Årsberetning
2023

DATATILSYNET

Datatilsynet

Årsberetning

2023

Indhold

Til Folketinget

I maj 2023 var det fem år siden, at databeskyttelsesforordningen (GDPR) begyndte at finde anvendelse herhjemme og i resten af Europa. For Datatilsynets vedkommende var det samtidig endnu et år præget af et højt aktivitetsniveau med mange vigtige vejledningsinitiativer og større sagskomplekser både nationalt som internationalt. Det var tillige et rekordår, hvor antallet af nyoprettede sager i Datatilsynet nåede sit hidtil højeste niveau med 18.062 sager.

Datatilsynets arbejdsfelt er bredt og varierereret, og det spænder fra at vejlede og rådgive til at behandle klagesager, som også er en del af Datatilsynets tilsynsaktiviteter, og ansøgninger om tilladelse til at behandle personoplysninger, ligesom tilsynet også hvert år gennemfører forskellige andre typer af tilsynsaktiviteter hos myndigheder og virksomheder. Datatilsynet deltager endelig også aktivt i bl.a. Det Europæiske Databeskyttelsesråds håndtering af flere større grænseoverskridende sager i forbindelse med den såkaldte One Stop Shop-mekanisme. Rådet har bl.a. skulle træffe endelig bindende afgørelse i en række større grænseoverskridende sager som følge af, at de berørte europæiske tilsynsmyndigheder ikke kunne blive enige om den ledende tilsynsmyndigheds udkast til en afgørelse i hver af sagerne.

Særligt når det gælder tilsynets vejledningsindsats, retter den sig mod meget forskelligartede aktører: Folketinget, borgerne, private organisationer og virksomheder, frivillige foreninger samt statslige, regionale og kommunale myndigheder. Datatilsynet arbejder i den forbindelse målrettet på at sikre, at alle kender og overholder reglerne for behandling af personoplysninger, og at borgerne kender og kan bruge deres rettigheder.

Informationskampagne for borgere
Den internationale databeskyttelsesdag 28. januar blev i 2023 markeret af Datatilsynet med lanceringen af en landsdækkende informationskampagne målrettet borgerne med et budskab om, at vi alle sammen har en række oplysninger, som vi gerne vil holde for os selv (”hemmeligheder”), og som vi derfor passer ekstra godt på, og at databeskyttelsesreglerne sikrer, at andre behandler vores oplysninger som hemmeligheder.

Kampagnen, der bestod af trykte annoncer og en film, der handler om hemmeligheder, var et supplement til den omfattende vejledning, Datatilsynet siden 2018 har rettet mod virksomheder og myndigheder om, hvordan de bedst kan efterleve reglerne. Den borgerrettede kampagne, som havde en lettere og mere personlig tone, havde til formål at fortælle, hvad databeskyttelsesreglerne kan gøre for borgerne.

GDPR-univers til mindre virksomheder
Et andet væsentligt vejledningsinitiativ var lanceringen i maj 2023 af et nyt vejledningsunivers om databeskyttelsesforordningen (GDPR) til mindre virksomheder. Vejledningsuniverset blev udviklet i et tæt samarbejde med Dansk Erhverv, Dansk Industri og SMVdanmark som repræsentanter for målgruppen, og det er bygget op om syv trin, som virksomheder kan følge for at få bedre styr på deres overholdelse af reglerne. Til hvert trin er der lavet konkrete eksempler. Endvidere består materialet af en omfattende FAQ og jordnære beskrivelser af de grundlæggende begreber i GDPR.

Særlig indsats i forhold til kunstig intelligens
Datatilsynet offentliggjorde i oktober 2023 også en vejledning om offentlige myndigheders brug af kunstig intelligens (AI). Vejledningen indeholder en gennemgang af de krav, som myndigheder skal være særligt opmærksomme på, inden de går i gang med at udvikle AI-løsninger.
Samtidig offentliggjorde Datatilsynet en kortlægning af offentlige myndigheders brug af AI, der giver det hidtil klareste indblik i offentlige myndigheders brug af AI. Bl.a. viser kortlægningen, at brug af AI endnu ikke er ret udbredt blandt offentlige myndigheder. I det omfang AI-løsninger bruges i den offentlige sektor, er der ofte tale om standardløsninger eller samme specialudviklede løsning, der bruges af flere myndigheder.

Forbedret statistik over brud på persondatasikkerheden
Hvert år modtager Datatilsynet flere tusinde anmeldelser om brud på persondatasikkerheden. og 2023 har indtil nu været det år, hvor tilsynet har modtaget flest anmeldelser (9.537). I marts 2023 lancerede Datatilsynet en ny side med statistik over de mange brud, som giver mulighed for at dykke ned i udviklingen i bl.a. typer af brud og de sektorer, hvor de finder sted.

I 2023 gennemførte og lancerede tilsynet tillige et projekt med hurtigere vejledning om relevante tiltag straks ved anmeldelse af brud på persondatasikkerheden gennem implementering af ny sagsgang, hvor der i forbindelse med visitationen af et anmeldt brud på 11 nærmere opregnede områder samtidig sendes målrettet vejledning til anmelder sammen med kvittering for anmeldelsen. Målet er således hurtig og anvendelig hjælp til de organisationer, der skal håndtere bruddene.

Overførsel af personoplysninger til USA
Datatilsynet spilede i 2023 også en meget aktiv rolle i forbindelse med Det Europæiske Databeskyttelsesråds udtalelse om Europa-Kommissionens udkast til en tilstrækkelighedsafgørelse vedrørende USA, og de informationer herom, som Det Europæiske Databeskyttelsesråd udgav i kølvandet på offentliggørelsen af den endelige afgørelse i juli 2023.

Opdateret strategi for en data- og risikobaseret indsats
Datatilsynet udarbejdede i 2023 tillige en ny opdateret strategi for en data- og risikobaseret indsats, som indeholder 12 nye initiativer, der på forskellig vis yderligere skal styrke tilsynets mulighed for at målrette kontrollen til de områder, hvor der er størst risiko for borgernes data. I den opdaterede strategi er der fortsat fokus på at styrke tilsynets datakvalitet, datakilder, dataanvendelse og dokumentation. Samtidig inkluderer strategien en ny strategisk udfordring omhandlende fremdrift i tilsynssager.

Valby, august 2024

Kristian Korfits Nielsen
Formand, Datarådet

Cristina Angela Gulisano
Direktør, Datatilsynet

Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2023 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 2023, herunder foranstaltninger 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.

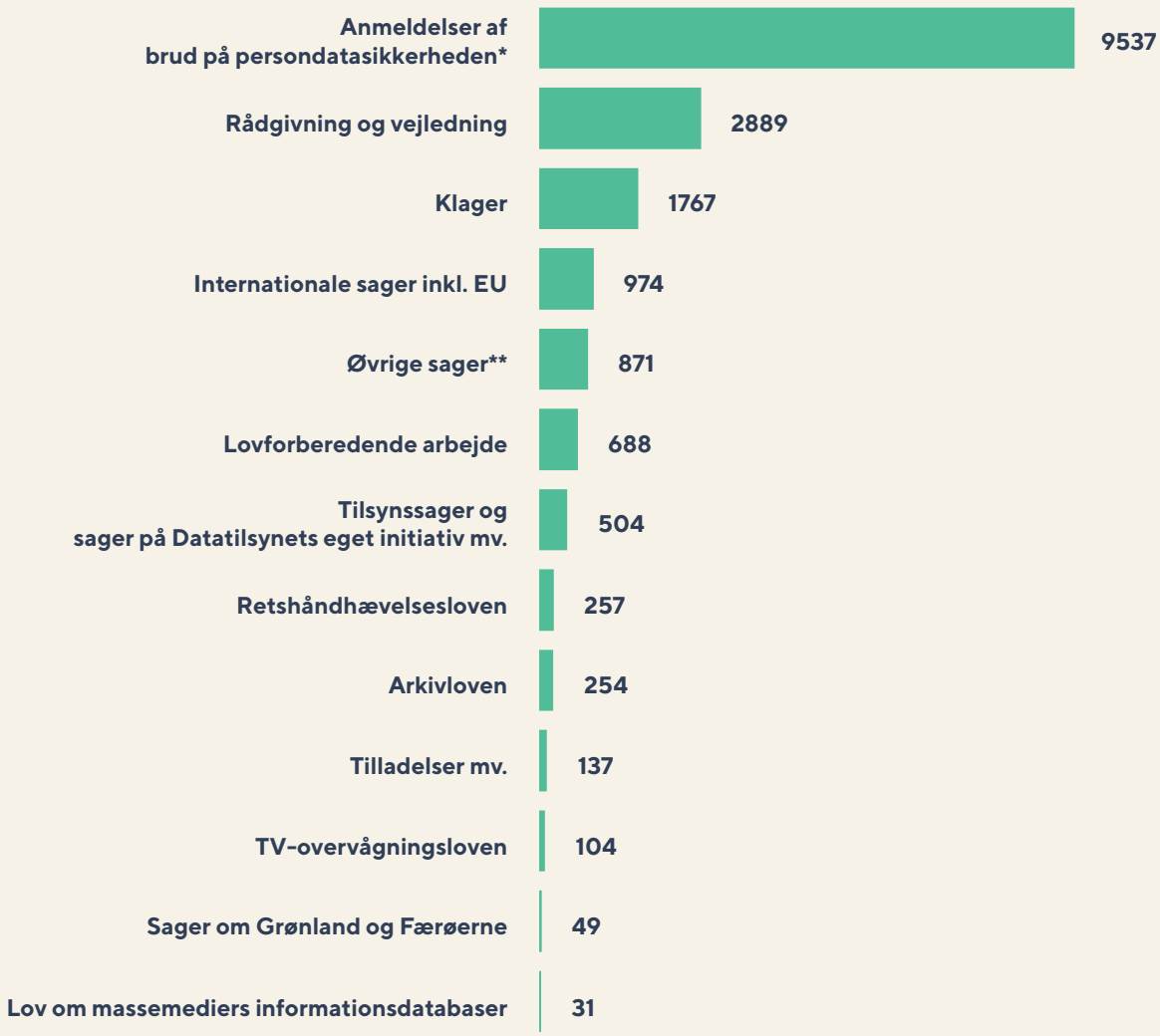
På Datatilsynets hjemmeside www.datatilsynet.dk offentliggør tilsynet løbende udtalelser og afgørelser i sager, som vurderes at være af generel interesse. Datatilsynet kan således henvise til sin hjemmeside for yderligere oplysninger. Årsberetningen sendes endvidere til Europa-Kommissionen og Det Europæiske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

På næste side findes oplysninger om antallet af nye sager, som er oprettet i Datatilsynets journalsystem i 2023.

