet traf i 2022 afgørelse i en sag, hvor tilsynet på baggrund af en række konkrete henvendelser fra tidligere ansatte af egen drift havde indledt en sag om Fitness World A/S' tv-overvågning af medarbejdere.

Fitness World A/S foretog den pågældende tv-overvågning med henblik på at forebygge kriminalitet, øge trygheden for medarbejdere og medlemmer samt forebygge grove overtrædelser af interne regler. Fitness World A/S havde bl.a. benyttet optagelser i forbindelse med skriftlige advarsler til ansatte.

Datatilsynet fandt ikke grundlag for at tilsidesætte Fitness World A/S' vurdering af, at behandling af oplysninger om medarbejdere i form af tv-overvågning i kriminalitetsforebyggende og -opklarende øjemed samt for at kunne gøre retskrav gældende over for medarbejderne kunne ske med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Datatilsynet fandt heller ikke grundlag for at konkludere, at behandlingen skulle være sket i strid med forordningens artikel 14, idet medarbejdere i forbindelse med deres ansættelse blev oplyst om tv-overvågningen og formålene hermed – herunder at formålet bl.a. var at kunne gøre retskrav gældende over for medarbejderne.

Datatilsynet udtalte imidlertid alvorlig kritik af, at der i et center var blevet opbevaret oplysninger om medarbejdere i form af bl.a. lægeerklæringer og opsigelser på en fælles computer, hvor oplysningerne havde været tilgængelige for andre medarbejdere, fordi de var blevet gemt på et forkert drev. Dette var ikke i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 1.

Tilsyn med anvendelse af en-faktor login og opbevaring af passwords i klartekst

I 2022 har Datatilsynet truffet afgørelse i to sager om sikkerheden i forhold til anvendelse af en-faktor login og opbevaring af passwords i klartekst.

EG Digital Welfare ApS

I 2022 traf Datatilsynet afgørelse i en sag vedrørende sikkerheden i IT-systemet Mediconnect, som udbydes af EG Digital Welfare ApS (EG). Tilsynet havde indledt sagen af egen drift på baggrund af en henvendelse om sikkerheden i systemet.

Mediconnect bliver bl.a. brugt af kommuner, regioner og forsikringsselskaber til at håndtere følsomme og fortrolige oplysninger om borgere. EG agerer i den sammenhæng som databehandler for IT-systemet Mediconnect.

Datatilsynet lagde på baggrund af det af EG oplyste til grund, at der ikke i Mediconnect er krav om flerfaktor-login for brugerne af databasen, og at passwords gemmes i klartekst i databasen.

Efter en gennemgang af sagen fandt Datatilsynet, at der var grundlag for at udtale kritik af, at EG's behandling af personoplysninger ikke var sket i overensstemmelse med kravet om passende sikkerhed i databeskyttelsesforordningens artikel 32. Tilsynet fandt endvidere grundlag for at meddele EG påbud om at foretage irreversibel kryptering af passwords og om at sikre login til særlige oplysninger.

Afgørelsen fastslår bl.a., at det normalt ikke vil være passende sikkerhed at give adgang til oplysninger af særlige kategorier alene ved indtastning af brugernavn og password, når dette sker over et netværk, som man ikke har kontrol over.

Det er i forlængelse heraf Datatilsynets opfattelse, at en-faktor-login medfører en forhøjet risiko for misbrug af adgange samt risiko for, at adgange deles af flere brugere, sådan at en eventuel logning af adgange til systemet ikke længere er effektiv, idet man ikke kan være sikker på, hvem der reelt har anvendt hvilke adgange. Datatilsynet foreslog i sagen, at adgangen kunne udbygges ud over brugernavn og password. Dette kunne være multifaktor-login, brug af certifikater, tokens eller en PKI-løsning.

Salling Group

Datatilsynet afsluttede i 2022 også en anden sag, som tilsynet blev bekendt med som følge af en anmeldelse af et brud på persondatasikkerheden fra Salling Group.

Det fremgik af sagen, at Salling Group anvender et fælleslogin – Salling Group profil – således at brugernavn og password kan anvendes på alle de tjenester, hvor Salling Group profilen er adgangsgivende, herunder blandt andet Føtex', Bilkas, Nettos, Sallings og Carl Junior hjemmesider.

I 2021 implementerede Salling Group et monitoreringsværktøj til at registrere hændelser og events – herunder login – på koncernens hjemmesider enkeltvis. Ved en menneskelig fejl blev kundernes passwords ikke krypteret, inden de blev lagret i systemets logfil, når kunderne loggede ind på hjemmesiden hjem.foetex.dk. Derved fik op mod 146 interne brugere i Salling Group teknisk adgang til at læse både brugernavne og passwords for et antal kunder, der havde foretaget login på hjemmesiden.

Hvis denne adgang blev udnyttet, ville der kunne skaffes adgang til navn, adresse, mailadresse, telefonnummer og eventuelle maskerede betalingskortoplysninger og købshistorik for et antal af Salling Groups kunder.

Datatilsynet udtalte på den baggrund alvorlig kritik af, at Salling Groups behandling af personoplysninger ikke er sket i overensstemmelse med reglerne om behandlingssikkerhed i databeskyttelsesforordningens artikel 32.

Datatilsynet udtalte i sagen, at personoplysninger i form af passwords altid skal behandles på en måde, der sikrer en tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret adgang og behandling. Passwords skal således til enhver tid opbevares i en irreversibel krypteret form og på en måde, der sikrer, at de ikke er umiddelbart læsbare, og at det ikke er muligt at genskabe passwordet til læsbart format. At opbevare passwords i læsbart format (klartekst) i en logfil, lever ikke op til dette krav. Datatilsynet udtalte i den forbindelse, at det er tilsynets vurdering, at passwords, der kan læses i klartekst, dermed kan gøres til genstand for misbrug, hvorfor risikoen for de registrerede er høj.

Datatilsynet fandt endvidere grundlag for at påbyde Salling Group at underrette de kunder, hvis passwords havde været opbevaret ukrypteret i loggen til monitoreringsværktøjet.

Krisecenters anmodning om personnummer via SMS

Datatilsynet traf i 2022 afgørelse i en sag, hvor børne- og ungekrisecenteret Joannahuset havde anmodet om at modtage en ung persons personnummer via SMS.

Det er Datatilsynets generelle vurdering, at transmission via SMS af fortrolige oplysninger, som for eksempel et personnummer, indebærer en betydelig risiko for de registreredes rettigheder og frihedsrettigheder. Tilsynet besluttede derfor at tage en sag op af egen drift over for krisecenteret for at undersøge sagen nærmere, og tilsynet anmodede i den forbindelse krisecenteret om at besvare en række spørgsmål.

Det fremgik af sagens oplysninger, at krisecenteret fandt det nødvendigt at få verificeret den pågældendes identitet for at kunne tilbyde ham husly. Der var efter sagens oplysninger tale om en akut og

helt særlig situation, hvor der ikke var andre og mere sikre transmissionsløsninger til rådighed, som kunne sikre en tilstrækkeligt hurtig verifikation af vedkommendes identitet.

Datatilsynet vurderede, at der ikke var grundlag for at tilsidesætte krisecenterets vurdering af, at der i den konkrete situation var hensyn til den unges tarv, der måtte veje tungere end hensynet til beskyttelse af personoplysninger, og at den unge person i sagen ville kunne lide et større rettighedstab, hvis den pågældende SMS ikke blev afsendt. Tilsynet fandt derfor ikke anledning til at udtale kritik af krisecenteret.

Datatilsynet bemærkede, at det er tilsynets opfattelse, at krav til databeskyttelsen i særlige tilfælde må vige for andre mere tungtvejende hensyn, herunder eksempelvis hensynet til akut at sikre liv og helbred i forhold til særligt udsatte grupper af mennesker, men at en sådan lempelse af databeskyttelsen skal ske efter en konkret vurdering, og at overvejelserne herom skal være dokumenteret.

Datatilsynet bemærkede i øvrigt, at kravet om passende sikkerhed efter databeskyttelsesforordningens artikel 32 efter tilsynets opfattelse normalt bl.a. vil indebære, at den dataansvarlige skal tilbyde de registrerede en tilstrækkelig sikker transmissionsløsning ved transmission af bl.a. fortrolige oplysninger, når den dataansvarlige indsamler oplysninger fra de registrerede til brug for behandling af en sag eller tjenesteydelse.

Manglende sikkerhed i e-Boks Express

I 2022 afsluttede Datatilsynet en sag, hvor en bruger af e-Boks Express gjorde tilsynet opmærksom på, at det var muligt at tilgå en andens brugers profil ved login på e-Boks Express.

E-Boks Express er en selvbetjeningsportal, hvor virksomheder kan sende beskeder og dokumenter. En fejl i Nets' opsætning af brugervalideringen af NemID medførte, at når en bruger tilgik e-Boks Express ved at logge på med NemID Erhverv/NemID medarbejdersignatur med nøglekort, kunne der blive etableret adgang til andre virksomheders oplysninger og oplysninger om sendte dokumenter i e-Boks Express.

E-Boks gjorde gældende, at NemID anvendes i e-Boks Express for at sikre, at kun de personer, der er autoriseret af afsendervirksomheden, har adgang til e-Boks Express.

Datatilsynet udtalte kritik af, at e-Boks ikke havde levet op til kravet om passende sikkerhedsforanstaltninger, fordi e-Boks ikke havde testet alle relevante brugsscenarier ved login i e-Boks Express.

Datatilsynet bemærkede i den forbindelse, at et login bruges til at identificere brugeren, som anvender it-løsningen – i dette tilfælde e-Boks Express. Efter login skal de rettigheder, som en bruger får afledt, sikre, at adgangen til data er netop det, denne bruger må have adgang til. E-Boks burde således have opdaget ved test, at e-Boks Express gav adgang til andre brugeres data, selv om brugeridentificeringen fejlede.

Afgørelsen illustrerer bl.a., at login – uanset at det er med NemID – ikke beskytter data, hvis rettighederne, brugeren får efter login, ikke er korrekte.

Tilsyn med rettigheds- og adgangsstyring

Datatilsynet afsluttede i 2022 en række tilsyn med 5 udvalgte kommuners rettigheds- og adgangsstyring. Kommunerne var Gladsaxe Kommune, Odsherreds Kommune, Køge Kommune, Gentofte Kommune og Høje Taastrup Kommune.

I sagerne udtalte Datatilsynet, at det er tilsynets opfattelse, at kravet om passende sikkerhed i databeskyttelsesforordningen artikel 32 normalt vil indebære, at der er implementeret foranstaltninger om

tildeling og fratagelse af adgangsrettigheder til systemer, således at kun brugere, der har et arbejdsbetinget behov for at have adgang til oplysningerne, autoriseres hertil.

Det er endvidere Datatilsynets opfattelse, at der ud over en procedure for inddragelse af rettigheder ved stillingsophør, skal være en kontrolprocedure, der effektivt følger op på, om dette også er sket. Denne kontrolprocedure skal være organisatorisk og/eller teknisk forankret, så den ikke ved en menneskelig fejl ikke bliver gennemført.

Endvidere indebærer kravet om passende sikkerhed i databeskyttelsesforordningen artikel 32 efter Datatilsynets opfattelse normalt, at den dataansvarlige løbende kontrollerer, om brugeradgange til systemer er begrænset til de personoplysninger, som er nødvendige og relevante for den pågældende brugers arbejdsbetingede behov, og at rettighederne afspejler rettighedsbegrænsninger i underliggende systemer.

Det er herudover Datatilsynets opfattelse, at kontrollen af adgangsrettigheder normalt som minimum bør bestå af en verifikation af det arbejdsbetingede behov ved tildelingen, en løbende kontrol baseret på verifikation af at dette behov stadig er til stede og en form for auditering heraf. Hvis auditeringen udføres som stikprøvekontroller, skal antallet af udtagne stikprøver stå repræsentativt i forhold til antallet af mulige hændelser og risikoen for de registreredes rettigheder.

I alle 5 tilsyn fandt Datatilsynet grundlag for at udtale kritik af, at kommunerne ikke havde handlet i overensstemmelse med reglerne om behandlingssikkerhed i databeskyttelsesforordningens artikel 32.

Datatilsynet lagde i afgørelsen vedrørende *Gladsaxe Kommune* vægt på, at kommunen ikke havde frataget en brugers adgangsrettigheder til det system, der var genstand for tilsynet, efter medarbejderens fratrædelse, og at kommunen ikke havde foretaget en opfølgning eller kontrol af ophørte medarbejderes rettigheder.

I afgørelsen vedrørende *Odsherred Kommune* lagde Datatilsynet vægt på, at kommunen ikke forud for tilsynet havde sikret sig, at brugernes rettigheder og dermed adgange til personoplysninger i det system, der var genstand for tilsynet, var nødvendige og relevante til de pågældende brugeres arbejdsbetingede behov.