En del af Datatilsynets sagsbehandling er en genoptagelse 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 **18.062** nye sager i 2023.

Oprettede sager i 2023: 18.062



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.

Rådgivning og vejledning

2.889 sager i alt

1.805
Sager vedr. private

930
Sager vedr. offentlige myndigheder

154
Forskelligt

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 2023 offentliggjort 22 nye eller opdaterede nationale vejledninger, hjemmesidetekster mv. om databeskyttelsesreglerne, som supplerer de 46 nationale vejledninger og vejledende tekster mv., som tilsynet har offentliggjort fra 2017 til 2022. De nye vejledninger omfatter bl.a. en ny vejledning om direkte markedsføring og tre vejledninger på tv-overvågningsområdet, der retter sig mod henholdsvis private virksomheder, offentlige myndigheder og boligforeninger. Datatilsynets vejledning om databeskyttelse i ansættelsesforhold, som er en af tilsynets mest populære vejledninger, blev også opdateret i 2023.

Datatilsynet yder også en aktiv indsats på vejledningsområdet i europæiske sammenhænge og har i regi af Det Europæiske Databeskyttelsesråd bidraget til udarbejdelsen af 5 nye fælleseuropæiske vejledninger om databeskyttelsesforordningen og retshåndhævelsesdirektivet. I 2023 udarbejdede Det Europæiske Databeskyttelsesråd bl.a. nye retningslinjer for udstedelse af bøder.

Alle de nævnte vejledninger og vejledende tekster mv. – såvel de nationale som de fælleseuropæiske vejledninger – 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 viden om, hvilke udfordringer de registrerede, andre offentlige myndigheder og den private sektor oplever inden for databeskyttelsesområdet. Datatilsynet var i 2023 f.eks. tilstede med en stand på OffDig, der er Danmarks største konference om offentlig digitalisering, og på Digitaliseringsmessen, ligesom tilsynet deltog i konferencen Lærfest. Endvidere talte Datatilsynets direktør bl.a. på konferencen Digital Tech Summit, der er nordens største deep tech-konference, og hvor der i 2023 var fokus på AI.

Datatilsynets podcast – ”Bliv klogere på GDPR”

Siden lanceringen i september 2019 har Datatilsynet produceret 25 tilgængelige episoder af tilsynets podcast ”Bliv klogere på GDPR”. I 2023 opnåede podcasten over 60.000 afspilninger, hvilket bringer det samlede antal afspilninger op på godt 260.000 afspilninger.

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. 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.

I anledning af de første fem år med databeskyttelsesforordningen udgav Datatilsynet i maj 2023 en særlig podcastepisode, hvor tilsynets direktør gav sit bud på, hvordan det var gået siden 2018, og hvad man kan forvente de kommende år. Derudover udkom der i juni en episode med særligt fokus på den meget omtalte Google Chromebook-sag.

Datatilsynets podcast er tilgængelig på alle gængse streamingtjenester.

Ny tjekliste til skoler om brug af billeder og video

Datatilsynet offentliggjorde i januar 2023 en tjekliste, som skal hjælpe skoler med at overholde databeskyttelsesreglerne, når de bruger billeder og video af børn og medarbejdere.

Tjeklisten er opbygget som en kvikguide med en række gode råd og konkrete eksempler. Den indeholder også et bilag med forklaring af databeskyttelsesreglerne og kommer bl.a. ind på, hvor længe billeder må ligge på intranettet, og hvordan skolerne skal passe på billeder og videoer.

En del af tjeklisten forholder sig til spørgsmålet om, hvornår skoler skal indhente samtykke fra forældre, og hvornår behandlingen af billeder kan ske på baggrund af andre lovlige grundlag.

Tilsynet modtog i forbindelse med offentliggørelsen af tjeklisten flere henvendelser fra bekymrede forældre og interesserede journalister, der undrede sig over, at skoler nu kunne bruge billeder af elever uden samtykke fra forældre.

For at give et samlet og nuanceret overblik over reglerne og tilsynets anbefaling på området, udgav Datatilsynet derfor også en podcastepisode, hvor tilsynet forklarede, hvorfor det ofte er mere oplagt at bruge et andet grundlag end samtykke – og hvor Datatilsynet opfordrede til en løbende dialog mellem skole, elever og forældre om netop deling af billeder.

En række interessenter har været inddraget under udarbejdelsen for at sikre, at tjeklisten dækker behovet hos deres medlemmer, bl.a. Kommunernes Landsforening, Danmarks Private Skoler, Skolelederforeningen og udvalgte kommuner.

Opdatering af Datatilsynets vejledning om databeskyttelse i ansættelsesforhold

Databeskyttelse i ansættelsesforhold er et komplekst område, hvor bl.a. de overordnede databeskyttelsesretlige regler, ansættelsesretlige regler samt kollektive overenskomster og aftaler har betydning for de behandlinger af personoplysninger, der sker på arbejdspladser og i fagforeninger mv.

Såvel offentlige som private arbejdsgivere behandler en stor mængde personoplysninger om ansøgere i forbindelse med rekruttering og om medarbejdere. Dette gælder både under ansættelsen og efter ansættelsens ophør. Tilsvarende behandler faglige organisationer og tillidsrepræsentanter person-oplysninger om både deres medlemmer og andre medarbejdere på arbejdspladsen. Hertil kommer, at der i vidt omfang udveksles oplysninger mellem de enkelte aktører.

Datatilsynets vejledning om databeskyttelse i ansættelsesforhold er som følge heraf en af tilsynets mest populære vejledninger, og tilsynet offentliggjorde derfor i marts 2023 en opdateret udgave af vejledningen.

Formålet med at opdatere vejledningen var at indarbejde Datatilsynets seneste praksis på området, herunder om indhentelse af straffeattester og referencer. Endvidere blev en række afsnit præciseret, herunder om arbejdsgiverens oplysningspligt og videregivelse af personoplysninger, ligesom vejledningens opbygning blev justeret for at gøre vejledningen mere letlæselig og brugbar.

GDPR-univers for små virksomheder

Databeskyttelsesreglerne gælder for både store og små virksomheder, men ofte er opgaven med at overholde reglerne noget mere overkommelig for de små virksomheder, hvis de får den rette hjælp.

Datatilsynet lancerede derfor i maj 2023 et nyt vejledningsunivers om databeskyttelsesforordningen (GDPR) målrettet små virksomheder.

Universet blev udviklet i et tæt samarbejde med Dansk Erhverv, Dansk Industri og SMVdanmark som repræsentanter for målgruppen, og det er bygget op omkring 7 trin, som virksomheder kan følge for at få bedre styr på deres GDPR-compliance. De 7 trin er:

- Skab overblik
- Spørg dig selv ”hvorfor?”
- Husk at slette
- Oplys om, at du behandler personoplysninger
- Sørg for at have gode procedurer
- Husk sikkerheden
- Du er også ansvarlig, når du deler

Derudover indeholder universet en række praksisnære eksempler, en omfattende FAQ og jordnære beskrivelser af de grundlæggende begreber i GDPR.

Ny vejledning om direkte markedsføring

Datatilsynet udgav i juni 2023 en vejledning om de regler i databeskyttelsesforordningen, der er særligt relevante i forbindelse med direkte markedsføring. Vejledningen er målrettet rådgivere og andre med erfaring med databeskyttelse.

Vejledningens fokus er behandling af personoplysninger, som foretages med henblik på direkte markedsføring. Det skyldes, at direkte markedsføring er en af de mest udbredte former for markedsføring, og at direkte markedsføring næsten altid indebærer en behandling af personoplysninger.

Formålet med vejledningen er at tydeliggøre, hvilke databeskyttelsesretlige regler der er særlig relevante, når personoplysninger behandles i markedsføringsøjemed. Vejledningen beskriver bl.a., hvilke overvejelser man skal gøre sig, inden man begynder sine markedsføringsaktiviteter, så man kan tage højde for databeskyttelsesreglerne, før aktiviteterne påbegyndes. Vejledningen indeholder også Datatilsynets vurdering af en række gængse markedsføringsaktiviteter.

Ny vejledning om rollefordeling i forskningsprojekter

Datatilsynet nedsatte i 2022 et specialudvalg med fokus på behandling af personoplysninger i forbindelse med forskning. På baggrund af input fra interessenter i specialudvalget offentliggjorde Datatilsynet i juli 2023 en ny vejledning om fordelingen af de databeskyttelsesretlige roller i forskningssammenhæng.

Målgruppen for vejledningen er især forskere og andre, der arbejder med databeskyttelse i forskning. Vejledningen består hovedsagelig af en lang række eksempler på forskellige konstruktioner af dataansvarlige, databehandlere og fælles dataansvarlige, der kan opstå i praksis. Derudover indeholder vejledningen en oversigt over de momenter, der kan lægges vægt på ved vurderingen af, hvilke databeskyttelsesretlige roller de enkelte parter har i forbindelse med forskningssamarbejder.

Ny vejledning om offentlige myndigheders brug af kunstig intelligens (AI)

Datatilsynet udgav i oktober 2023 en vejledning om offentlige myndigheders udvikling og brug af kunstig intelligens (AI).