Datatilsynet lagde i afgørelsen vedrørende *Køge Kommune* vægt på, at kommunen ikke havde haft systematiske kontroller f.eks. med faste tidsintervaller eller baseret på stikprøver med brugernes rettigheder i det system, der var genstand for tilsynet, og at kommunen ikke havde ført kontrol med andre brugere end medarbejderes adgange til det pågældende system.

I afgørelsen vedrørende *Gentofte Kommune* lagde Datatilsynet vægt på, at når det gjaldt kommunens rettighedsstyring til e-mailpostkasser, hvortil flere brugere har adgang, typisk kaldet afdelings- og funktionspostkasser, havde kommunen ikke foretaget de fornødne kontroller af, om adgangsrettighederne til disse afdelings- og funktionspostkasser var korrekte, hvilket ikke var i overensstemmelse med reglerne om behandlingssikkerhed. Gentofte Kommune havde ved seneste kvartalsvise stikprøve således kun kontrolleret to postkasser ud af 564.

Tilsynet med *Høje Taastrup Kommune* fokuserede på adgangsrettigheder i kommunens filsystemer. Et filsystem er i denne sammenhæng den stistruktur, kommunen opbevarer data i på deres servere. Tilsynet så på, om der var differentierede rettigheder til de forskellige mapper med oplysninger, og om adgange blev tildelt ud fra arbejdsbetingede behov. I forbindelse med tilsynet udvalgte Datatilsynet en database, hvor der var tildelt adgang for 12 AD-grupper, dvs. 12 grupper af brugere.

Datatilsynet fandt i afgørelsen over for Høje-Taastrup Kommune, at kommunen – ved ikke at have retningslinjer eller objektive kriterier for indmeldelse i AD-grupperne – ikke havde levet op til reglerne om behandlingssikkerhed. Datatilsynet lagde i den forbindelse vægt på, at 410 personer havde AD-adgang til den udvalgte database, og at kommunen ikke kunne dokumentere, at der var foretaget en vurdering af de pågældende medarbejderes arbejdsbetingede behov for adgang til den pågældende database.

Tilsyn med udstedelse af adgangskort

Tilsynet fokuserede på Region Nordjyllands procedurer for udstedelse af adgangskort til de af regionens hospitaler og lokaler, hvor der behandles personoplysninger.

I forbindelse med behandlingen af sagen modtog Datatilsynet bl.a. Region Nordjyllands retningslinjer om tildeling og udstedelse af adgangskort.

Datatilsynet udtalte i sagen, at det er tilsynets opfattelse, at kravet om passende sikkerhed i databeskyttelsesforordningens artikel 32 normalt vil indebære, at det i lokaler, hvor der behandles følsomme oplysninger, herunder helbredsoplysninger, skal sikres, at uvedkommende ikke får adgang.

Datatilsynet fandt, at der ikke var grundlag for at tilsidesætte regionens vurdering af, at de iværksatte procedurer for udstedelse af adgangskort udgør passende sikkerhedsforanstaltninger.

Datatilsynet lagde i den forbindelse vægt på, at Region Nordjylland benytter adgangskontrol til aflåste rum, at regionen har procedurer for udstedelse af adgangskort, og at regionen har yderligere sikkerhedsforanstaltninger for at undgå, at uvedkommende får adgang til personoplysninger på regionens lokationer, f.eks. krav om en personlig bruger til regionens IT-systemer og procedurer for tildeling af adgange til systemerne.

Tilsyn med statslige myndigheders kontrol med databehandlere

Datatilsynet afsluttede i december 2022 en række tilsyn med 6 statslige myndigheders kontrol med databehandlere, som blev indledt i efteråret 2021. De statslige myndigheder var Beskæftigelsesministeriets departement, Forsvarsministeriets Personalestyrelse, Hjemrejsestyrelsen, Skatteforvaltningen, Styrelsen for International Rekruttering og Integration og Sundhedsdatastyrelsen.

I 5 af tilsynene fandt Datatilsynet ikke grundlag for at tilsidesætte de dataansvarliges vurdering af, at tilsynet med deres databehandlere var sket i overensstemmelse med databeskyttelsesreglerne.

Datatilsynet lagde vægt på, at de dataansvarlige havde taget stilling til de risici, der var for de registrerede ved behandlingen hos databehandleren og på den baggrund havde vurderet i hvilken grad, der skulle føres tilsyn med databehandleren – og at der i praksis var gennemført tilsyn i overensstemmelse hermed.

Datatilsynet udtalte bl.a., at dataansvarlige skal være i stand til at påvise, at databehandleren giver tilstrækkelige garantier for implementering af tekniske og organisatoriske foranstaltninger, der opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af de registreredes rettigheder. Denne påvisning skal kunne foretages i hele behandlingsforløbet over tid, hvilket bl.a. kan ske ved kontroller.

I tilsynet med Styrelsen for International Rekruttering og Integration fandt Datatilsynet dog bl.a. anledning til at udtale kritik af, at styrelsen ikke havde gennemført det planlagte årlige tilsyn med en af sine databehandlere i 2021.

Anmeldelser af brud på persondatasikkerheden

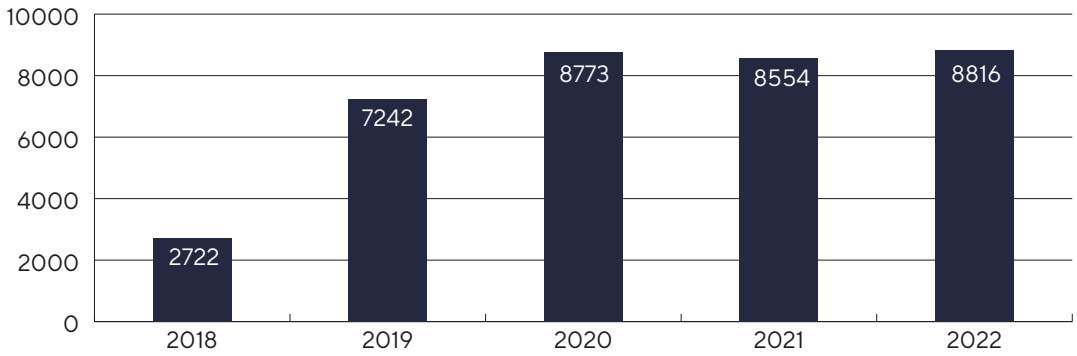
Datatilsynet modtager fortsat en stor mængde anmeldelser af brud på persondatasikkerheden. I 2022 blev der anmeldt **8.816** brud på persondatasikkerheden, hvilket er 261 flere anmeldelser end i 2021.

For at understøtte de dataansvarlige i at anmelde brud på persondatasikkerheden korrekt til Datatilsynet, gennemførte tilsynet i 2022 en række vejledningsinitiativer. Initiativerne bestod bl.a. i fysiske oplæg om "Den gode anmeldelse", hvor Datatilsynet tog ud i landet for at fortælle om og vejlede dataansvarlige i, hvordan de mest hensigtsmæssigt anmelder brud på persondatasikkerheden til tilsynet. I den forbindelse foretog Datatilsynet også en række ændringer i den blanket, som dataansvarlige bruger til at anmelde brud på persondatasikkerheden til tilsynet, så den blev mere brugervenlig og målrettet. Herudover opstartede Datatilsynet en række tilsynstiltag, der havde fokus på dataansvarliges anmeldelser af brud på persondatasikkerheden og underretning af berørte registrerede.

I 2023 forventer Datatilsynet at udsende nyt vejledningsmateriale om håndtering af brud på persondatasikkerheden, som er baseret på mange af de praktiske erfaringer, tilsynet gennem behandling af anmeldelser og konkrete sager om brud på persondatasikkerheden har gjort sig siden 25. maj 2018, hvor anmeldelsespligten blev indført.

De anmeldte brud på persondatasikkerheden i 2022 fordeler sig på en række forskellige kategorier. Som i de foregående år er det oplysninger, der sendes forkert, der udgør den største andel af de anmeldte brud på persondatasikkerheden. I 2022 var det således 5066 ud af de anmeldte brud, der skyldtes fejlagtig fremsendelse af oplysninger – enten fordi oplysningerne utilsigtet sendes til en forkert modtager, eller fordi det utilsigtet er de forkerte oplysninger, der bliver sendt til den rigtige modtager. Af denne type anmeldelser af brud udgør langt størstedelen – 3945 – anmeldelser, hvor oplysninger er sendt utilsigtet til en forkert modtager.

Anmeldelser af brud på persondatasikkerheden



Manglende overholdelse af princippet om databeskyttelse gennem design

Datatilsynet traf i 2022 afgørelse i en sag, som handlede om, at LB Forsikring A/S havde designet selskabets arkiveringssystem med en indstilling, der gjorde, at e-mails i forsikringsselskabets bilskadeafdeling i en periode blev tilknyttet en skadessag med læserettigheder alt efter, hvilket e-maildomæne det var afsendt fra.

Det betød i praksis, at al dokumentation, der var identificeret med samme skadesnummer – og som var afsendt fra flere udbredte mailudbydere – blev synlig på kundens "Min side". Dokumenterne kunne bl.a. være fra modparter, vidner og automekanikere og indeholdt personoplysninger som kontaktinformationer, vidneerklæringer, betalingsoplysninger – og i mindst ét tilfælde et personnummer.

LB Forsikring havde før implementeringen af arkiveringssystemet i 2019 udarbejdet en implementeringsplan, der indeholdt adskillige tests. Testene skulle bl.a. sikre, at dokumenterne blev tildelt korrekt dokument-ID og blev placeret korrekt, men den pågældende indstilling blev ikke identificeret i testforløbet.

Datatilsynet udtalte i sagen, at det – ud over brugen af alle de anerkendte testformer – allerede fra udviklingen af systemets forretningsprocesser og design påhviler den dataansvarlige at sikre en effektiv implementering af databeskyttelsesprincipperne ved at indbygge dette i systemunderstøttelsen, så det giver de fornødne garantier i behandlingen af personoplysninger og opfylder kravene i databeskyttelses-forordningen.

Datatilsynet udtalte endvidere, at det ikke er i overensstemmelse med det aktuelle tekniske niveau, at et maildomæne isoleret set har betydning for, hvilke dokumenter der gives adgang til, når man udvikler en portalløsning som LB Forsikrings arkiveringssystem, hvor der gives adgang til opbevarede dokumenter med personoplysninger.

Herudover vil det være en del af det aktuelle tekniske niveau, at den dataansvarlige indbygger opfølgende kontroller, der sikrer, at en sådan automatisk proces, alene giver den korrekte adgang.

På den baggrund fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at LB Forsikring A/S' behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1, og artikel 25, stk. 1.

Hackere fik adgang til betalingsoplysninger

Datatilsynet har i 2022 i to sager udtalt alvor kritik af, at manglende sikkerhedsforanstaltninger i forbindelse med webshops medførte, at hackere kunne få adgang til kunders betalingsoplysninger.

Designbysi

Virksomheden Designbysi var blevet udsat for et hackerangreb, hvor uvedkommende havde indsat et uautoriseret JavaScript på Designbysis webshop for at indsamle kunders kortoplysninger. JavaScriptet medførte, at kunder i forbindelse med deres køb fik en fejlmeddelelse, hvorefter de blev anmodet om at indtaste deres kortoplysninger endnu en gang.

Forud for hændelsen havde Designbysi ikke indført multifaktor login for de medarbejdere hos Designbysi, der havde adgang til at ændre i betalingsscriptet (administrative rettigheder).

Datatilsynet udtalte, at det er tilsynets opfattelse, at kravet om passende sikkerhed i forordningens artikel 32 normalt vil indebære, at loginoplysninger, der giver adgang til betalingsoplysninger eller mulighed for at ændre i betalingsscript, skal sikres mod, at hackere kan få adgang til oplysningerne alene med et franarret brugernavn og adgangskode, f.eks. fra et phising-angreb. Det er således Datatilsynets vurdering, at det er en passende sikkerhedsforanstaltning at implementere multifaktorgodkendelse på sådanne loginoplysninger.

Datatilsynet anførte endvidere, at en adgang til betalingsmoduler og ændringsrettigheder til domænet generelt bør begrænses til en særligt navngivet konto, der alene bruges til dette formål, ligesom der skal være et passende komplekst password samt multifaktor login. Dette er for at mindske muligheden for, at de konti medarbejdere bruger til dagligt ved et angreb på deres daglige kommunikation, kompromitterer betalingsservicen og roddomænets adgangssikkerhed.

Sports Connection ApS

Den anden sag drejede sig om et lignende tilfælde, hvor virksomheden Sports Connection ApS var udsat for et hackerangreb, hvor uvedkommende injicerede skadelig programkode på virksomhedens webshop for at indsamle kunders betalingsoplysninger. Forud for hændelsen havde virksomheden ikke sikkerhedspatchet e-handelsprogrammet til seneste version.

Datatilsynet udtalte, at det er tilsynets opfattelse, at kravet om passende sikkerhed indebærer, at den dataansvarlige skal sikre, at kunder ved brug af den dataansvarliges webshop ikke utilsigtet videregiver oplysninger til uvedkommende, f.eks. ved at sikre, at kunder ikke bliver videresendt til en betalingsside, hvor kundernes betalingsoplysninger bliver opsnappet af uvedkommende.

Datatilsynet udtalte endvidere mere generelt, at der ved webshops og betalingsløsninger, der stilles til rådighed via åbne tilgængelige hjemmesider, skal være procedurer og kontroller, der sikrer, at administrative brugerkonti holdes separat fra enkeltbrugerkonti, og at disse generelt skal sikres ved brug af multifaktorautentifisering. Herudover skal der i videst muligt omfang benyttes forskellige brugernavne og kendeord til de moduler og dele, løsningen består af.

Herudover bemærkede Datatilsynet, at det er et kendt risikoscenarie, at de hyppigt anvendte e-handelsplat-forme og deres add-on produkter bliver forsøgt kompromitteret ved indbyggede svagheder. Derfor er det essentielt, at der patches, lige så snart leverandøren udgiver en sikkerhedspatch. Det gælder både de patches, der udbedrer specifikke trusler, men også dem der blot angiver at udbedre generelle sårbarheder.

Det er i den forbindelse Datatilsynets opfattelse, at den dataansvarlige som led i udvikling og tilpasning af it-løsninger til behandling af personoplysninger skal sikre, at it-systemer løbende opdateres og kontrolleres med henblik på at identificere forhold, som kan føre til hændelig eller ulovlig tilintetgørelse, tab, ændring uautoriseret videregivelse af eller adgang til personoplysninger.

Sports Connection ApS havde endvidere generelt ikke kunnet påvise overholdelse af forordningen, da virksomheden ikke kunne dokumentere, hvornår systemet blev patchet, idet der ikke har kunnet fremskaffes en logfil over løbende opdateringer. Ved ikke at kunne påvise dette fandt Datatilsynet, at Sports Connection ApS ikke havde levet op til kravet om, at den dataansvarlige skal kunne påvise en passende sikkerhed ved behandlingen af personoplysninger, jf. databeskyttelsesforordningens artikel 24, stk. 1, jf. artikel 32, stk. 1.

Serie af utilsigtede videregivelser af personoplysninger

Datatilsynet udtalte i 2022 alvorlig kritik af Familieretshusets for ikke at have levet op til kravet om passende sikkerhed i forbindelse med utilsigtede videregivelser af personoplysninger, herunder beskyttede navne- og adresseoplysninger.

Der var tale om en sag, som tilsynet havde taget op på eget initiativ. Baggrunden for sagen var, at Familieretshuset i perioden fra den 27. maj 2021 til den 16. august 2022 havde anmeldt 37 brud på persondatasikkerheden, som omhandlede uberettiget videregivelse af oplysninger om bl.a. den ene parts beskyttede adresse til den anden part i en sag hos myndigheden. I de fleste tilfælde havde personerne adressebeskyttelse for at undgå, at den anden part skulle få kendskab til adressen.

Datatilsynet havde også i en afgørelse fra 2021 udtalt alvorlig kritik af Familieretshuset i forbindelse med en række utilsigtede videregivelser af bl.a. beskyttede navne- og adresseoplysninger.

Datatilsynet konstaterede i sagen, at Familieretshuset – efter tilsynets afgørelse i 2021 – havde gennemført betydelige foranstaltninger for at undgå utilsigtet videregivelse af beskyttede navne- og adresseoplysninger.

Datatilsynet fandt imidlertid også, at Familieretshuset ikke havde levet op til kravet om passende sikkerhed, idet Familieretshuset, på trods af at have konstateret og anmeldt flere lignende brud på persondatasikkerheden, ikke havde genovervejet de eksisterende foranstaltninger med henblik på at forhindre fremtidige brud af samme type.

Tilsynet lagde særligt vægt på, at Familieretshuset ikke i tilstrækkeligt omfang havde haft de fornødne procedurer for regelmæssig efterprøvning, vurdering og evaluering af effektiviteten af de allerede etablerede foranstaltninger. Datatilsynet udtalte i den forbindelse, at nye og gentagne brud på persondatasikkerheden bør få den dataansvarlige til at reflektere over allerede foretagne risikovurderinger, og at brudtyper, der henføres til personlige fejl eller enkeltstående episoder, ved gentagelse bør give anledning til indførelse af yderligere effektive kontrolforanstaltninger eller teknisk understøttelse, der minimerer de nu kendte og aktualiserede risici.

Ved valg af reaktion lagde Datatilsynet i skærpende retning vægt på, at det kan være forbundet med store konsekvenser for de registrerede, hvis deres beskyttede adresse eller andet opholdssted, som f.eks. navnet på et krisecenter, utilsigtet bliver videregivet til den person, de prøver at skjule sig for.

Datatilsynet fandt endvidere, at der var grundlag for at meddele Familieretshuset påbud om at foretage en fornyet risikovurdering på baggrund af de i sagen omhandlende 37 brud på persondatasikkerheden.

CRM-system opsat i strid med princippet om rigtighed og kravet om passende sikkerhed

I 2022 udtalte Datatilsynet også alvorlig kritik af 3F Østfyn for ikke at have levet op til princippet om rigtighed og kravet om passende sikkerhed ved utilsigtet at videregive oplysninger om et medlem til medlemmets tidligere og voldelige samlever.

3F Østfyn anmeldte et brud på persondatasikkerheden til Datatilsynet. Det fremgik af anmeldelsen og de supplerende oplysninger i sagen, at 3F Østfyn ajourførte medlemmernes navne og adresser på baggrund af adresseoplysninger fra CPR-registeret.

I tilfælde, hvor et medlem vælger adressebeskyttelse i CPR-registret, modtager 3F ikke længere oplysninger om bl.a. medlemmets adresse, og adressefeltet låses op i 3F's CRM-system sådan, at medlemmets oplysninger skal vedligeholdes manuelt. I sådanne tilfælde vil det være den sidst kendte adresse, der står i adressefeltet, indtil en opdatering af adressefeltet gennemføres manuelt og lokalt.

I den konkrete sag kontaktede et medlem 3F Østfyn for at få opdateret sine navne- og adresseoplysninger, men ved en menneskelig fejl blev kun navnet opdateret. I forbindelse med udsendelse af Fagbladet 3F blev medlemmets navneændring anført på bladet, men det blev sendt til medlemmets oprindelige adresse, hvor den tidligere samlever fortsat var bosiddende. Derved fik den tidligere samlever kendskab til medlemmets nye navn.

Datatilsynet fandt, at 3F Østfyns system generelt var sat op på en måde, så det potentielt ville behandle forkerte oplysninger, og at 3F Østfyn ikke havde taget ethvert rimeligt skridt til at sikre, at oplysningerne blev slettet eller berigtiget. 3F Østfyn behandlede derfor personoplysninger i strid med princippet om rigtighed.

Datatilsynet konstaterede yderligere, at 3F Østfyn ikke havde truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passede til den konkrete risiko for de registreredes rettigheder, særligt da der ikke var opsat procedurer eller systemunderstøttelse for at sikre, at oplysningerne ajourførtes.

Datatilsynet lagde ved vurderingen bl.a. vægt på, at princippet om rigtighed forpligter til, at systemer ikke må sættes op på en måde, der medvirker til at skabe og behandle forkerte eller ufuldstændige data. Herudover er det væsentligt, at den dataansvarlige identificerer de risici, den konkrete behandling udgør for de registrerede. Det er ikke tilstrækkeligt blot at fokusere på generiske risikoscenarier og indføre sikkerhedsforanstaltninger, der beskytter de registrerede mod disse risici.

Datatilsynet angav i øvrigt i sagen en række mulige forslag til tekniske og organisatoriske foranstaltninger, som kunne anses for relevante i den konkrete sag. Datatilsynet anførte, at CRM-systemet f.eks. kunne opsættes med en automatisk reaktion (advarsel), som gør medarbejderen opmærksom på, at der nu er navne- og adressebeskyttelse, efter adressefeltet er låst op i CRM-systemet, og at den konkrete medarbejder skal kontrollere, om oplysningerne er korrekte, inden de kan bruges – f.eks. til at sende materiale ud (spærring af alle automatiske behandlinger af den data, der er registreret en ændring i). Denne tekniske foranstaltning bør understøttes af særlige processer og retningslinjer for vedligeholdelse og administration af feltværdierne, når der er tale om et manuelt vedligeholdt felt.

Utilstrækkelig sikker fjernelse af oplysninger fra materiale i aktindsigtssag

Datatilsynet udtalte i 2022 alvorlig kritik af Finanstilsynet for ikke at have levet op til kravet om passende sikkerhed, idet Finanstilsynet havde videregivet oplysninger om whistleblowere til en journalist i forbindelse med en anmodning om aktindsigt.

Den utilsigtede videregivelse skete, fordi Finanstilsynet ikke på en tilstrækkelig sikker måde havde fjernet personoplysninger fra det materiale, der var givet aktindsigt i. Finanstilsynet havde således overstreget personoplysninger i de udleverede pdf-dokumenter for at undtage disse fra materialet, men oplysningerne kunne aflæses ved at "holde musemarkøren" på overstregede passager.

Finanstilsynet var ikke opmærksom på, at det er nødvendigt at slette de skjulte oplysninger, som befinder sig bag det viste dokument (metadata mv.), for at sikre, at de ikke længere vil kunne findes.

Ved vurderingen af sagen lagde Datatilsynet bl.a. vægt på, at kravet om passende sikkerhed indebærer, at den dataansvarlige skal etablere foranstaltninger, der sikrer, at materiale, der videregives, ikke indeholder personoplysninger, som skulle have været anonymiseret.

Datatilsynet lagde derudover særligt vægt på, at risikoen for den registreredes rettigheder generelt må anses for højere, når oplysningerne stammer fra en whistleblowerordning, ligesom Datatilsynet konstaterede, at det er en alment kendt del af funktionaliteten i programmer, der teknisk bliver brugt til overstregning, at metadataoplysninger eller underliggende lag af oplysninger kan findes efter overstregning.

Kuratorer fik uautoriseret adgang til digitale postkasser på grund af en menneskelig fejl

Datatilsynet udtalte i 2022 kritik af Digitaliseringsstyrelsen for ikke at have levet op til kravet om passende sikkerhed i forbindelse med, at der utilsigtet blev givet adgang til forkerte digitale postkasser.

Digitaliseringsstyrelsen havde ved en fejl givet 26 kuratorer adgang til forkerte virksomheders digitale postkasser. Fejlen skyldtes formentlig, at linjerne med cvr-numre var blevet forskudt på den liste, styrelsen havde sendt til deres leverandør e-Boks.

Under sagens behandling gjorde Digitaliseringsstyrelsen gældende, at styrelsen ikke tidligere havde oplevet, at der var sket fejl i udarbejdelsen af den pågældende liste. Efter hændelsen indførte styrelsen en procedure, hvor en ekstra medarbejder gennemgår listerne for fejl, inden de sendes til leverandøren, for at minimere risikoen for fejl.

Datatilsynet anførte i afgørelsen, at det er tilsynets opfattelse, at kravet om passende sikkerhed normalt vil indebære, at der i systemer med et stort antal fortrolige oplysninger om et stort antal brugere skal stilles højere krav til den dataansvarliges omhyggelighed ved sikring af, at der ikke sker uautoriseret adgang til personoplysninger. Tilsynet anførte ligeledes, at der ved adgang til data i sådanne systemer stilles større krav til sikring imod, at en enkelt menneskelig fejl kan resultere i større brud på persondatasikkerheden.

Datatilsynet fandt, at Digitaliseringsstyrelsen ikke havde levet op til reglerne om behandlingssikkerhed ved ikke at have indført foranstaltninger til at sikre, at listerne var korrekte og ved alene at have baseret sikkerheden på, at der ikke tidligere var sket menneskelige fejl.

Datatilsynet lagde ved valg af reaktion i skærpende retning vægt på, at Digitaliseringsstyrelsen har oplevet lignende fejl før. Det er således ikke nok at basere sin sikkerhed på, at der ikke tidligere er sket menneskelige fejl, da det er alment kendt, at menneskelige fejl sker, hvorfor sikkerhed ikke alene kan baseres på en tiltro til, at mennesker ikke begår fejl.

Utilstrækkelig test af softwareændringer

Datatilsynet har i 2022 i en række sager udtalt kritik af, at der ikke er levet op til kravet om passende sikkerhed som følge af utilstrækkelige test af softwareændringer. Datatilsynet har i flere af sagerne endvidere taget stilling til, om ansvaret påhvilede den dataansvarlige eller databehandleren, herunder når der er tale om integrerede systemer.