Udover at synliggøre Datatilsynets rolle som vejledende og tilsynsførende myndighed inden for det databeskyttelsesretlige område, var formålet med vejledningen at lede myndighederne på rette vej, når de håndterer databeskyttelsesretlige udfordringer i forbindelse med udvikling og anvendelse af AI.

Vejledningen ser nærmere på AI og de grundlæggende overvejelser, som myndigheder skal gøre sig, inden de går i gang med at udvikle AI-løsninger. Det omfatter bl.a. spørgsmål om behandlingsgrundlag, oplysningspligt og konsekvensanalyse.

Kortlægning af AI på tværs af den offentlige sektor

Parallelt med udarbejdelsen af vejledningen gennemførte Datatilsynet en kortlægning af offentlige myndigheders brug af AI. Formålet med kortlægningen var dels at give offentligheden, dels Datatilsynet, der som nævnt ovenfor fører tilsyn med databeskyttelsesreglernes overholdelse, et større kendskab til og forståelse for brugen af nye teknologier i den offentlige sektor.

Kortlægningen viste, at brug af AI endnu ikke er ret udbredt blandt offentlige myndigheder. I det omfang AI bruges i den offentlige sektor, er der ofte tale om standardløsninger eller samme specialudviklede løsning, der bruges af flere myndigheder. Derudover viste kortlægningen, at myndighederne overvejende sikrer sig et relevant behandlingsgrundlag, når de bruger AI-løsninger, men at myndighederne generelt har udfordringer med at overholde kravet om at foretage konsekvensanalyser eller at foretage dem rettidigt.

Ny vejledning om sikkerhedsforanstaltninger

Datatilsynet udgav i november 2023 en vejledning (et katalog) med primært forslag til sikkerhedsforanstaltninger, der er målrettet god rettighedsstyring.

Formålet med kataloget er at samle en række praktisk orienterede forslag til sikkerhedsforanstaltninger, der kan implementeres for at imødegå konkrete sikkerhedsmæssige problemområder. Kataloget indeholdt ved offentliggørelsen i alt 25 tekster med beskrivelse af tekniske og organisatoriske foranstaltninger, som både adresserer it-sikkerhedsmæssige tiltag og den juridiske ramme for gældende krav. Teksterne kan læses uafhængigt af hinanden og er bygget op som individuelle vejledningstekster med henvisning til både relevant praksis og andet relevant vejledningsmateriale fra både tilsynet og andre, som vejleder om it-sikkerhed.

Nye vejledninger om tv-overvågning

Tv-overvågning spiller en stadig større rolle, når det kommer til at bekæmpe og forebygge kriminalitet. Men der er tale om et komplekst område lovgivningsmæssigt, da der er regler i både tv-overvågningsloven, databeskyttelsesforordningen, databeskyttelsesloven og straffeloven, man skal iagttage for at sikre, at tv-overvågningen er lovlig.

Datatilsynet udgav derfor i løbet af 2023 tre nye vejledninger om tv-overvågning målrettet henholdsvis private virksomheder, offentlige myndigheder og boligorganisationer for at give et samlet overblik over reglerne på området, og hvad man særligt skal være opmærksom på, hvis man vil anvende tv-overvågning.

Vejledningerne, der blev udarbejdet med bidrag fra Justitsministeriet for så vidt angår de regler, som hører under politiet, beskriver bl.a., hvornår der er tale om tv-overvågning, hvor man må opsætte tv-overvågning, og hvordan man kan iagttage oplysningspligten over for de personer, som bliver tv-overvåget. Vejledningerne kommer også omkring emner som reglerne om opbevaring og videregivelse af optagelser, de registreredes rettigheder i forbindelse med tv-overvågning og brugen af databehandlere.

Fokus på uberettigede registeropslag

På baggrund af en række historier i pressen – og på baggrund af Datatilsynets egne sager – om offentligt ansattes og privatansattes uberettigede opslag i registre, opfordrede Datatilsynet i løbet af 2023 til særlig opmærksomhed vedrørende opslag i registre.

Datatilsynet gjorde opmærksom på, at mens mange mennesker har adgang til registre med personoplysninger gennem deres arbejde, så må man kun slå op i disse registre, hvis der er en saglig grund. Typisk fordi det er nødvendigt for at udføre arbejdsopgaverne. Datatilsynet gjorde i den forbindelse opmærksom på, at det gælder for alle, der har adgang til registre, herunder journalsystemer, kundekartoteker, CPR o.l., som indeholder personoplysninger. Det er således ikke kun personalet på hospitaler og lægehuse, men også kommunale sagsbehandlere, medarbejdere i skatteforvaltningen og f.eks. ansatte i et forsikringsfirma.

Man må ikke slå op, fordi man f.eks. er nysgerrig, eller fordi man vil bruge oplysningerne i privat sammenhæng. Normalt må man kun må slå op på personoplysninger, hvis det er nødvendigt for at kunne udføre arbejdet. Hvis man går ud over den grænse, kan man som ansat risikere at overtræde databeskyttelsesreglerne, og det kan i sidste ende føre politianmeldelse og bødestraf.

Samtidig oplyste Datatilsynet, at arbejdsgiverne også har et ansvar. Det er nemlig som udgangspunkt arbejdsgiveren, der er ansvarlig for de registeropslag, som deres ansatte foretager på arbejdet, og arbejdsgiveren har både et ansvar for at informere de ansatte om brugen af de registre, som er til rådighed, og for i et vist omfang at indrette registrene forsvarligt og føre kontrol med, hvad de ansatte slår op på.

Mens ansattes misbrug af adgangsrettigheder ikke i alle tilfælde kan forhindres, kan omfanget begrænses gennem systematisk rettighedsstyring, gode kontrolprocedurer og effektiv håndhævelse fra arbejdsgiverens side. Datatilsynet offentliggjorde i 2023 på den baggrund som nævnt ovenfor også et lille katalog over tiltag, man som organisation kan gøre brug af for at minimere risikoen for, at medarbejderne uberettiget slår op i registre. Hvis arbejdspladsen lever op til disse krav, og en ansat alligevel foretager opslag uden et sagligt formål, vil ansvaret kunne lande hos den ansatte selv.

Skriftlige forespørgsler til Datatilsynet

Som en del af Datatilsynets rådgivnings- og vejledningsindsats besvarer tilsynet hvert år også et betydeligt antal telefoniske og skriftlige forespørgsler. Herunder er gengivet eksempler på nogle af de skriftlige forespørgsler, som Datatilsynet har besvaret i 2023.

Kommunes hjemmel til AI-løsning

I november 2023 vurderede Datatilsynet efter anmodning fra Københavns Kommune, om kommunen havde hjemmel til udvikling, drift og gentræning af en AI-løsning, der kan identificere borgere med behov for vedligeholdende træning og rehabiliterende indsats.

Københavns Kommune ønskede at udvikle, idriftsætte og gentræne en AI-løsning med udgangspunkt i egne data, der stammer fra historiske sager om tilbud af træning og rehabiliterende indsats. AI-løsningen var tiltænkt som beslutningsstøtte til sagsbehandlere i kommunens sundheds- og omsorgsforvaltning og ville på baggrund af en statistisk analyse med relativt stor nøjagtighed identificere, hvilke borgere der kan gennemføre et træningsforløb, og hvem der vil få effekt af forløbet.

Datatilsynet vurderede, at udvikling, drift og gentræning af en sådan AI-løsning generelt kunne ske på baggrund af databeskyttelsesforordningens bestemmelse om myndighedsudøvelse (artikel 6, stk. 1, litra e) og forordningens bestemmelse om behandling nødvendig af hensyn til væsentlige samfundsinteresser (artikel 9, stk. 2, litra g). Begge bestemmelser forudsætter dog et såkaldt supplerende nationalt retsgrundlag.

Behandling af personoplysninger til udvikling, herunder gentræning, af løsningen kunne efter Datatilsynets vurdering ske med henvisning til de eksisterende bestemmelser i serviceloven, der forpligter kommunen til at træffe afgørelser om og levere vedligeholdende træning og rehabiliterende indsats.

Efter Datatilsynets opfattelse kan offentlige myndigheder inden for rammerne af den lovgivning, der forpligter eller berettiger offentlige myndigheder til at udføre en bestemt opgave, ofte designe, udvikle og teste AI-løsninger, som kan understøtte myndigheden i at varetage denne opgave.

Behandling af personoplysninger som led i driften af løsningen kunne imidlertid ikke ske inden for rammerne af disse bestemmelser, da der ikke var tale om et tilstrækkeligt klart retsgrundlag i lyset af, hvor indgribende en behandlingsaktivitet der er tale om.

Behovet for et tilstrækkeligt klart retsgrundlag var bl.a. begrundet i, at der ved brug af AI-løsninger, bl.a. som den omhandlede, ofte vil blive behandlet store mængder personoplysninger og følsomme oplysninger. Derfor har brug af AI som led i sagsbehandlingen, som det var tilfældet i denne sag, en betydning for, hvor klart det supplerende nationale retsgrundlag skal være. Det skyldes, at brug af AI bl.a. medfører, at AI-løsninger kan lære, finde sammenhænge og gennemføre sandsynlighedsanalyser og drage konklusioner langt ud over det, som en fysisk sagsbehandler ville være i stand til. Brug af AI i administrativ sagsbehandling er dermed grundlæggende forskellig fra den traditionelle menneskelige sagsbehandling, som har været normen hidtil. Endelig indebærer brug af AI-løsninger til beslutningsstøtte en risiko for, at medarbejderne tillægger løsningens vurdering af en sag større betydning end deres egen vurdering, hvilket udgør en yderligere risiko for borgeren.

Anvendelse af undtagelse til oplysningspligten

På grundlag af en henvendelse fra Uddannelses- og Forskningsstyrelsen vurderede Datatilsynet, at styrelsen ikke kunne undlade at oplyse forældre om, at oplysninger om deres indkomst behandles med henblik på bl.a. at udregne uddannelsesstøtte med henvisning til, at behandlingen af oplysningerne udtrykkeligt er fastsat i lovgivning.