Utilsigtet adgang til oplysninger om børn

Datatilsynet traf afgørelse i en sag, hvor tilsynet på baggrund af anmeldelser om brud på persondatasikkerheden fra en række kommuner startede en sag af egen drift over for kommunernes databehandler KMD.

Bruddet bestod i, at der utilsigtet var sket overførsel af oplysninger om plejeforældre til AULA fra systemer, som KMD drev som databehandler for kommunerne. Det medførte, at plejeforældre uberettiget havde haft adgang til AULA og dermed til oplysninger om bl.a. plejebørn. Årsagen til bruddet var, at en ny funktionalitet i et system, som KMD var databehandler for, ikke var blevet testet tilstrækkeligt, herunder hvordan funktionaliteten fungerede sammen med f.eks. AULA, som KMD ikke er databehandler for.

KMD anførte, at årsagen til bruddet ikke kunne opdages af KMD ved test af de systemer, som KMD var ansvarlig for, idet fejlen kun kunne opdages ved test i modtagersystemet AULA.

KOMBIT, der er databehandler for AULA, anførte, at deres underdatabehandler hjælper med at teste ændringer på AULA's testsystemer, hvis andre leverandører beder om det.

Datatilsynet lagde på baggrund af sagens oplysninger til grund, at det havde været muligt for KMD at foretage test af den nye funktionalitets sammenspil med AULA, herunder ved selv at kunne foretage test i AULA.

Datatilsynet udtalte i sagen, at det er tilsynets opfattelse, at kravet om passende sikkerhed, jf. databeskyttelsesforordningens artikel 32, normalt vil indebære, at når der udvikles en ny funktionalitet til it-systemer, der skal behandle personoplysninger, skal ændringerne ske efter aftalte principper, hvor der overvejes mulige konsekvenser ved ændringen og planlægges test, som kan verificere, at sikkerhedskrav fortsat er opfyldt, efter ændringen er gennemført.

For så vidt angår systemer, som databehandleren ikke selv er ansvarlig for, men hvor databehandleren er ansvarlig for væsentlige input i form af personoplysninger, er det Datatilsynets opfattelse, at kravet om passende sikkerhed normalt vil indebære, at databehandleren skal skabe det fornødne overblik over egen it-arkitektur og it-miljø, herunder de systemer, som er integreret med andre systemer ved at levere eller modtage data, og hvor tab af integritet af personoplysninger vil medføre en betydelig risiko for de registreredes rettigheder, og sikre kortlægning af integrationerne og dertilhørende afhængigheder.

Som følge af ovenstående, påhviler der databehandleren en pligt til at melde kodeændringer i integrerede systemer ud til relevante dataansvarlige og/eller databehandlere for de integrerede eksterne systemer, inden de går i produktion. Disse krav skal sikre, at eksterne dataansvarlige og/eller databehandlere er rettidigt informeret om de planlagte ændringer og kan foretage hensigtsmæssige test af integritet af personoplysninger, som udveksles mellem de integrerede systemer.

Datatilsynet fandt på den baggrund, at ved ikke at have udført passende tests af den nye funktion havde KMD ikke truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passede til de risici, der var ved KMD's behandling af personoplysninger, jf. databeskyttelsesforordningens artikel 32, stk. 1. Datatilsynet udtalte i den forbindelse alvorlig kritik af KMD.

Databehandler ansvarlig for test af softwareændring foretaget af tredjepart

Datatilsynet udtalte i 2022 alvorlig kritik af Kombit i en sag, hvor 30 kommuner i slutningen af 2019 og starten af 2020 havde anmeldt et brud på persondatasikkerheden til tilsynet på grund af en systemfejl i Aula.

Fejlen i Aula indebar, at det fra den 24. november til den 20. december 2019 var muligt for en bruger A at tilgå en anden bruger B's sikre filer i Aula, hvis bruger B ikke var logget ud af computeren, og bruger A loggede ind med eget NemID. Sikre filer er et område i Aula med følsomme personoplysninger, der kræver ekstra login. Fejlen skyldtes en programmeringsfejl hos Netcompany i forbindelse med udviklingen af en ændring til loginløsningen i Aula.

Datatilsynet udtalte i sagen, at det er tilsynets opfattelse, at kravet om passende sikkerhed i forordningens artikel 32 normalt vil indebære, at alle sandsynlige fejlscenarier bør testes i forbindelse med udviklingen af og ændring af software, hvor der behandles personoplysninger.

Datatilsynet fandt, at Kombit ikke havde levet op til reglerne om behandlingssikkerhed, da Kombit ikke havde sikret, at der blev foretaget tilstrækkelig test af Aula i forbindelse med ændringen af koden i Aula.

Datatilsynet lagde vægt på, at en fejl i udviklingen af løsningen medførte, at der ikke var korrekt styring af adgangsrettigheder i Aula. Endvidere lagte tilsynet vægt på, at Netcompany og Kombit ikke kunne blive enige om, hvilke tests der kunne forventes udført i forbindelse med udviklingsprojektet, og at de ikke kunne blive enige om, hvorvidt Netcompany agerede som underdatabehandler eller ej.

Datatilsynet udtalte i sagen, at det er tilsynets opfattelse, at det i instruksen fra den dataansvarlige skal stå klart, hvorledes en sådan uenighed skal håndteres. Datatilsynet udtalte videre, at det til tilsynets opfattelse, at ingen underdatabehandler på egen hånd kan træffe beslutninger om, hvilken sikkerhed der er fornøden, når de ændringer, der skal udføres, reelt berører behandlinger, der alene sker under den dataansvarliges ansvar og instruks, og dette ikke entydigt kan udledes af den dataansvarliges instruks til databehandleren.

Kodeændringer i Sundhedsplatformen gav utilsigtede ændringer i det Fælles Medicinkort

Datatilsynet behandlede i 2022 flere sager, hvor der var sket brud på persondatasikkerheden som følge af utilsigtede ændringer i det Fælles Medicin Kort (FMK).

Sundhedsdatastyrelsen anmeldte to brud på persondatasikkerheden i FMK til Datatilsynet. Bruddene opstod ved, at kodeændringer i Sundhedsplatformen (SP), som Region Hovedstaden er dataansvarlig for, medførte utilsigtede ændringer i FMK, som Sundhedsdatastyrelsen er dataansvarlig for. Baggrunden for bruddene var, at integrationerne mellem FMK og SP muliggør, at en opdatering i SP kan påvirke integriteten af visningen af oplysninger i FMK.

I august 2020 påvirkede bruddet 4.223 medicinordinationer for 2.310 patienter, og i juli 2021 påvirkede bruddet 1.311 lægemiddelordinationer fordelt på 1.149 patienter fra Region Hovedstaden og Region Sjælland.

Datatilsynet udtalte i sagen, at Region Hovedstaden ikke havde udarbejdet kvalificerede og relevante testscenarier med henblik på bedre at kunne identificere afhængigheder til andre it-systemer, ligesom regionen ikke havde gennemført nødvendige test, inden ændringerne blev sat i produktion, og Region Hovedstaden havde endvidere undladt at informere Sundhedsdatastyrelsen om persondatasikkerheds-bruddene, da hændelserne blev konstateret.

På den baggrund fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at Region Hovedstaden ikke havde levet op til kravet om passende sikkerhed i forbindelse med utilsigtede ændringer i FMK.

Datatilsynet fandt endvidere grundlag for at meddele Region Hovedstaden påbud om at udarbejde og indføre en proces, der sikrer, at ingen ændringer i SP's funktionalitet eller datagrundlag gennemføres og sættes i drift, før det er sikret, at der ikke ved kendte integrationer med andre systemer skabes urigtige informationer i disse. Påbuddet omfattede ikke kun integrationer med FMK, men alle it-systemer, der er integreret med SP, herunder også it-systemer som har andre dataansvarlige.

Datatilsynet udstedte endvidere en advarsel til Region Hovedstaden om, at det sandsynligvis vil være i strid med databeskyttelsesforordningen at idriftsætte systemændringer i SP, hvor der forekommer dataintegration med andre systemer, uden at foretage tests af dataintegritet.

Datatilsynet udtalte efterfølgende i juli 2022 alvorlig kritik af, at Sundhedsdatastyrelsen ikke havde levet op til kravet om passende sikkerhed i forbindelse med de ovenfor nævnte utilsigtede ændringer i FMK.

Datatilsynet anførte i sagen, at det er tilsynets opfattelse, at kravet om passende sikkerhed i forordningens artikel 32 indebærer, at Sundhedsdatastyrelsen som udgangspunkt bør teste alle sandsynlige fejlscenarier i forbindelse med udvikling og ændring af software i FMK. I tilfælde, hvor en tredjepart som Region Hovedstaden kan lave ændringer, er Sundhedsdatastyrelsen som dataansvarlig for FMK også ansvarlig for, at disse ændringer bliver testet.

Da det ikke skete i det konkrete tilfælde, havde Sundhedsdatastyrelsen efter Datatilsynets opfattelse ikke levet op til kravet om passende sikkerhed.

Datatilsynet fandt, at det var en skærpende omstændighed, at Sundhedsdatastyrelsen før havde oplevet lignende fejl, og tilsynet lagde ved afgørelsen endvidere vægt på, at styrelsen overskred fristen på 72 timer for at anmelde sikkerhedsbruddet.

I forbindelse med offentliggørelse af afgørelsen på Datatilsynets hjemmeside bemærkede tilsynet endvidere mere generelt, at i sager, hvor flere aktører udveksler data i servicebaseret arkitektur, ser Datatilsynet ofte konsekvenser i andre systemer, end der, hvor ændringen er sket. På den baggrund understregede Datatilsynet, at hver dataansvarlig er forpligtet til for sine egen systemer at fastsætte fornødne retningslinjer og procedurer for, hvordan ændringer i kildesystemer, som andre er dataansvarlige for, skal kunne få gennemslagskraft. Særligt skal der være procedurer for servicevinduer, change management, designkrav, test af funktionalitet og dataintegritet.

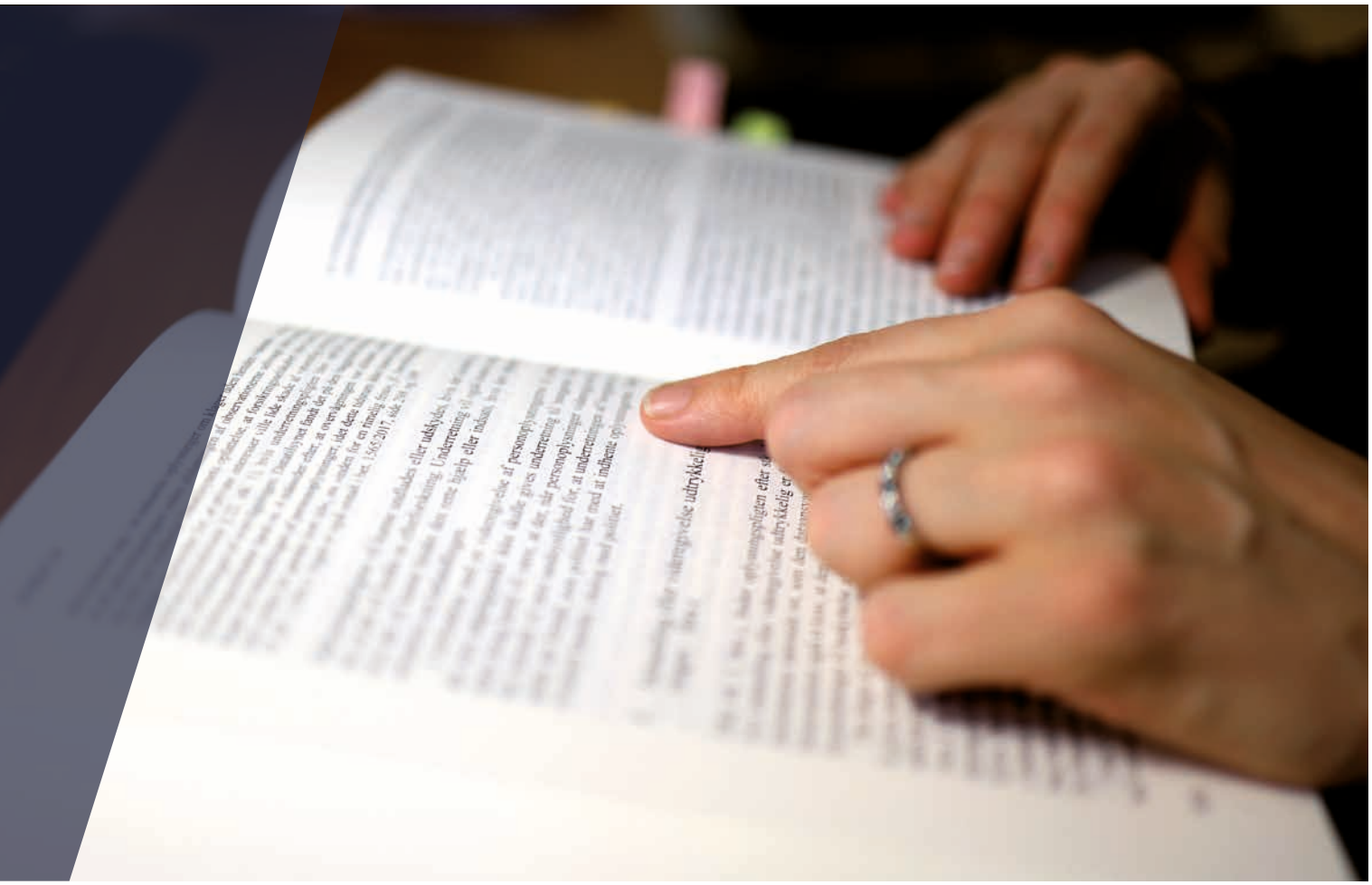
Utilstrækkelige testning af softwareopdatering i HR-system

Datatilsynet udtalte i 2022 alvorlig kritik af Syddansk Universitet i forbindelse med, at rettighedsstyringen i universitets HR-system blev nulstillet. Dette betød, at alle 7011 ansatte på universitetet havde potentiel adgang til at se ansøgninger fra i alt 471 ansøgere. Ud af disse havde ca. 400 ansatte et arbejdsbetinget behov for at kunne tilgå personoplysninger i HR-systemer.

Rettighedsstyringen var indstillet således, at specifikke ansatte kunne få tildelt en rolle, der gav adgang til ansøgningerne. Den utilsigtede nulstilling skete på baggrund af en softwareopdatering, som Syddansk Universitet ikke havde testet tilstrækkeligt, inden den blev implementeret i produktionssystemet. Herudover havde universitetet ikke ført log på adgangen til ansøgningsmaterialet og kunne derfor ikke identificere, hvad der var blevet tilgået.

Syddansk Universitet oplyste i sagen, at det ikke havde haft kendskab til, at opdateringen ville medføre en ændring i rollestyringen og derfor ikke havde haft mulighed for at iagttage den normale praksis med 14 dages test på et testsystem.

Datatilsynet fastslog imidlertid, at dataansvarlige som led i udviklingen og tilpasningen af it-løsninger til behandling af personoplysninger skal teste en løsning med henblik på at kunne identificere og vurdere forhold, der f.eks. kunne have ført til ændring eller nulstilling af tidligere valgte indstillinger. Dette er særligt væsentligt, når der er tale om en grundlæggende funktion som rettighedsstyring. Dette ansvar bortfalder ikke, blot fordi softwareleverandøren ikke fyldestgørende har oplyst om opdateringens omfang.



Tilladelser mv.

Visse behandlinger kræver, at den dataansvarlige indhenter Datatilsynets tilladelse, før behandlingen iværksættes.

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 et eksempel på en af de tilladelsessager, som Datatilsynet har behandlet i 2022

Tilladelse til at oprette advarselsregister over lejere

Privous ApS ansøgte om Datatilsynets tilladelse til førelse af et advarselsregister over lejere, som havde misligholdt lejemål eller -aftale.

Efter ansøgningen havde været forelagt Datarådet, meddelte Datatilsynet i 2022 Privous ApS, at der ikke kunne gives tilladelse til, at lejere blev registreret i advarselsregistret som følge af, et lejemål var ophævet efter lejelovens § 93, stk. 1, litra i (og den tilsvarende bestemmelse i erhvervslejelovens § 69, stk. 1, nr. 8), og lejelovens § 93, stk. 1, litra j, fordi oplysninger om strafbare forhold ikke kan indgå i et advarselsregister.

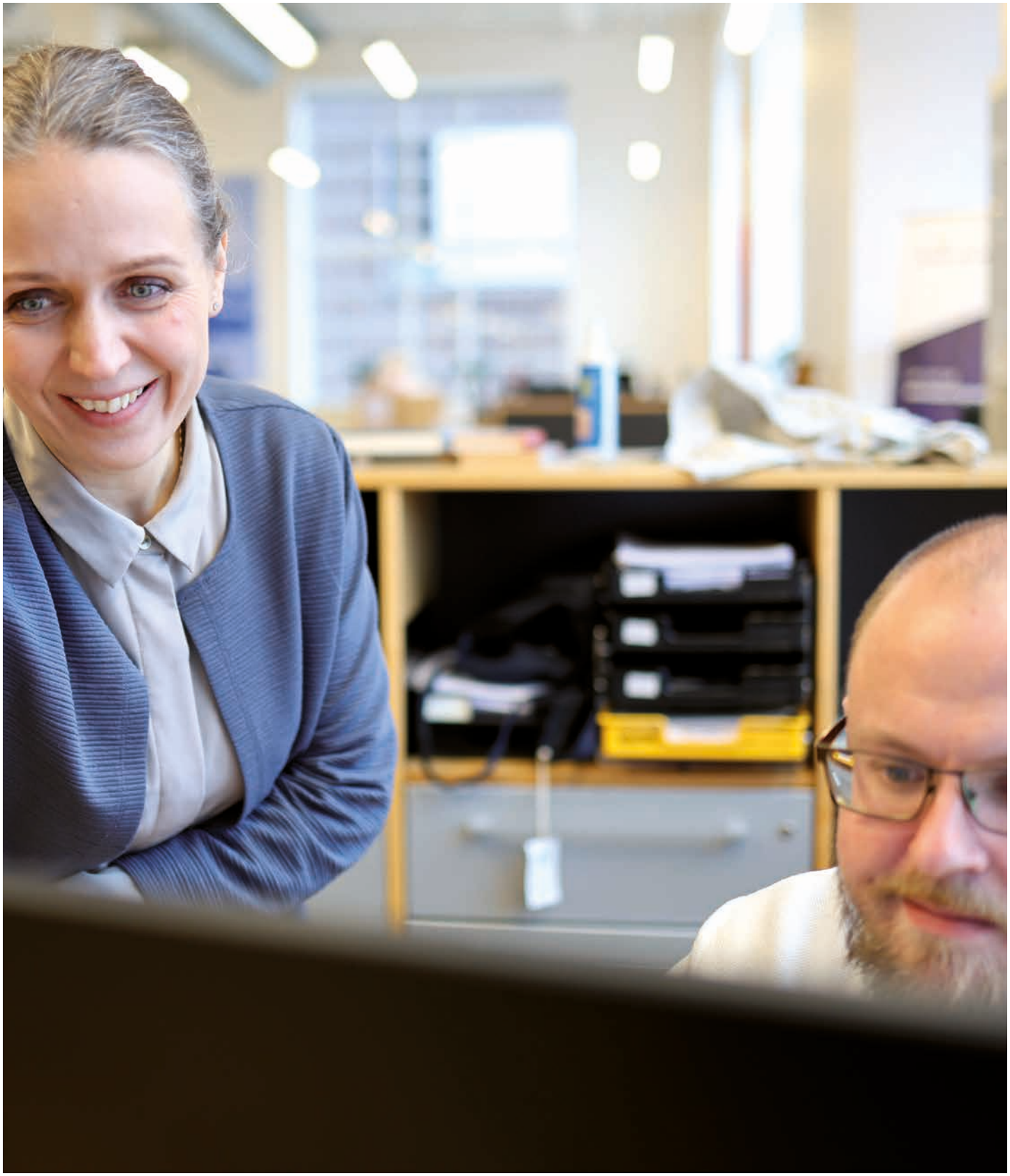
Datatilsynet fandt endvidere, at Privous ApS ikke kunne registrere og videregive oplysninger om personnummer i advarselsregistret inden for rammerne af databeskyttelseslovens § 11, stk. 2, nr. 3.

Herudover fandt Datatilsynet, at optagelse i registret på baggrund af lejelovens § 93 og den næsten tilsvarende bestemmelse i erhvervslejelovens § 69 i flere tilfælde ville indebære subjektive vurderinger. Privous ApS havde i forbindelse med sagens behandling selv peget på, at optagelse i registret på baggrund af en ophævelse efter lejelovens § 93 derfor skulle suppleres med betingelse om, at ophævelsen enten var stadfæstet ved dom eller ved, at lejeren havde accepteret ophævelsen ved fraflytning. Datatilsynet fandt, at den omstændighed, at en lejer har valgt at fraflytte sit lejemål, ikke nødvendigvis er ensbetydende med, at lejeren er enig i præmissen for ophævelsen, og at en fraflytning derfor ikke kan tages som udtryk for en erkendelse. Optagelse i registret på baggrund af lejelovens § 93 eller erhvervslejelovens § 69 skulle derfor suppleres med en endelig dom for at sikre tilstrækkelig objektivitet i forhold til optagelse i registret.

Det var endvidere Datatilsynets vurdering, at optagelse i registret alene på baggrund af lejelovens § 97, stk. 2 (hvorefter lejer senest 8 dage før fraflytning skal opgive den adresse, som meddelelser kan sendes til) ville være uproportionalt henset til de indgribende konsekvenser, som en optagelse i registret kunne medføre. Datatilsynet fastsatte derfor vilkår om, at registrering på baggrund af lejelovens § 97, stk. 2, kun må ske, hvis lejer i forbindelse med fraflytning af lejemålet har et økonomisk mellemværende med udlejer.

Endelig fastslog Datatilsynet, at hverken registrering fra eller videregivelse til almennyttige boligselskaber kunne anses for sagligt og proportionalt i forbindelse med Privous ApS' advarselsregister, fordi almennyttige boligselskaber kun under visse særlige omstændigheder kan afvise boligsøgende.

Datatilsynet fandt i øvrigt ikke grundlag for at tillade Privous ApS at opbevare oplysningerne i mere end 2 år.



Internationalt arbejde

Med databeskyttelsesforordningen har det internationale samarbejde fået en ny og større betydning. Databeskyttelsesområdet er således nu i langt højere omfang reguleret på EU-niveau, ligesom der med forordningen er etableret et ganske 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 Datatilsynet.

Datatilsynet har på den baggrund udarbejdet en strategi for det internationale arbejde, som skal være med til at sikre dette, ligesom strategien skal sikre, at tilsynet kan deltage aktivt og kvalificeret såvel på arbejdsgruppeniveau som på møder i EDPB og på den måde få gjort danske synspunkter gældende i rette tid og på rette sted. Tilsynet deltager i alle arbejdsgrupper under EDPB, ligesom tilsynet aktivt involverer sig i arbejdet med udarbejdelse af vejledninger, afgørelser mv., både som ledende skribent på udvalgte dokumenter og som medforfatter på andre.

Herudover deltager Datatilsynet meget aktivt i det nordiske samarbejde. ligesom tilsynet er involveret i det øvrige internationale samarbejde på databeskyttelsesområdet, herunder Global Privacy Assembly og Europarådet.

Det Europæiske Databeskyttelsesråd (EDPB)

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 de 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. Der holdes møde ca. en gang om måneden enten online eller fysisk.

Arbejdet med forberedelsen af vejledninger, udtalelser, afgørelser mv., som EDPB skal godkende, forestås primært af 12 ekspertarbejdsgrupper, som normalt mødes med 1-2 måneders intervaller. Møderne holdes enten online eller fysisk i Bruxelles, ligesom der nogle gange afholdes hybridmøder, dvs. deltagerne kan vælge at møde op fysisk i Bruxelles eller deltage 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 D atatilsynets hjemmeside og LinkedIn profil bliver der også løbende offentliggjort vejledninger mv. fra EDPB.

Styrket samarbejde om grænseoverskridende sager

I april 2022 afholdt EDPB et møde i Wien, der havde til formål at styrke medlemsstaternes samarbejde om grænseoverskridende sager. Det styrkede samarbejde skal bl.a. sikre en stærkere og mere effektiv håndhævelse af databeskyttelsesreglerne i komplicerede, grænseoverskridende sager.

EDPB vedtog på mødet en liste med udvælgelseskriterier for de grænseoverskridende sager, der skal behandles som såkaldte strategiske sager. Dette indebærer, at sagen vil blive opprioriteret og understøttet af EDPB, bl.a. ved oprettelse af en task-force bestående af frivillige tilsynsmyndigheder, der kan udveksle viden og sikre en hurtig, ensartet håndhævelse af databeskyttelsesforordningen. Strategiske sager vil blive udvalgt af EDPB på baggrund af forslag fra de enkelte tilsynsmyndigheder.

På mødet vedtog EDPB endvidere, at der skal udarbejdes en liste til Europa-Kommissionen over procedureregler, der ønskes harmoniseret på EU-niveau med henblik på at strømline samarbejdet mellem tilsynsmyndighederne.

EDPB vedtog efterfølgende i oktober 2022 en sådan liste, som bl.a. indeholder forsalg til harmonisering af partsrettigheder, tidsfrister og betingelser for afvisning af klager. Listen blev sendt til Europa-Kommissionen, som i februar 2023 har offentliggjort, at der vil blive tage initiativ til lovgivningsmæssige ændringer som følge heraf i løbet af året.