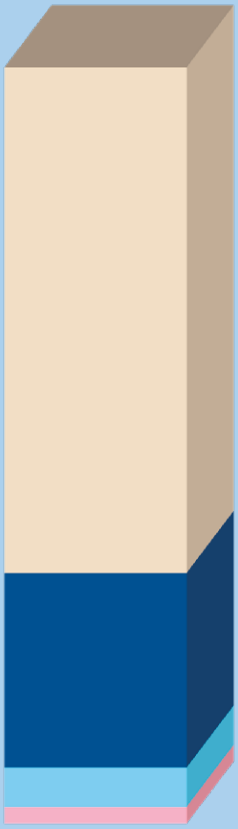
Datatilsynet udtalte, at der i kravet om udtrykkelighed ligger, at det ikke må give anledning til tvivl, hvorvidt det i lovgivningen er fastsat, at den dataansvarlige skal foretage indsamling eller videregivelse af oplysninger. Endvidere udtalte Datatilsynet, at der i kravet om udtrykkelighed ligger, at der skal være tale om en egentlig forpligtelse til at indsamle eller videregive oplysninger, ligesom det af denne forpligtelse skal fremgå, hvilke oplysninger der skal indsamles eller videregives. Det skyldes, at det i disse tilfælde vil være klart for den registrerede (gennem bekendtgørelse i Lovtidende), at der vil blive indsamlet eller videregivet oplysninger om vedkommende og hvilke oplysninger.

Det vil således ikke være tilstrækkeligt, at loven hjemler en mulighed for at indsamle eller videregive oplysninger, da det ikke efter en sådan bestemmelse vil være klart for de registrerede, at der vil blive registreret eller videregivet oplysninger og hvilke oplysninger.

Bestemmelserne i SU-lovens § 25, stk. 5 og stk. 6, sammenholdt med § 39, stk. 1, der efter sin formulering giver Uddannelses- og Forskningsstyrelsen mulighed for at indsamle en række forskellige oplysninger, herunder om indkomst- og formueforhold for den uddannelsessøgendes forældre, den ene forældres eventuelle ægtefælle, samlever eller registrerede partner og antallet af dennes børn under 18 år, gav efter Datatilsynets opfattelse ikke den tilstrækkelige klarhed for den registrerede over, om der indhentes oplysninger om vedkommende og i bekræftende fald, hvilke oplysninger, der er tale om.

Det var på baggrund heraf Datatilsynets vurdering, at SU-lovens § 25, stk. 5 og 6, og § 39, stk. 1, ikke i fornødent omfang kunne anses for ”udtrykkeligt at fastsætte indsamling/videregivelse” i overensstemmelse med databeskyttelsesforordningens artikel 14, stk. 5, litra c.

Høring over lovforslag mv.



688 sager i alt

460 Høringer over bekendtgørelser, cirkulærer, vejledninger, anordninger mv.

177 Høringer over betænkninger, lovforslag, EU-retsakter, konventioner mv.

36 Folketingsspørgsmål, private lovforslag, folketingsbeslutninger, høringer mv.

15 Forskelligt

*Der skal efter databeskyttelseslovens § 28 indhentes en udtalelse fra Datatilsynet ved udarbejdelse af lovforslag, bekendtgørelser, cirkulærer mv., der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger. Datatilsynet registrerede **688** sager i 2023 vedrørende høringer over lovforslag m.v.*

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

I det følgende er der gengivet nogle af de lovforslag, som har været sendt i høring hos Datatilsynet i 2023.

Ændring af sundhedsloven (Godkendelse af sundheds-apps)

I juni 2023 sendte Indenrigs- og Sundhedsministeriet et udkast til ændring af sundhedsloven i høring hos Datatilsynet. Lovforslaget handlede bl.a. om bedre mulighed for digital forældreadgang til børns helbredsoplysninger og om etablering af Nævnet for sundhedsapps.

Det fremgik af lovforslaget, at ministeren skulle kunne nedsætte et "Nævn for sundhedsapps", der skulle kunne vurdere og anbefale sundhedsapps. Der var lagt op til, at nævnet skulle vurdere sundhedsapps ud fra sundhedsfaglige parametre såsom evidens for effekt, brugervenlighed og værdi. Dette havde Datatilsynet ikke bemærkninger til. Men tilsynet bemærkede, at det var vigtigt, at når sundhedsapps blev godkendt, burde det udtrykkeligt anføres, at der i godkendelsesprocessen ikke var taget stilling til, om appen levede op til de databeskyttelsesretlige regler.

Dette var efter Datatilsynets opfattelse vigtigt, for at der ikke skulle kunne opstå tvivl hos borgere og sundhedspersoner om, hvorvidt en sundhedsapp var blevet vurderet i forhold til de databeskyttelsesretlige regler.

Datatilsynet opfordrede derfor til, at Indenrigs- og Sundhedsministeriets databeskyttelsesrådgiver blev involveret tidligt i processen, og inden der blev udviklet på en applikation, for at sikre at det var vurderet, hvordan løsningen skulle designes for at overholde databeskyttelsesreglerne. Datatilsynet henviste i den forbindelse til reglerne i databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design og indstillinger.

Datatilsynet gjorde samtidig opmærksom på, at det ikke er alle sundhedsfaglige forretningsidéer, der kan rummes inden for de databeskyttelsesretlige regler.

Ændring af databeskyttelsesloven

I september 2023 sendte Justitsministeriet et udkast til forslag til lov om ændring af databeskyttelsesloven i høring.

Lovforslaget indeholdt bl.a. et forslag om at ophæve lovens § 13, stk. 1-3 og 5-9, vedrørende behandling af personoplysninger i forbindelse med markedsføring. Justitsministeriet havde i forbindelse med udarbejdelsen af databeskyttelsesloven oprindelig vurderet, at lovens § 13 lå inden for rammerne af det såkaldte nationale råderum i databeskyttelsesforordningen, hvorefter medlemsstaterne inden for nærmere bestemte områder kan eller skal fastsætte nationale regler. På baggrund af en henvendelse fra Datatilsynet om, at tilsynet fandt det tvivlsomt, om denne vurdering var korrekt, genovervejede Justitsministeriet sin oprindelige vurdering og var herefter enig med Datatilsynet. Derfor blev det foreslået at ophæve de pågældende bestemmelser, hvilket Datatilsynet ikke havde bemærkninger til.

Lovforslaget indeholdt endvidere bl.a. forslag om tilpasning af oplysningspligten og indsigtsretten hos Procesbevillingsnævnet og Folketingets Ombudsmand. I forhold til Procesbevillingsnævnet udtalte Datatilsynet, at tilsynet havde noteret sig, at begrænsningen af de registreredes rettigheder var i overensstemmelse med de begrænsninger, der gælder for behandling af personoplysninger, der foretages for domstolene, når disse handler i deres egenskab af domstol, jf. databeskyttelseslovens § 22, stk. 4. I forhold til Folketingets Ombudsmand henviste Datatilsynet til et tidligere høringssvar fra 2022, hvor tilsynet havde anført nogle mere overordnede betragtninger vedrørende begrænsning af de registreredes rettigheder i forhold til indsigt i personoplysninger hos Folketingets Ombudsmand.

Lov om CO2-kvoter

I et forslag fra Energistyrelsen til lov om CO_2-kvoter fra oktober 2023 var der foreslået en bestemmelse om oplysningspligt, hvorefter der efter anmodning fra klima-, energi- og forsyningsministeren eller fra erhvervsministeren skulle være pligt for de virksomheder, som var omfattet af loven, til at afgive "enhver oplysning", som ministeren efter en rimelig vurdering anså for nødvendig til varetagelse af ministerens opgaver, "herunder opgaver i forbindelse med indhentning af oplysninger ved told- og skatteforvaltningen samt miljøoplysninger fra miljøministeriet".

Energistyrelsen havde anført i lovforslagets bemærkninger, at der var lagt op til, at der skulle gælde "en bred skønsmargen" for klima-, energi og forsyningsministeren og erhvervsministeren i forhold til, hvilke oplysninger der kunne indhentes, dog med den begrænsning at disse oplysninger skulle være relevante for at kunne administrere kvoteordningen.

Energistyrelsen var opmærksom på databeskyttelsesforordningens regler om underretning til registrerede personer, hvis der indhentes oplysninger om dem - i dette tilfælde oplysningspligten for det ministerium, som indhentede oplysningerne via den foreslåede pligt til at afgive oplysninger. Men Energistyrelsen pegede samtidig på den undtagelse til oplysningspligten, som findes i databeskyttelsesforordningens artikel 14, stk. 5, litra c. Efter den bestemmelse finder oplysningspligten ikke anvendelse, hvis indsamlingen "udtrykkeligt er fastsat i EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, og som fastsætter passende foranstaltninger til beskyttelse af den registreredes legitime interesser." Det var Energistyrelsens vurdering, at denne undtagelsesbestemmelse kunne bringes i anvendelse i de tilfælde, hvor pligten til at afgive oplysninger blev aktualiseret, således at der ikke ville være pligt til underretning.

Datatilsynet oplyste til Energistyrelsen, at lovforslagets bestemmelse om oplysningspligt ikke levede op til betingelserne i databeskyttelsesforordningen artikel 14, stk. 5, litra c, om, at indsamlingen skulle være "udtrykkelig fastsat". Det skyldtes, at lovforslaget efter tilsynets opfattelse ikke gjorde det klart for den registrerede, om og i givet fald under hvilke betingelser der ville blive indsamlet eller videregivet personoplysninger om vedkommende, herunder til hvem.

Ændring af lov om spil

Skatteministeriet sendte i november 2023 et udkast til ændring af lov om spil i høring hos Datatilsynet. Formålet med lovforslaget var bl.a. at styrke indsatsen mod matchfixing ved at indføre krav til udbydere af væddemål, der forpligtede udbyderne til at forebygge og bekæmpe matchfixing, ligesom spildata blev foreslået inddraget til at understøtte bekæmpelsen af matchfixing.

Udkastet indeholdt bl.a. bestemmelser om udveksling af oplysninger, herunder mellem Spillemyndigheden og tilladelsesindehavere. Lovforslaget indeholdt også en bestemmelse om, at Spillemyndigheden skulle have adgang til at behandle indsamlede data, herunder "til profilering, samkøring og videregivelse af data, til brug for opfyldelse af de i § 1 fastsatte formål." Det fremgik endvidere, at adgangen til at behandle indsamlede data også skulle gælde til brug for overholdelse af anden lovgivning.

Datatilsynet udtalte over for Skatteministeriet, at bestemmelsen kunne medføre en meget vid og generel hjemmel til behandling af personoplysninger. Tilsynet lagde derfor til grund, at ministeriet grundigt havde overvejet bestemmelsens proportionalitet, herunder om bestemmelsen indebar, at oplysninger indsamlet til ét formål ville kunne anvendes til et andet formål.

Datatilsynet anførte endvidere, at det burde uddybes i lovforslagets bemærkninger, hvad der mentes med "videregivelse af data" og hvornår – og under hvilket betingelser – oplysninger skulle kunne videregives.

Endelig anførte Datatilsynet, at de vide rammer for databehandling, som den foreslåede bestemmelse indebar, burde give anledning til, at der som led i Spillemyndighedens løbende myndighedsudøvelse foretages grundige overvejelser om bl.a. mængden og karakteren af de oplysninger, som anses for nødvendige at behandle for at forfølge et eller flere konkrete formål, samt om hvor længe indsamlede oplysninger vil være tilgængelige for Spillemyndigheden til at forfølge (nye) formål.

Tilsyn

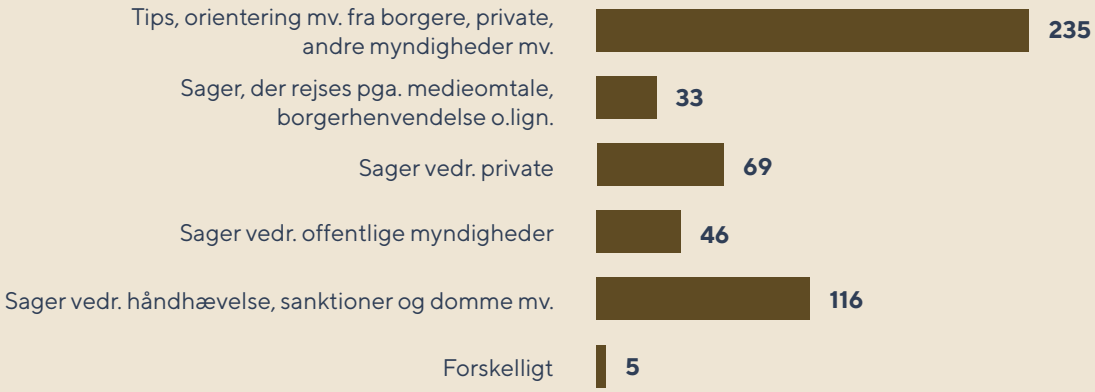
2.271 sager i alt

Klager

1.767

Sager på Datatilsynets eget initiativ

504



En vigtig opgave for Datatilsynet er at føre tilsyn med, at myndigheder, virksomheder og andre dataansvarlige og databehandlere overholder reglerne for databeskyttelse.

Tilsynsopgaven består i behandling af klagesager og generelle tilsynssager, som Datatilsynet enten fra begyndelsen af året har planlagt at gennemføre, eller som tilsynet i løbet af året beslutter at tage op af egen drift på baggrund af konkrete hændelser. Datatilsynet håndterer også løbende de mange brud på persondatasikkerheden, der hver uge bliver anmeldt til tilsynet.

Alle disse sager kan munde ud i forskellige former for sanktioner – herunder kritik, påbud, forbud og/eller en anmeldelse til politiet med en bødeindstilling.

*Datatilsynet har i 2023 indgivet **6** politianmeldelser med indstilling om bøde for overtrædelse af databeskyttelsesreglerne.*

Behandling af klage- og andre tilsynssager

Hidtil har en relativt stor del af Datatilsynets ressourcer gået til at iværksætte undersøgelse i de mange klagesager, som tilsynet modtager hvert år. Samtidig har der i tilsynet i de senere år været stort fokus på at rådgive og vejlede om databeskyttelsesreglerne, ligesom tilsynet har haft fokus på at sætte aftryk på national lovgivning og internationalt samarbejde. Datatilsynet har endvidere hvert år løbende taget sager op med udspring i tips, medieomtale o.l. Tilsynet har i samme periode ligeledes formået at øge antallet af generelle tilsynsaktiviteter i form af skriftlige og fysiske tilsyn, modenhedsanalyser og anvendelse af nyt tilsynskoncept, som er udviklet som led i den data- og risikobaserede strategi, som Datatilsynet udarbejdede og offentliggjorde i efteråret 2020.

Mens de målrettede tilsynsaktiviteter sætter fokus på nøje overvejede problemstillinger i udvalgte brancher og sektorer, har klagesagsbehandlingen i sagens natur i højere grad haft sit udspring i den enkelte borgers perspektiv. Klager har været og er fortsat en vigtig kilde til at få fokus på de rigtige problemstillinger, men en tilbundsgående undersøgelse af samtlige klager kan være på bekostning af andre sager, der er mere alvorlige og berører langt flere borgere – men som ikke nødvendigvis kommer til potentielle klageres kendskab. I løbet af 2022 besluttede Datatilsynet derfor at foretage en justering af kursen, så der i færre tilfælde sker en tilbundsgående undersøgelse af de enkelte klagesager - mens der bliver taget flere generelle sager op af egen drift. Disse sager udvælger Datatilsynet som hidtil ud fra bl.a. klager, brud på persondatasikkerheden, medieomtale og tips – og tilsynet styrker samtidig brugen af data for at kunne fokusere indsatsen på de områder, hvor der er tale om mange borgeres oplysninger, særligt beskyttelsesværdige oplysninger eller en høj risiko for borgerne.

Når det gælder klagesagerne, sker der nu en graduering af behandlingen af de enkelte klager, alt efter hvad der er relevant og formålstjenligt i den enkelte sag. Datatilsynet afslutter eksempelvis nogle klagesager ved at kontakte den dataansvarlige og orientere om klagen og de relevante regler, men ikke nødvendigvis gennemføre en omfattende og tidskrævende undersøgelse med høringer af parterne osv.

Med andre ord: I stedet for at undersøge et antal individuelle klagesager om indsigt fra kunder hos en bestemt virksomhed, kan Datatilsynet i stedet beslutte at tage en sag op af egen drift over for den pågældende virksomhed og spørge mere generelt ind til håndteringen af de registreredes rettigheder, herunder retten til indsigt. På denne måde løfter Datatilsynet med de samme ressourcer databeskyttelsen – ikke blot for de enkelte klagere, men for alle virksomhedens kunder, ligesom tilsynets undersøgelse kan få andre problemer frem i lyset.

One-Stop-Shop-mekanismen

Datatilsynet vurderer i forbindelse med sin behandling af klagesager, om klagen omhandler grænseoverskridende 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 næste afsnit følger en række eksempler på klage- og tilsynssager, som Datatilsynet i 2023 traf afgørelse i. For eksempler på anmeldelser af brud på persondatasikkerheden, som Datatilsynet i 2023 har truffet afgørelse i, henvises til afsnittet herom.

Brug af cookie walls

I februar 2023 traf Datatilsynet to principielle afgørelser vedrørende henholdsvis Gul og Gratis' og Jysk Fynske Mediers brug af såkaldte cookie walls på hjemmesider. Datatilsynet udgav i samme forbindelse et sæt generelle retningslinjer for brugen af sådanne samtykke-løsninger. Sagerne blev behandlet i Datarådet.

En cookie wall er en fremgangsmåde, hvor en virksomhed gør adgangen til sin hjemmeside eller tjeneste betinget af, at den besøgende giver sit samtykke til behandling af sine personoplysninger, oftest til brug for markedsføring. I nogle tilfælde gives den besøgende som et alternativ til samtykke mulighed for at få adgang til indholdet eller tjenesten mod betaling.

Datatilsynet fandt overordnet, at en fremgangsmåde, hvor indholdet på en hjemmeside kan tilgås mod enten at give samtykke til behandling af personoplysninger eller mod betaling, opfylder databeskyttelsesreglernes krav til et gyldigt samtykke.

I forhold til Gul og Gratis fandt tilsynet, at virksomheden tilbød et alternativ til at give samtykke i form af adgang mod betaling, og at betaling gav adgang til en tjeneste, der i vidt omfang var tilsvarende den tjeneste, som man kunne få adgang til gennem samtykke. Derudover var prissætningen af betalingsalternativet ikke urimelig høj, dvs. at prissætningen ikke var så høj, at den besøgende reelt og i praksis ikke havde et valg mellem betalingsalternativet og at give sit samtykke.

Datatilsynet fandt dog samtidig, at Gul og Gratis ikke havde påvist, at behandling af personoplysninger til statistiske formål også var en nødvendig del af alternativet, hvorfor virksomheden blev meddelt et påbud om at kunne påvise dette.

Med hensyn til Jysk Fynske Medier fandt Datatilsynet, at virksomhedens fremgangsmåde, hvor besøgende mod deres samtykke kunne få adgang til dele af indholdet på jv.dk eller alt indholdet på jv.dk ved at tegne et abonnement, ikke opfyldte kravene til et gyldigt samtykke. Det skyldtes, at den tilbudte tjeneste mod samtykke ikke i vidt omfang var tilsvarende den, der blev tilbudt mod betaling, hvorfor de besøgende dermed ikke reelt blev præsenteret for et frit valg.