Overførsel af personoplysninger til USA

Databeskyttelsesforordningen giver mulighed for, at Europa-Kommissionen med en såkaldt tilstrækkelighedsafgørelse kan fastslå, at beskyttelsesniveauet for personoplysninger i et tredjeland eller en international organisation i det væsentlige svarer til beskyttelsesniveauet inden for EU/EØS. I givet fald vil det pågældende land blive anset for et såkaldt sikkert tredjeland, og overførsler af personoplysninger fra EU/EØS til landet kan ske uden yderligere foranstaltninger fra dataeksportørens side.

Siden juli 2020, hvor EU-Domstolen i den meget omtalte Schrems II-sag ugyldiggjorde den såkaldte Privacy Shield-ordning, som havde dannet grundlag for en tilstrækkelighedsafgørelse vedrørende USA, har USA været at betragte som et usikkert tredjeland, hvilket indebærer, at dataeksportører skal sikre et tilstrækkeligt beskyttelsesniveau, når de overfører personoplysninger dertil.

På baggrund af Schrems II-afgørelsen indledte Europa-Kommissionen og de amerikanske myndigheder forhandlinger om en ny ordning, som skal afløse Privacy Shield-ordningen. Dette resulterede i marts 2022 i vedtagelsen af det såkaldte Trans Atlantic Data Privacy Framework, som skal danne grundlag for en ny tilstrækkelighedsafgørelse vedrørende USA.

Efterfølgende præsenterede Europa-Kommissionen i december 2022 et udkast til en tilstrækkelighedsafgørelse vedrørende USA.

Inden tilstrækkelighedsafgørelsen kan vedtages, skal EDPB afgive en udtalelse herom til Europa-Kommissionen. EDPB's udtalelse blev sendt til Europa-Kommissionen i slutningen af februar 2023, og Datatilsynet har deltaget i den gruppe af tilsynsmyndigheder, som udarbejdede udkastet til EDPB-udtalelsen. EDPB's udtalelse er alene rådgivende, og EU-Kommissionen skal derfor nu vurdere, hvilke tiltag udtalelsen giver anledning til. Europa-Parlamentet skal ligeledes komme med en ikke bindende udtalelse. Herefter skal EU-Kommissionen forelægge sit udkast til tilstrækkelighedsafgørelse for det såkaldte Artikel 93-udvalg, der består af repræsentanter for medlemsstaternes regeringer (i Danmark er det Justitsministeriet), inden EU-Kommissionen endeligt kan vedtage afgørelsen.

Bindende afgørelser

I løbet af 2022 har EDPB truffet fire bindende afgørelser i såkaldte tvistbilæggelsessager efter proceduren i databeskyttelsesforordningens artikel 65.

Den første bindende afgørelse blev vedtaget af EDPB i juli 2022. I sagen, der vedrørte virksomheden Accor, havde det franske datatilsyn som ledende tilsynsmyndighed udarbejdet et udkast til en afgørelse, hvori man havde konstateret en række overtrædelser af de databeskyttelsesretlige regler, herunder retten for de registrerede til at gøre indsigelse mod behandling af personoplysninger i markedsføringsøjemed. Udkastet til afgørelse blev mødt af en indsigelse fra en anden berørt tilsynsmyndighed, der mente, at den bøde, der blev lagt op til i udkastet til afgørelse, ikke var tilstrækkelig. Indsigelsen blev ikke fulgt af det franske datatilsyn, hvorved tvistbilæggelsesproceduren blev iværksat.

EDPB slog i sin bindende afgørelse fast, at bøden hverken var proportional, effektiv eller havde afskrækkende virkning, hvorfor bødeniveauet skulle hæves. Datatilsynet deltog som såkaldt co-rapporteur i sagen og var dermed med til at udfærdige afgørelsen, inden den blev endeligt vedtaget.

De øvrige tre bindende afgørelser omhandlede alle Metas behandling af personoplysninger på henholdsvis Facebook, Instagram og WhatsApp. Det irske datatilsyn, som var ledende tilsynsmyndighed, havde i sine udkast til afgørelser konstateret overtrædelser af princippet om gennemsigtighed. Udkastene til afgørelser blev i alle tre sager mødt af indsigelser fra flere berørte tilsynsmyndigheder. Det irske datatilsyn valgte ikke at følge de fremsatte indsigelser og indledte dermed tvistbilæggelsesproceduren.

EDPB slog i sine bindende afgørelser fast, at Facebook, Instagram og WhatsApps behandling af personoplysninger af hensyn til opfyldelse af en kontrakt i de konkrete sager ikke var en passende behandlingshjemmel, når formålet med behandlingen var adfærdsbaseret markedsføring og, som det var tilfældet med WhatsApp-sagen, forbedring af services. EDPB slog endvidere fast, at bødeniveauet skulle være højere, og at det irske tilsyn skulle tage overtrædelsen af databeskyttelsesforordningens artikel 6, stk. 1, om behandlingsgrundlag i betragtning ved udregningen af det nye bødeniveau.

Særlige internationale tilsynsforpligtelser

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

SIS (Schengen-informationssystemet)

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), 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 2022 tre tilsyn vedrørende Rigspolitiets behandling af personoplysninger i relation til SIS II.

Som led i tilsynet med behandlingen 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 2022 afholdt to møder.

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 idriftsættes i 2023.

Herudover deltog Datatilsynet i efteråret 2022 i en såkaldt Schengen-evaluering af Danmark, hvor bl.a. databeskyttelsesområdet blev evalueret i forhold til de krav, som Schengen-reglerne opstiller. Evalueringen blev foretaget af et evalueringshold bestående af eksperter fra forskellige EØS-lande, Europa-Kommissionen og Den Europæiske Tilsynsførende for Databeskyttelse. Eksperterne skulle bl.a. evaluere, hvordan Datatilsynet lever op til sin tilsynsforpligtelse med behandling af personoplysninger i SIS og i Visuminformationssystemet (VIS).

Det overordnede formål med evalueringen er at sikre, at Schengen-reglerne bliver anvendt effektivt, konsekvent, rettidigt og gennemsigtigt af Schengen-medlemsstaterne, samtidig med at der opretholdes et højt niveau af gensidig tillid mellem medlemsstaterne.

Datatilsynet skal i 2023 følge op på evalueringsholdets anbefalinger og bemærkninger.

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 (Told-informationssystemet)

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 deltager endvidere på EU-niveau i Den Fælles Tilsynsmyndighed for Toldinformationssystemet (JSA Customs) og Koordinationsgruppen for tilsynet med Toldinformationssystemet (CIS SCG). Der har i 2022 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 2022 har Datatilsynet ført tilsyn med Rigspolitiets behandling af personoplysninger i medfør af Eurodac-forordningen til retshåndhævende formål.

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 2022 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
- Retshåndhævende myndigheders adgang til Eurodac
- Arbejdsprogrammet i gruppen for 2022-2024

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 (Visum-informationssystemet)

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 2022 gennemført et tilsyn vedrørende Udlændinge-og Integrationsministeriets behandling af personoplysninger i VIS og igangsat et tilsyn vedrørende Udenrigsministeriets behandling af personoplysninger i VIS.

Som led i tilsynet med behandling af personoplysninger i VIS deltager Datatilsynet endvidere i Koordinationsgruppen for tilsynet med visuminformationssystemet (VIS 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 2022 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 Europa-Kommissionens forslag til digitalisering af visumproceduren og arbejdet med implementeringen af den reviderede 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 af arbejdsdokument vedrørende sletning af oplysninger i VIS før tid.
- Arbejdsprogrammet i gruppen 2022-2024.


HALIÇ
RESTAURANT

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 Marked-informationssystemet)

Informationssystemet for det indre marked (IMI) er oprettet af Europa-Kommissionen og har overordnet til formål at lette europæiske myndigheders grænseoverskridende samarbejde og sagsbehandling.

Datatilsynet fører tilsyn med danske myndigheders behandling af personoplysninger i IMI.

På EU-niveau deltager Datatilsynet i Koordinationsgruppen for tilsynet med Indre marked-informations-systemet (IMI CSC). Koordinationsgruppen består af repræsentanter for Den Europæiske Tilsynsførende for Databeskyttelse, de nationale datatilsyn i EU-medlemslandene og de nationale datatilsyn i Island, Norge og Liechtenstein.

Der har i 2022 været afholdt to møder i koordinationsgruppen, hvor man bl.a. arbejder på et sæt anbefalinger til nationale myndigheder om iagttagelse af oplysningspligten, når personoplysninger behandles i IMI.

På Datatilsynets hjemmeside under punktet "Internationalt" findes generel information om IMI og Datatilsynets opgaver i relation hertil, 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.

Af ressourcemæssige årsager har Datatilsynet ikke deltaget i møder i Europarådet i 2022.

Den internationale arbejdsgruppe om databeskyttelse i teknologi

Den internationale arbejdsgruppe om databeskyttelse i teknologi (tidligere kaldet "Berlin-gruppen") har i 2022 afholdt to møder.

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 gruppens hjemmeside.

Gruppens fokus på privatliv og sikkerhed har i 2022 ført til vedtagelsen af to udtalelser.

Den ene udtalelse omhandler privatlivsbeskyttelse ved brug af teknologi til ansigtsgenkendelse; den anden udtalelse beskæftiger sig med de såkaldte "smart cities", herunder særligt om overvågningen ved brug af teknologier der pejler, følger og interagerer med individet i bymiljøet.

Udtalelsen om ansigtsgenkendelse berører både de tekniske aspekter ved teknologien og den data-

behandling, der foretages af private og offentlige som en del af retshåndhævende virksomhed. Særligt databeskyttelsesretlige problemstillinger omkring den kontinuerlige og udbredte overvågning, både i forhold til proportionalitet og i forhold til ændringer i individets frie adfærd på overvågede arealer, er i fokus. Herudover behandles spørgsmål om bias, udøvelsen af rettigheder samt de IT-sikkerhedsmæssige udfordringer, der er specifikke for teknologien.

Udtalelsen om "smart cities" berører problemstillinger som gennemsigtighed, dataminimering, rettighedsudøvelse og datastøttede beslutningsprocesser, herunder profilering, der kan ske i byrum, hvor signaler fra det enkelte individs bærbare enheder, indsamles og behandles. Der er i papiret 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.

I årets løb har gruppen i øvrigt arbejdet med aktuelle emner, som indeholder problemstillinger med hensyn til databeskyttelse og beskyttelse af privatliv, eksempelvis blockchain, webtracking, smart dust, quantum computing, telemetridata, syntetisk data, elektroniske vaccinecertifikater, centralbankers digitale pengeudstedelse, kasseløs butiksbetjening (just walk out), biometri i elektronisk online autentifikation, ISO-standardisering, privatlivsbeskyttelse og forhold omkring forfølgelse og uønsket opmærksomhed i digital forstand, såkaldt cyber bullying og stalking.

Nordisk samarbejde

Datatilsynet lægger stor vægt på at have et tæt samarbejde med de øvrige nordiske datatilsyn, da tilsynene har mange fælles interesser og synspunkter. De nordiske tilsyn er derfor i jævnlig kontakt om såvel konkrete som generelle emner og drøfter også emner af fælles interesse i forbindelse med deltagelse i møder i Det Europæiske Databeskyttelsesråd og dets ekspertarbejdsgrupper.

I tillæg hertil afholder tilsynene en gang om året et nordisk møde med deltagelse af både ledelse, sagsbehandlere og it-eksperter.

Det nordiske møde blev i 2022 afholdt i Helsinki, hvor man ved en erklæring fulgte op på den såkaldte Stockholm-erklæring, som tilsynene vedtog i 2019, da det svenske datatilsyn var vært for mødet. Der blev som følge af Covid-19 ikke afholdt nordiske møder i 2020 og 2021.

Helsinki-erklæringen lægger især vægt på at fortsætte det tætte nordiske samarbejde på databeskyttelsesområdet – både i EU-sammenhæng og de nordiske lande imellem.

På initiativ fra det danske datatilsyn blev det med Helsinki-erklæringen endvidere besluttet at nedsætte en arbejdsgruppe, som skal beskæftige sig med beskyttelse af børns personoplysninger i forbindelse med onlinespil. Arbejdsgruppen skal bl.a. bidrage til at identificere muligheder for en fælles vejledningsindsats og håndhævelsesforanstaltninger.

Den europæiske konference

Den europæiske konference for datatilsynsmyndigheder, også kaldet Forårskonferencen, afholdes en gang årligt.

Af bl.a. ressourcemæssige årsager deltog Datatilsynet ikke i konferencen i 2022, som blev afholdt i Kroatien.