Tilsvarende fandt Datatilsynet, at Jysk Fynske Medier ikke havde påvist, at behandling af personoplysninger til statistiske formål også var en nødvendig del af alternativet til betaling. Virksomheden blev derfor meddelt et påbud om at sikre, at samtykket fra de besøgende på jv.dk opfyldte kravene i databeskyttelses-forordningen, og om at kunne påvise dette. Det vil sige, at virksomheden enten skulle påvise, at statistiske formål var en nødvendig del af alternativet til betaling eller tilpasse samtykkeløsningen, så de besøgende kunne give særskilt samtykke til dette formål.

Fjernaflæsning af elmålere

Datatilsynet traf i februar 2023 afgørelse i en sag, hvor en række borgere havde klaget over Radius Elnet A/S' behandling af personoplysninger, idet virksomheden via fjernaflæste elmålere indsamlede personoplysninger om klagernes elforbrug i kWh på timebasis og herefter indberettede oplysningerne til Energinet. Radius er en netvirksomhed, dvs. en virksomhed, der driver distributionsnet til el i Danmark. I denne forbindelse indsamler Radius forbrugsdata hos elkunder, herunder klagerne, via fjernaflæste elmålere.

Datatilsynet fandt, at Radius' behandling af personoplysningerne var sket inden for rammerne af databeskyttelsesforordningen og de nationale særregler, der tilpasser anvendelsen af forordningen. Sagen blev behandlet i Datarådet.

Datatilsynet lagde vægt på, at det fremgik klart og præcist af det lovgrundlag, som Radius som netvirksomhed er underlagt, at Radius som netvirksomhed skal indsamle oplysninger om elforbrug mv. på timebasis og indberette oplysningerne til Energinet, og at det skal ske på en nærmere angiven måde.

Endvidere lagde Datatilsynet vægt på, at indsamling af oplysninger om elforbrug mv. med henblik på at sikre forsyningssikkerheden samt kvalitet og kapacitet i elnettet indgår som en integreret del af forpligtelsen om at stille fornøden transportkapacitet til rådighed og give adgang til transport af elektricitet i elforsyningsnettet, samt at sikre den tekniske kvalitet i nettet, som Radius er underlagt som netvirksomhed.
I den forbindelse bemærkede Datatilsynet, at oplysninger om elforbrug mv. som udgangspunkt ikke i sig selv udgør følsomme personoplysninger.

Med hensyn til spørgsmålet om databeskyttelse gennem design og gennem standardindstillinger vurderede Datatilsynet, at formålene med og hjælpemidlerne til den omhandlede behandling af personoplysninger, dvs. indsamling af oplysninger om elforbrug mv. på timebasis til brug afregnings- og systemdriftsformål, under alle omstændigheder senest var blevet fastlagt i december 2017, hvor den såkaldte flexafregning blev idriftsat af Energinet, hvorefter netvirksomhederne, herunder Radius, har været forpligtet til at indsamle og indberette de oplysninger om elforbrug mv. til datahubben. Der var dermed tale om en behandlingsaktivitet, der blev iværksat inden den 25. maj 2018, hvorfor databeskyttelsesforordningens krav om databeskyttelse gennem design og standardindstillinger ikke fandt anvendelse på behandlingsaktiviteten. Den omstændighed, at der (fortsat) er sket udskiftning af elmålere hos elkunder i perioden 25. maj 2018 til den 31. december 2020 kunne efter Datatilsynets opfattelse ikke føre til et andet resultat.

For så vidt angår spørgsmålet om proportionalitet fandt Datatilsynet efter en samlet vurdering, at der ikke var grundlag for at fastslå, at de behandlingsaktiviteter, som Radius foretog på baggrund af den nævnte retlige forpligtelse efter elforsyningsloven mv., var i strid med proportionalitetsprincippet i databeskyttelses-forordningen.

Datatilsynet lagde navnlig vægt på, at det fremgik klart og specifikt af lovgivningen, at netvirksomhederne, herunder Radius, er forpligtet til at kontrollere rigtigheden af de oplysninger, der indberettes til datahubben, og at denne kontrol forudsætter adgang til de konkrete måleværdier, der indsamles på timebasis.

Endvidere fandt Datatilsynet, at der ikke var grundlag for at tilsidesætte vurderingen af, at det var nødvendigt at kontrollere de individuelle måleværdier, som forudsat i lovgivningen, og at der ikke var grundlag for at fastslå, at der fandtes andre, mindre indgribende måder at behandle de omhandlede oplysninger, henset til det mål som forfølges.

Datatilsynet lagde endelig lagt vægt på, at den af klagerne foreslåede metode – efter klagernes egne oplysninger – ikke var egnet til at kontrollere de individuelle måleværdier, og at metoden alene gjorde det muligt at kontrollere rigtigheden af aggregerede måleværdier på månedsbasis.

Videregivelse af oplysninger til forskningsprojekt

Datatilsynet modtog en række henvendelser fra borgere, som var utilfredse med, at Rigspolitiet havde videregivet oplysninger om, at de havde modtaget en fartbøde, til Aalborg Universitet til brug for forskningsprojektet Intervention Against Speed Offenders (EASE). Forskningsprojektet handlede om at forebygge hastighedsovertrædelser i trafikken og skulle vise, om bilister fik færre fartbøder, hvis de efter at have fået en fartbøde gennemgik onlinelæring om trafiksikkerhed. En af henvendelserne til Datatilsynet var fra en borger, der havde gjort indsigelse mod et bødeforlæg, som afventede domstolenes behandling af sagen.

I marts 2023 traf Datatilsynet – efter at sagen var blevet behandlet i Datarådet – afgørelse i sagen. Datatilsynet fandt ikke grundlag for at tilsidesætte Rigspolitiets vurdering af, at Rigspolitiet kunne videregive oplysninger om bilisters overtrædelse af færdselsloven til Aalborg Universitet til brug for forskningsprojektet i medfør af databeskyttelseslovens § 10, stk. 1.

Datatilsynet fandt imidlertid grundlag for at udtale alvorlig kritik af, at Rigspolitiets videregivelse i den konkrete sag ikke var sket i overensstemmelse med principperne om formålsbegrænsning og dataminimering, da Rigspolitiets videregivelse ikke var sket til et sagligt og relevant formål. Datatilsynet lagde i den forbindelse vægt på, at det på tidspunktet for Rigspolitiets videregivelse fortsat måtte anses for at have formodningen imod sig, at den pågældende borger havde overtrådt færdselsloven, og at forskningsprojektets målgruppe efter Datatilsynets opfattelse var personer, der havde overtrådt færdselsloven.

Endvidere fandt Datatilsynet grundlag for at meddele Rigspolitiet påbud om at ophøre med at videregive oplysninger til Aalborg Universitet om borgere, som havde modtaget en fartbøde, men havde gjort indsigelse mod bødeforlægget, og hvor sagen endnu ikke var afgjort ved domstolene.

Brug af Facebook Business Tools

Datatilsynet modtog i slutningen af 2020 én af i alt 101 klager, som organisationen 'None of Your Business' (NOYB) havde sendt til flere europæiske datatilsyn. Klagerne vedrørte forskellige dataansvarliges brug af enten Google Analytics eller de såkaldte Facebook Business Tools på deres hjemmesider. I Datatilsynets tilfælde vedrørte klagen Boligportals behandling af klagers (repræsenteret af NOYB) personoplysninger ved virksomhedens brug af Facebook Business Tools på sin hjemmeside.

Facebook Business Tools udbydes af Meta og er værktøjer, der kan indlejres på en hjemmeside. Når en person besøger hjemmesiden, indsamler værktøjerne oplysninger om bl.a. personens IP-adresse, at personen har besøgt hjemmesiden, tidspunkt for besøget, øvrige oplysninger om bl.a. browser og operativsystem samt oplysninger om andre online-identifikatorer, der er blevet indsamlet via cookies.

Datatilsynet traf i april 2023 afgørelse i sagen. Datatilsynet fandt i den forbindelse, at tilsynet på baggrund af de indsamlede oplysninger ikke kunne træffe afgørelse om den mulige overførsel af personoplysninger til USA, idet der var uenighed blandt parterne om, hvorvidt personoplysninger om klager faktisk er blevet overført til USA. Dette gav dog Datatilsynet anledning til at undersøge, hvorvidt Boligportal havde overholdt sine forpligtelser efter databeskyttelsesforordningen, navnlig virksomhedens forpligtelse til at kunne påvise, at den overholder reglerne.

Datatilsynet konkluderede, at Boligportalen og Meta Irland måtte anses som fælles dataansvarlige for behandlingen af klagers personoplysninger. Datatilsynet fandt i den forbindelse grundlag for at udtale alvorlig kritik af, at Boligportal ikke kunne påvise en tilstrækkelig rolle- og ansvarsfordeling mellem Boligportal og Meta Ireland i lyset af den behandling af personoplysninger, der fandt sted, bl.a. ved, at der ikke forelå en ordning om rolle- og ansvarsfordelingen på tidspunktet for klagers besøg på Boligportals hjemmeside, som ellers er påkrævet ved fælles dataansvar.

Endvidere fremgik det ikke af ordningen, som efterfølgende blev indgået mellem Boligportal og Meta Ireland som fælles dataansvarlige, om personoplysninger om hjemmesidebesøgende blev behandlet ved brug af hjælpemidler eller databehandlere, der befandt sig uden for EU/EØS, og hvem der i givet fald var ansvarlig for at sikre, at reglerne om overførsler til usikre tredjelande blev overholdt. Datatilsynet meddelte endvidere påbud til Boligportal om at bringe behandlingen af personoplysninger i overensstemmelse med databeskyttelsesforordningen. Boligportal standsede som følge af påbuddet sin brug af Facebook Business Tools.

Sagen blev behandlet i samarbejde med de øvrige europæiske datatilsyn i den såkaldte Taskforce 101 i regi af Det Europæiske Databeskyttelsesråd (EDPB).

Tilsyn med Statens Serum Instituts opfyldelse af oplysningspligten

Datatilsynet iværksatte i 2023 på baggrund af en borgerhenvendelse en sag af egen drift med Statens Serum Instituts (SSI) opfyldelse af oplysningspligten i følgende tilfælde:

- når SSI modtager blodprøver mv. fra regionerne med henblik på analyse, og
- når SSI beslutter at gemme restmateriale i Danmarks Nationale Biobank.

SSI oplyste, at selv om instituttet kunne underrette registrerede ved brug af digital eller fysisk post, ville dette kræve en uforholdsmæssigt stor indsats i form af store administrative og økonomiske omkostninger. I den forbindelse henviste SSI bl.a. til, at instituttet behandlede oplysninger om et stort antal registrerede, at instituttet ikke havde et system, som kunne foretage automatisk underretning af de registrerede, og at instituttet havde etableret visse kompensatoriske foranstaltninger ved at oplyse om behandlingen på sin hjemmeside og på Danmarks Nationale Biobanks hjemmeside.

Datatilsynet fandt – efter behandling af sagen i Datarådet – at SSI ikke kunne undlade at opfylde sin oplysningspligt med henvisning til, at det ville kræve en uforholdsmæssigt stor indsats. Tilsynet lagde i den forbindelse bl.a. vægt på, at oplysningspligten er central for at sikre gennemsigtighed ved behandling af personoplysninger og for skabe et tillidsforhold mellem den dataansvarlige og de registrerede.

Derudover bemærkede Datatilsynet, at det er en forudsætning for at undlade at opfylde sin oplysningspligt med henvisning til, at det vil kræve en uforholdsmæssigt stor indsats, at den uforholdsmæssigt store indsats er foranlediget af eller forbundet med den omstændighed, at oplysningerne ikke er indsamlet hos den registrerede. I så fald vil den dataansvarlige være i en anden og – efter omstændighederne – mindre velegnet position til at underrette en registreret end en dataansvarlig, som har indsamlet oplysningerne direkte fra den registrerede.

SSIs vanskeligheder med at opfylde oplysningspligten var imidlertid ikke foranlediget af den omstændighed, at SSI ikke havde indsamlet oplysningerne direkte fra de registrerede. Vanskelighederne skyldtes derimod, at instituttet ikke havde indrettet sit system på en sådan måde, at processen i forbindelse med opfyldelse af oplysningspligten lettedes, eksempelvis ved brug af automatiserede processer.

Efter anmodning fra Datatilsynet sendte SSI efterfølgende redegørelser for, hvad instituttet ville foretage sig med henblik på at opfylde oplysningspligten.

Tilsyn med kommuners og bankers håndtering af brud på persondatasikkerheden

I 2023 afsluttede Datatilsynet tilsyn med otte kommuners og otte bankers håndtering af brud på persondatasikkerheden. Tilsynene var tilrettelagt således, at kommunerne og bankerne blev inddelt i to grupper – dem, der havde anmeldt henholdsvis flest og færrest brud i forhold til henholdsvis kommunens indbyggertal og antal.

For gruppen med flest anmeldte brud på persondatasikkerheden fokuserede tilsynene bl.a. på, om kommunerne og bankerne havde truffet passende sikkerhedsforanstaltninger med henblik på at nedbringe antallet af brud på persondatasikkerheden, hvor der var sket uautoriseret videregivelse af personoplysninger i forbindelse med fremsendelse af oplysninger til bl.a. borgere, myndigheder mv., herunder i relation til borgere med navne- og adressebeskyttelse og økonomiske oplysninger.

Datatilsynet fandt på det foreliggende grundlag, at alle de dataansvarlige havde truffet passende sikkerhedsforanstaltninger. Datatilsynet lagde ved vurderingen heraf vægt på, at:

- Der var udarbejdet procedurer mv. og gennemført aktiviteter med henblik på at uddanne medarbejderne i databeskyttelse, herunder med henblik på at de er opmærksomme på, at der ikke sker utilsigtet videregivelse af personoplysninger til en forkert modtager.
- De havde gjort sig overvejelser og løbende indført både tekniske og organisatoriske foranstaltninger i forlængelse af passerede brud på persondatasikkerheden for at udgå lignende brud.
- Der var stort fokus på at undgå utilsigtet videregivelse af fortrolige oplysninger, hvilket både understøttes ved hjælp af forretningsgange, løbende vejledning mv. og systemmæssige tiltag mv.

For gruppen med færrest anmeldte brud på persondatasikkerheden fokuserede tilsynene på, om kommunerne og bankerne foretager anmeldelse af og dokumenterer brud på persondatasikkerheden i overensstemmelse med kravene i databeskyttelsesforordningen, herunder deres processer for håndtering og registrering af brud på persondatasikkerheden.

Datatilsynet fandt, at alle de dataansvarlige overordnet set havde vedtaget passende procedurer og retningslinjer mv. og havde gennemført passende uddannelsesaktiviteter, som kunne understøtte overholdelsen af kravene i databeskyttelsesforordningen om anmeldelse af brud på persondatasikkerheden. Dermed kunne de sikre, at brud på persondatasikkerheden opfanges i organisationen, sådan at disse kan blive vurderet med henblik på, om bruddet skal anmeldes til Datatilsynet, ligesom der kan foretages dokumentation af bruddene, herunder bl.a. begrundelsen herfor, hvis de ikke anmeldes til Datatilsynet.

Datatilsynet bemærkede dog i forhold til alle tilsynene, at Datatilsynet ikke som led i tilsynet havde haft lejlighed til at tage konkret stilling til, om alle relevante medarbejdere har gennemført de pågældende uddannelsesaktiviteter, og at tilsynet ikke var bekendt med det fulde indhold af uddannelsesmaterialet, herunder indholdet af f.eks. løbende awareness-indsatser.

Herudover udtalte Datatilsynet, at reglen om, at den dataansvarlige skal dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger, bl.a. skal sikre, at Datatilsynet skal kunne kontrollere, at bestemmelsen om anmeldelse af brud

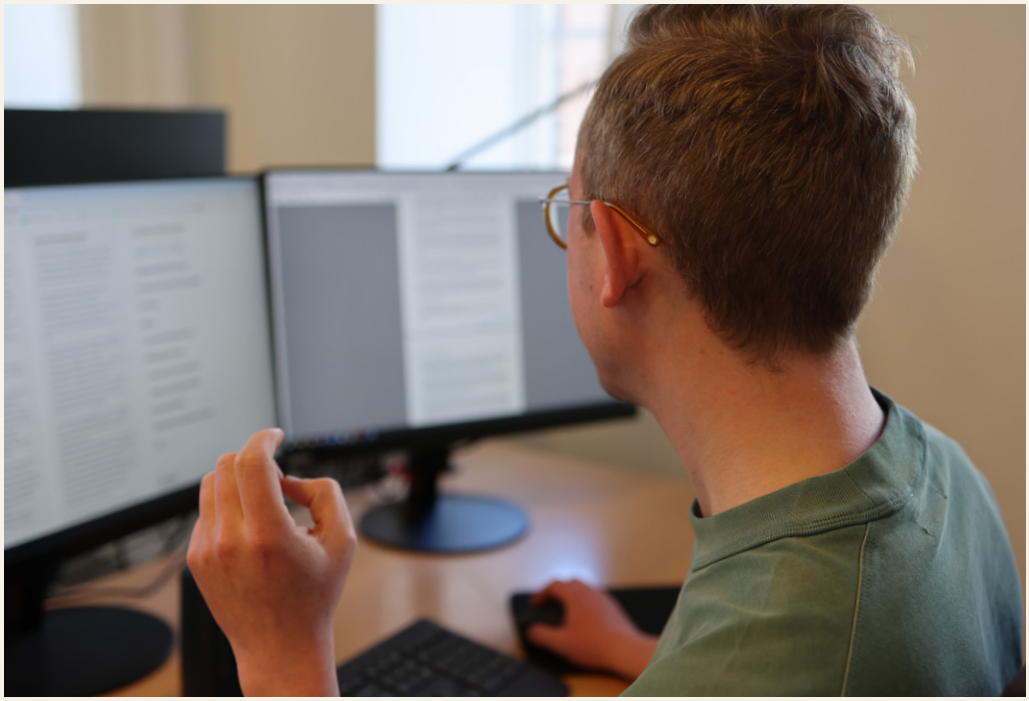
på persondatasikkerheden er overholdt. Den dataansvarlige bør derfor dokumentere sine begrundelser for alle væsentlige beslutninger, der træffes som følge af bruddet. Dette gælder ikke mindst, hvis den dataansvarlige efter at have vurderet bruddet er nået frem til, at det ikke skal anmeldes til Datatilsynet. Dokumentationen bør i relation til denne beslutning omfatte en nærmere redegørelse for, hvorfor den dataansvarlige mener, at bruddet sandsynligvis ikke vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder.

Datatilsynet udtalte kritik i to af tilsynssagerne, hvor to af de dataansvarlige – begge kommuner – ikke havde dokumenteret alle brud på persondatasikkerheden.

I den ene sag udtalte Datatilsynet alvorlig kritik af, at Roskilde Kommune ikke havde dokumenteret, hvor mange brud på persondatasikkerheden kommunen havde konstateret i perioden fra den 25. maj 2018 til september 2019, og at kommunen ikke kunne dokumentere, hvorvidt de registrerede sikkerhedshændelser siden september 2019 udgjorde egentlige brud på persondatasikkerheden.

I den anden sag udtalte Datatilsynet kritik af, at Frederikshavn Kommune ikke havde dokumenteret, hvor mange brud på persondatasikkerheden kommunen havde konstateret i 2018.

Datatilsynet anførte, at listen over brud – udover at tjene som dokumentation over for Datatilsynet – også bør bruges af den dataansvarlige til bl.a. at få overblik over, hvilke brud der typisk sker i organisationen og til på den baggrund at overveje, om der ud fra en risikovurdering er behov for at iværksætte nye eller supplerende foranstaltninger for at undgå eller nedbringe risikoen yderligere brud. Datatilsynet bemærkede, at det også fremgik af de modtagne høringssvar, at flere af de dataansvarlige aktivt anvender listerne til dette formål.