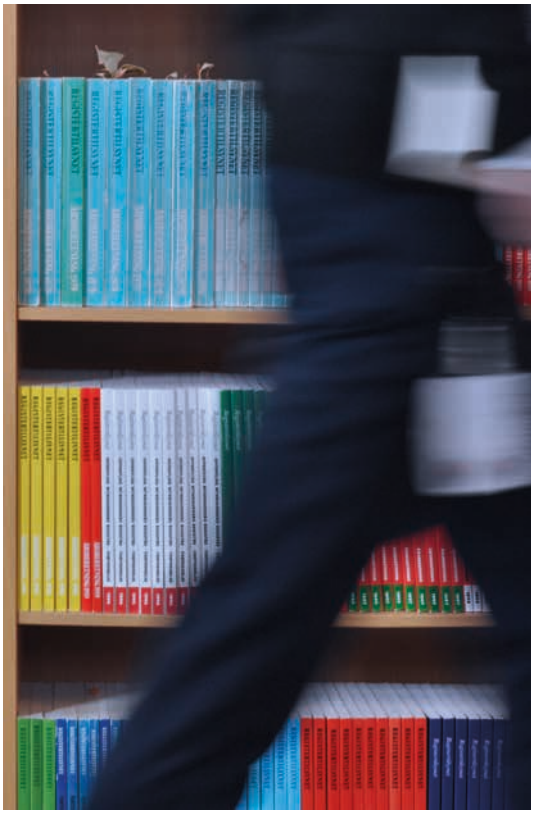
Global Privacy Assembly

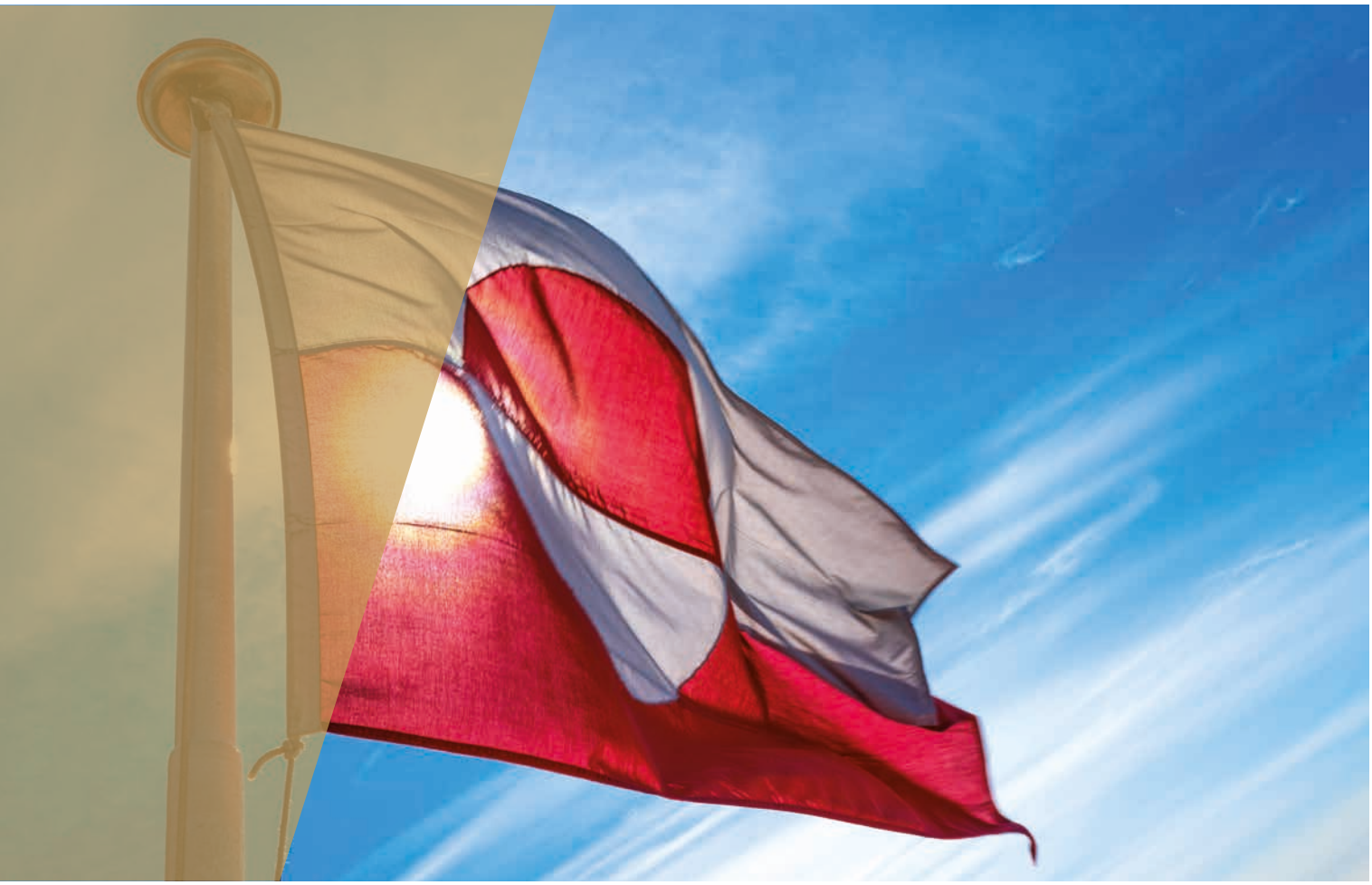
Global Privacy Assembly (GPA) er et globalt forum, som har til formål at fremme samarbejdet mellem nationale databeskyttelsesmyndigheder.

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.

På konferencen i 2022 i Istanbul, som Datatilsynet deltog i, vedtog GPA en række resolutioner om bl.a. opbygningen af en større kapacitet i forbindelse med det internationale samarbejde om cybersikkerhed og om hensigtsmæssig brug af personoplysninger i forbindelse med ansigtsgenkendelse.

Som en del af konferencen blev der også uddelt de årlige GPA Awards. Her modtog Datatilsynet priser i kategorierne "Education and Public Awareness" og "People's Choice" for Datadysten, som er et online spil, der er udviklet særligt til børn og unge med henblik på at fremme deres kendskab til databeskyttelse. Priserne blev tildelt på baggrund af en afstemning blandt GPA-medlemmer fra hele verden.





Grønland og Færøerne

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

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

Datatilsynet har i 2022 i lighed med foregående år kun modtaget få konkrete henvendelser om behandling af personoplysninger i Grønland eller ved rigsmyndighederne på Færøerne og har ikke behandlet mere principielle sager herom. Endvidere har tilsynet modtaget enkelte anmeldelser om behandling af personoplysninger i Grønland. Formålet med anmeldelsesordningen er at give Datatilsynet mulighed for at kunne kontrollere visse behandlinger af personoplysninger.

Anmeldelsesordningen har endvidere til formål at gøre det muligt for offentligheden at gøre sig bekendt med behandlingerne. På Datatilsynets hjemmeside findes fortegnelser over anmeldelser fra myndigheder og virksomheder mv. i Grønland af igangværende behandlinger.

Del 2: Retshåndhævelsesloven

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

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

I 2022 har Datatilsynet bl.a. behandlet klagesager og anmeldelser fra de retshåndhævende myndigheder om brud på persondatasikkerheden.

Vejledning om brugen af ansigtsgenkendelse for retshåndhævende myndigheder

Det Europæiske Databeskyttelsesråd (EDPB) vedtog i maj 2022 en vejledning om brugen af ansigtsgenkendelse for retshåndhævende myndigheder.

Vejledningen henvender sig til lovgivere på EU- og nationalt plan samt til de retshåndhævende myndigheder, som har til hensigt at indføre og anvende ansigtsgenkendelsesteknologi til retshåndhævende formål.

Selv om moderne teknologi giver de retshåndhævende myndigheder fordele, f.eks. hurtig identifikation af personer, der er mistænkt for alvorlige forbrydelser, skal den opfylde kravene om nødvendighed og proportionalitet. Ansigtsgenkendelsesteknologi er tæt forbundet med behandling af personoplysninger, herunder biometriske data, og udgør dermed en alvorlig risiko for individuelle rettigheder.

EDPB understreger derfor i vejledningen, at ansigtsgenkendelsesværktøjer kun bør anvendes i nøje overensstemmelse med retshåndhævelsesdirektivet, og at anvendelsen skal være nødvendig og forholdsmæssig, sådan som det er fastsat i EU's Charter om grundlæggende rettigheder. EDPB gentager samtidig sin opfordring til et forbud mod ansigtsgenkendelse under visse omstændigheder.

Databekymringspostkassen

I juli 2019 lancerede Datatilsynet en databekymringspostkasse i samarbejde med Dataetisk Råd, hvor borgere frem til udgangen af 2022, hvor postkassen blev nedlagt, kunne henvende sig via e-mail med deres databekymringer. Lanceringen skete i forbindelse med nedsættelsen af Dataetisk Råd, hvor det var hensigten, at de indsendte databekymringer skulle være med til at understøtte Dataetisk Råd i dets opgaver. Begge initiativer skete på baggrund af den daværende regerings Sammenhængsreform om Digital Service i Verdensklasse.

Datatilsynet modtog i 2022 i alt 32 databekymringer. Siden lanceringen den 4. juli 2019 og frem til den 31. december 2022, hvor postkassen blev nedlagt, har Datatilsynet modtaget i alt 186 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.

I 2022 har en generel tendens været, at en række bekymringer har vedrørt den behandling, der sker af personoplysninger i forbindelse med MitID.

Herudover har bekymringerne bl.a. omhandlet private virksomheders behandling af personoplysninger, f.eks. i forhold til deres brug af personnummer (cpr.nr) og i forbindelse med anvendelsen af cookies. Enkelte bekymringer har omhandlet videregivelse af oplysninger uden samtykke.

Databekymringspostkassen er som nævnt ophørt, idet det politisk er besluttet ikke at føre den videre. Det betyder dog ikke, at man ikke længere har mulighed for at kontakte Datatilsynet, hvis man har en databekymring. Fremadrettet kan man fortsat, som det hele tiden har været muligt, sende eventuelle bekymringer eller f.eks. et tip om manglende overholdelse af databeskyttelsesreglerne til tilsynet. Dette skal i så fald blot ske via Datatilsynets hovedpostkasse.

Indberetninger til Den Nationale 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). 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 over-trædelser af EU-retten inden for en række områder, herunder offentligt udbud, produktsikkerhed, miljøbeskyttelse, fødevaresikkerhed m.fl., og indberetninger om alvorlige lovovertrædelser eller øvrige alvorlige forhold, herunder chikane. Den eksterne whistleblowerordning etableret i Datatilsynet trådte i kraft den 17. december 2021, som også var datoen for whistleblowerlovens ikrafttrædelse.

Den eksterne whistleblowerordning i Datatilsynet har siden skiftet navn til Den Nationale Whistleblower-ordning for tydeligere at signalere til omverdenen, at selv om ordningen er etableret i Datatilsynet, så kan ordningen bruges til at indberette om alle forhold omfattet af whistleblowerloven – ikke kun forhold vedrørende databeskyttelse.

Den Nationale Whistleblowerordning er etableret i Datatilsynet, men fungerer uafhængigt og selvstændigt i forhold til tilsynet. I 2022 var 9 medarbejdere tilknyttet whistleblowerordningen. Medarbejderne er ansat i Datatilsynet og beskæftiger sig også med databeskyttelsesretlige opgaver, men de er særligt autoriseret til at arbejde med indberetninger i Den Nationale Whistleblowerordning, og deres arbejde med indberetningerne foregår adskilt fra Datatilsynets øvrige virksomhed. Medarbejderne er underlagt en særlig tavshedspligt med hensyn til oplysninger, der indgår i indberetningerne.

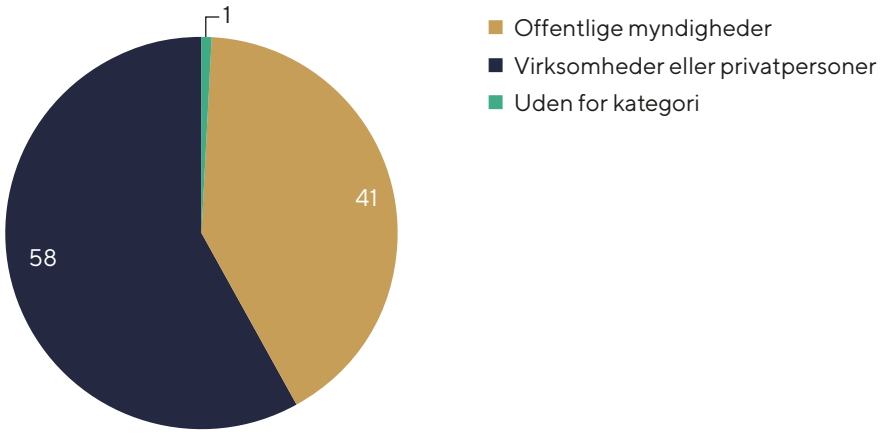
Ifølge whistleblowerlovens § 27 skal myndigheder m.v. omfattet af reglerne om aktindsigt i offentlighedsloven mindst én gang årligt offentliggøre oplysninger om deres virksomhed efter whistleblowerloven. Den Nationale Whistleblowerordning har i forbindelse med rapporteringen for 2022 besluttet at lave opgørelsen for perioden fra lovens ikrafttræden den 17. december 2021 til og med den 31. december 2022.

Modtagne indberetninger i 2022

Den Nationale Whistleblowerordning modtog i perioden fra den 17. december 2021 til og med den 31. december 2022 i alt 116 indberetninger.

Af de 116 modtagne indberetninger vedrørte 67 indberetninger forhold hos private virksomheder eller privatpersoner, 48 indberetninger vedrørte forhold hos offentlige myndigheder, mens en enkelt indberetning faldt uden for kategori.

Hvem blev der indberettet om?



En stor del af de modtagne indberetninger i 2022 omhandlede forhold vedrørende databeskyttelse, hvilket sandsynligvis skyldes, at ordningen er etableret i Datatilsynet. Af de indberetninger, som faldt inden for whistleblowerlovens anvendelsesområde, omhandlede 66 % således forhold om databeskyttelsesforordningen, navnlig vedrørende utilstrækkelig behandlingssikkerhed, men en del sager omhandlede også overvågning af medarbejdere.

Gennemgående for flere sager var indberetninger om dårlige arbejdsforhold, især relateret til det psykiske arbejdsmiljø. 4 % af indberetningerne modtaget i 2022 omhandlede egentlige chikaneforhold.

En række sager omhandlede indberetninger om økonomiske forhold, herunder sager om muligt misbrug af offentlige midler og regnskabssvindel.

Der blev også modtaget flere indberetninger om inddragelse af usaglige hensyn i forbindelse med ansættelser i det offentlige.

Af de 116 modtagne indberetninger fandt Den Nationale Whistleblowerordning i 30 sager grundlag for at videregive oplysningerne til videre foranstaltning hos relevante tilsynsmyndigheder. Ingen af de modtagne indberetninger gav Den Nationale Whistleblowerordning anledning til at overdrage sagen direkte til politiet.

11 indberetninger blev efter endt undersøgelse vurderet til at være klart mindre alvorlige forhold, som ikke krævede yderligere opfølgning, og to indberetninger blev afsluttet, fordi forholdene allerede tidligere var blevet undersøgt af Den Nationale Whistleblowerordning, jf. whistleblowerlovens § 21.

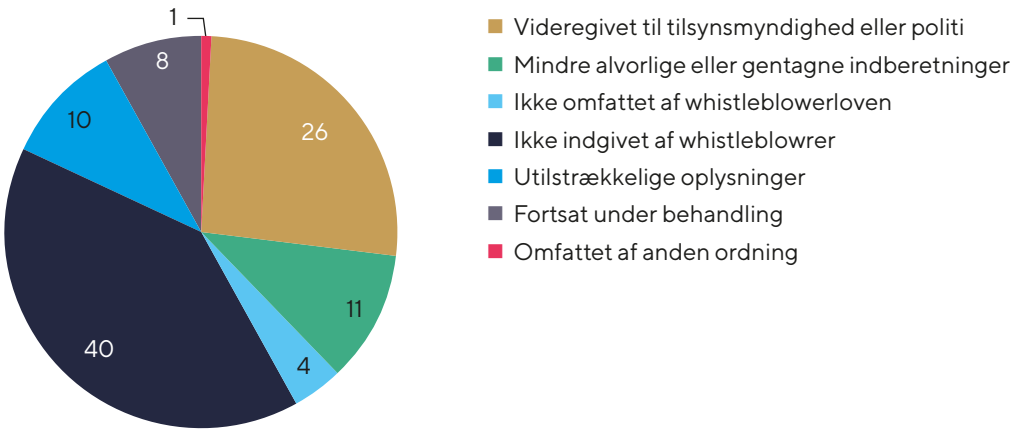
En enkelt indberetning indgivet til Den Nationale Whistleblowerordning skulle i stedet behandles af en af de særligt oprettede eksterne whistleblowerordninger, jf. whistleblowerlovens § 17.

12 indberetninger blev afsluttet, fordi det ikke var muligt at få tilstrækkelige oplysninger fra whistleblowerne til, at Den Nationale Whistleblowerordning kunne færdigbehandle sagerne.

5 indberetninger faldt uden for whistleblowerlovens anvendelsesområde, og 46 indberetninger var indgivet af personer, som ikke var whistleblowere i lovens forstand. Disse personer blev i stedet for – så vidt muligt – vejledt om mulighederne for at kontakte andre instanser.

9 indberetninger var fortsat under behandling pr. 31. december 2022.

Udfald af indberetningerne



Alle sager afsluttet i 2022 blev færdigbehandlet inden for fristerne i whistleblowerlovens § 20, stk. 2. 96 % af de modtagne indberetninger blev således færdigbehandlet inden for 3 måneder, mens 4 % blev behandlet inden for 6 måneder. Den gennemsnitlige sagsbehandlingstid var i 2022 på 27 dage.

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 med senere ændringer 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 med senere ændringer 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 med senere ændringer 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 med senere ændringer om videregivelse af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2.
- Bekendtgørelse nr. 1860 af 23. september 2021 med senere ændringer om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret).
- Bekendtgørelse nr. 220 af 11. februar 2022 om hel eller delvis opbevaring her i landet af personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning.
- Bekendtgørelse nr. 736 af 24. maj 2022 om tilbagemelding om væsentlige helbredsmæssige fund fra anmeldelsespligtige sundhedsvidenskabelige og sundhedsdatavidenskabelige forskningsprojekter, kliniske afprøvninger af medicinsk udstyr m.v. samt visse registerforskningsprojekter.

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
- Vejledende principper om dataansvar for vikarer og konsulenter
- Vejledende tekst af november 2021 om rollefordelingen, når private er leverandører til det offentlige
- Vejledning af december 2017 om databeskyttelsesrådgivere
- Vejledning af januar 2018 om adfærdskodekser og certificeringsordninger (opdateret i december 2018) (under opdatering)
- 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
- Vejledende tekst af juni 2019 om risikovurdering
- 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 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 (under opdatering)
- Vejledning af januar 2021 om udmåling af bøder til virksomheder (under opdatering)
- 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
- Informationspjece af august 2021 – det skal du vide om databeskyttelse
- Begrebet personoplysninger af august 2021 – få et hurtigt overblik
- Vejledning af oktober 2021 om tilsyn med databehandlere
- Vejledende tjekliste af december 2021 til vuggestuer og børnehaver ved brug af billeder og video
- Vejledning af februar 2022 om udmåling af bøder til fysiske personer
- Vejledning af marts 2022 om cloud
- Vejledning af juni 2022 om overførsel af personoplysninger til tredjelande
- Vejledning af oktober 2022 om advarselsregistre
- Vejledning af oktober 2022 om databeskyttelsesreglerne i forbindelse med valgkampagner
- Retningslinjer af november 2022 for lokalarkivers behandling af personoplysninger

De oplistede vejledninger mv. er offentliggjort på Datatilsynets hjemmeside.

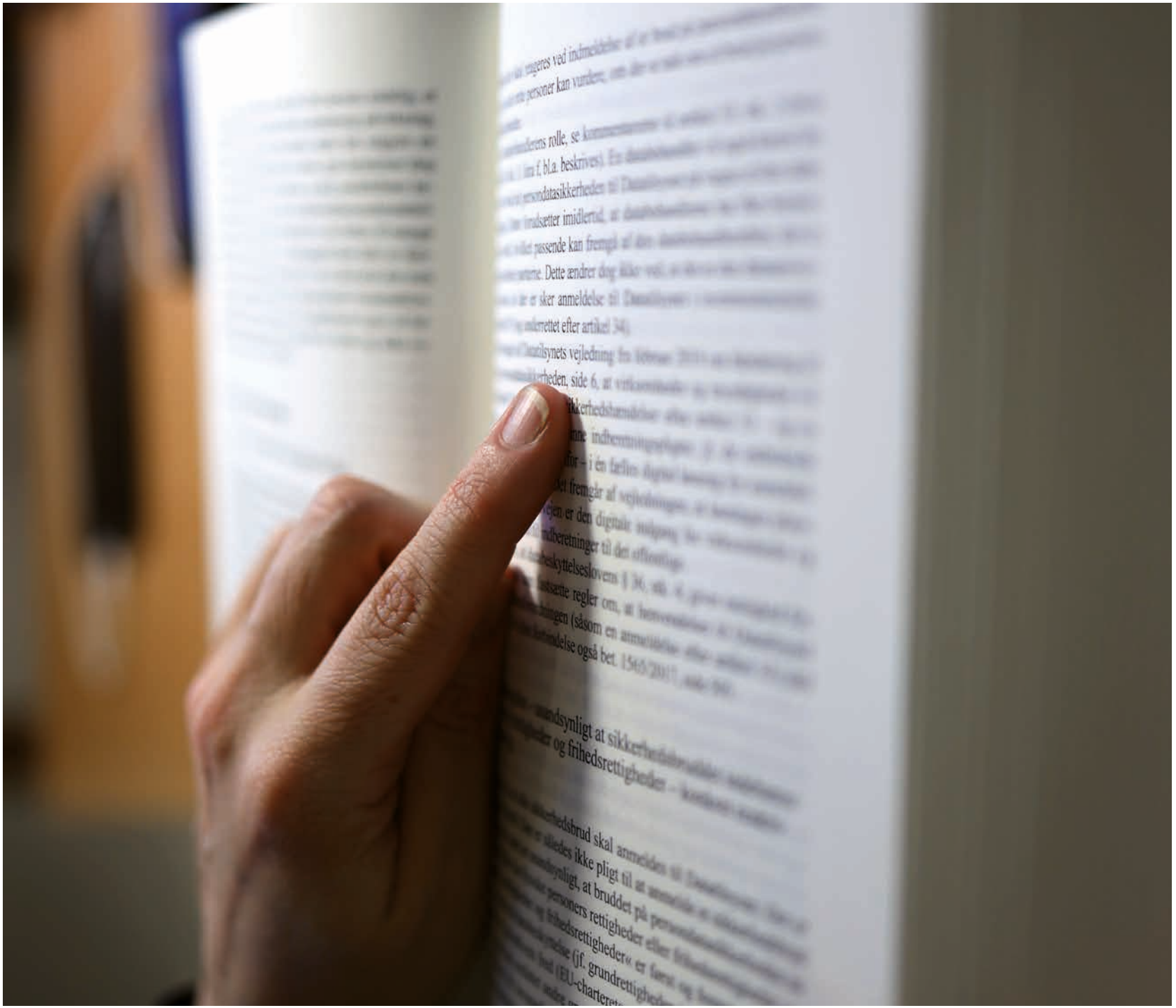
Vejledninger fra Justitsministeriet
- Vejledning af juni 2017 om udveksling af personoplysninger som led i den koordinerede myndighedsindsats over for rocker- og bandekriminalitet.
- Vejledning af december 2018 - Ofte stillede spørgsmål om frivillige foreningers behandling af personoplysninger.
- Vejledning 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.
- (foreløbige) Retningslinjer af juli 2022 for statslige myndigheders opbevaring af SMS-beskeder 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)
- Anvendelse af databeskyttelsesforordningens artikel 60 (Vejledning 2/2022)
- 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)
- Administrative bøder i henhold til databeskyttelsesforordningen, udregning (Vejledning 4/2022)
- Anmeldelse af brud på persondatasikkerheden (Vejledning 9/2022)
- 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 Co-vid-19-udbruddet (Vejledning 3/2020)
- Bindende virksomhedsregler (BCR) for dataansvarlige, ansøgning om godkendelse og om de ele-

menter og principper, der findes i bindende virksomhedsregler for dataansvarlige (Art. 47) (Anbefaling 1/2022)
- 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 databehandlere, standardansøgning (wp265)
- Brug af videoudstyr til behandling af personoplysninger (Vejledning 3/2019)
- Brug af ansigtsgenkendelse i henhold til retshåndhævelsesdirektivet (Vejledning 5/2022)
- Certificering (Vejledning 1/2018)
- Certificering som overførselsgrundlag (Vejledning 7/2022)
- 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 (Vejledning 8/2022)
- 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)
- Praktisk gennemførelse af mindelige løsninger (Vejledning 6/2022)
- Registreredes rettigheder – retten til indsigt (Vejledning 1/2022)
- Relevant og begrundet indsigelse i henhold til forordningen (Vejledning 9/2020)
- Restriktioner i henhold til artikel 23 i databeskyttelsesforordningen (Vejledning 10/2020)
- Samtykke (wp259)
- Samtykke i henhold til forordningen (Vejledning 5/2020)
- Samspillet mellem det andet direktiv om betalingstjenester og databeskyttelsesforordningen (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)
- Vildledende designmønstre i grænseflader på sociale medier: hvordan man genkender og undgår dem (Vejledning 3/2022)
- 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
Layout og tryk: Stibo Complete

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

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