Særlige fokusområder for Datatilsynets tilsynsaktiviteter i 2023

Datatilsynets aktiviteter i 2023 omfattede blandt andet vejledning, rådgivning, klagesagsbehandling, internationalt arbejde og målrettede tilsynsaktiviteter. Ligesom tidligere år offentliggjorde Datatilsynet i januar måned en oversigt over de temaer, som især var i fokus for de målrettede tilsynsaktiviteter:

Beskyttelse af børn
Datatilsynet vil i 2023 have fokus på beskyttelse af oplysninger om børn. Datatilsynet vil i den forbindelse bl.a. fortsætte med at føre tilsyn med tv-overvågning på døgninstitutioner og lignende. Tilsynene vil primært være rettet mod behandling af oplysninger om de anbragte børn og unge, men også fokusere på oplysninger om medarbejderne, herunder oplysningspligt.

Databeskyttelsesrådgivere – udpegning og rolle
Det Europæiske Databeskyttelsesråd (EDPB) vedtog i oktober 2020 en koordinerede håndhævelsesramme (Coordinated Enforcement Framework (CEF) med det formål at koordinere fælles aktiviteter mellem de europæiske tilsynsmyndigheder og derved harmonisere og styrke håndhævelsen af GDPR. Den første fælles indsats blev iværksat i 2022 og omhandlede offentlige myndigheders brug af cloudservices. EDPB har besluttet, at den fælles indsats i 2023, som Datatilsynet vil deltage i, kommer til at handle om udpegning af databeskyttelsesrådgivere og deres rolle.

Behandling af personoplysninger hos fremstillingsvirksomheder med fokus på specialfremstillede produkter med levering direkte til borgerne
I 2023 vil Datatilsynet føre tilsyn med en række virksomheder, som fremstiller hjælpemidler og andre produkter, som leveres direkte til borgerne efter rekvisition fra kommuner, hospitaler mv., og som i den forbindelse behandler særligt beskyttelsesværdige oplysninger, herunder følsomme oplysninger om de pågældende borgere. Tilsynene vil navnlig være fokuseret på virksomhedernes opbevaring og eventuelle videregivelse af oplysninger, dataminimering og behandlingssikkerhed.

Dette fokusområde er udvalgt for også at undersøge brancher, som ikke tidligere har været genstand for tilsynsaktiviteter og som heller i øvrigt har været genstand for tilsynets opmærksomhed på baggrund af mange klagesager eller anmeldte sikkerhedsbrud mv., men hvor der f.eks. behandles oplysninger om et stort antal borgere, særligt beskyttelsesværdige oplysninger, eller hvor der er tale om en høj risiko for borgerne.

Folketinget og Folketingets institutioner
I modsætning til, hvad der var gældende efter den tidligere persondatalov, er Folketinget og de institutioner, der hører under Folketinget, omfattet af reglerne i databeskyttelsesforordningen og databeskyttelsesloven. Dog finder forordningen og loven ikke anvendelse på behandling af oplysninger, der foretages som led i Folketingets parlamentariske arbejde.

Datatilsynet vil i 2023 føre tilsyn med en af disse institutioner, der ikke tidligere har været underlagt tilsynets kompetence.

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 2021/2022, har Datatilsynet for at fastholde fokus på området besluttet også i 2023 at iværksætte tilsyn inden for dette felt.

TV-overvågning
Ud over tilsyn med behandling af personoplysninger i forbindelse med tv-overvågning af anbragte børn og unge vil Datatilsynet i 2023 føre tilsyn med parkeringsselskabers brug af tv-overvågning i forbindelse med udstedelse af parkeringsafgifter.

Tilladelser til at videregive oplysninger fra forskning
Efter databeskyttelseslovens § 10, stk.1, må følsomme oplysninger og oplysninger om strafbare forhold behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne. Efter § 10, stk. 2, må de oplysninger, der er omfattet af stk. 1 – og oplysninger, som alene foretages i statistisk eller videnskabeligt øjemed efter databeskyttelsesforordningens artikel 6 – ikke senere behandles i andet end videnskabeligt eller statistisk øjemed.

Personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2, må alene videregives – f.eks. til et andet forskningsinstitut – med henblik på modtagerens udførelse af en undersøgelse i statistisk eller videnskabeligt øjemed af væsentlig samfundsmæssig betydning.

Der skal som udgangspunkt ikke indhentes tilladelse hos Datatilsynet til videregivelse af sådanne personoplysninger. Dog skal Datatilsynets forudgående tilladelse til videregivelse indhentes i følgende tre tilfælde:

- når videregivelsen sker til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde
- når videregivelsen vedrører biologisk materiale
- når videregivelsen sker med henblik på offentliggørelse af oplysninger i anerkendte videnskabelige tidsskrifter eller lignende.

I forbindelse med meddelelse af tilladelse efter § 10, stk. 3, fastsætter Datatilsynet en række vilkår.

Datatilsynet har besluttet i 2023 at føre tilsyn med, om de vilkår, som Datatilsynet har fastsat i forbindelse med en række tilladelser efter § 10, stk. 3, bliver overholdt.

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 2023 at føre tilsyn med en række myndigheders behandling af personoplysninger i forbindelse med anvendelsen af flere 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 2023 valgt at føre tilsyn med de retshåndhævende myndigheders overholdelse af en række af lovens bestemmelser.

Tilsyn med behandling af personoplysninger i Kørekort-appen

Datatilsynet undersøgte i 2023, om Digitaliseringsstyrelsen overholdt princippet om dataminimering i forbindelse med administrationen og driften af det digitale kørekort. Det digitale kørekort er et elektronisk supplement til det fysiske kørekort, som brugerne kan have på deres telefoner via en kørekort-app.

Datatilsynets undersøgelse viste, at i forbindelse med driften af det digitale kørekort modtog Digitaliseringsstyrelsen oplysninger om alle kørekortindehavere fra kørekortregisteret. Ud af de ca. 4 mio. borgere, der har gyldigt kørekort, var det dog kun ca. 1,7 mio., som havde tilmeldt sig det digitale kørekort. Digitaliseringsstyrelsen opbevarede dog kørekortoplysninger om alle ca. 4 mio. kørekortindehavere, og spørgsmålet var derfor, om Digitaliseringsstyrelsen behandlede personoplysninger om flere mennesker end nødvendigt.

I forbindelse med undersøgelsen oplyste Digitaliseringsstyrelsen bl.a., at fordi kørekortregisteret er et ældre mainframe-system, var der ikke andre muligheder, end at Digitaliseringsstyrelsen modtog et udtræk af kørekortregisteret omfattende oplysninger om alle borgere, der har et gyldigt kørekort. Og for at Digitaliseringsstyrelsen skulle kunne tilbyde hurtig tilmelding for nye brugere af kørekort-appen, var styrelsen også nødt til at være i besiddelse af oplysninger om alle.

Efter forelæggelse af sagen for Datarådet fandt Datatilsynet, at det var i strid med dataminimeringsprincippet, at Digitaliseringsstyrelsen behandlede personoplysninger om over 2 mio. borgere, som ikke havde tilsluttet sig Kørekort-appen. Datatilsynet udtalte derfor alvorlig kritik af Digitaliseringsstyrelsen og meddelte styrelsen et forbud mod at behandle oplysninger om borgere, som ikke havde tilmeldt sig ordningen.

Det følger af Datatilsynets afgørelse, at Digitaliseringsstyrelsen kun må behandle personoplysninger om de borgere, som faktisk har tilsluttet sig Kørekort-appen.

Offentliggørelse af oplysninger (patientbilleder) på Instagram

Datatilsynet traf i 2023 afgørelse i en sag om Aarhus Universitetshospitals brug af Instagram til at offentliggøre billeder af patienter.

Region Midtjylland oplyste i forbindelse med sagen, at billederne blev offentliggjort på baggrund af et indhentet skriftligt samtykke med det formål at informere omverdenen om hospitalets virke og give generel sundhedsoplysning, ligesom opslagene blev delt med det formål at rekruttere nye medarbejdere.

Efter behandling af sagen i Datarådet fandt Datatilsynet, at Region Midtjylland i den konkrete situation ikke kunne anvende samtykke som behandlingsgrundlag til offentliggørelse af billeder af patienter. Datatilsynet lagde i den forbindelse vægt på det ulige forhold mellem patienten og regionen/hospitalet og den særlige situation, man befinder sig i som patient på et hospital.
Datatilsynet fandt endvidere, at Region Midtjyllands behandling af oplysninger om patienter på Instagram ikke var i overensstemmelse med de grundlæggende principper for behandling af personoplysninger.

Datatilsynet udtalte på den baggrund alvorlig kritik, ligesom tilsynet udstedte et påbud til Region Midtjylland om at slette opslag indeholdende helbredsoplysninger om patienter fra Instagramkontoen.

Efterfølgende bekræftede Region Midtjylland, at regionen have imødekommet Datatilsynets påbud. Region Midtjylland oplyste endvidere, at regionen var gået i gang med en proces vedrørende gennemgang af øvrige profiler på sociale medier.

Rigsrevisionens indsamling af personoplysninger

Rigsrevisionen er en uafhængig institution under Folketinget og er en del af den parlamentariske kontrol i Danmark. Rigsrevisionen har til opgave at undersøge, om statsregnskabet er rigtigt (finansiel revision). Herudover undersøger Rigsrevisionen i forbindelse med revisionen og de større undersøgelser, om statslige myndigheder og andre statsligt finansierede styrelser og virksomheder overholder gældende love og regler (juridisk-kritisk revision) og forvaltes sparsommeligt, produktivt og effektivt (forvaltningsrevision).

Datatilsynet behandlede i 2023 en sag om Rigsrevisionens behandlingsgrundlag til at indhente personoplysninger, når Rigsrevisionen udfører sin revisionsvirksomhed, og hvorledes Rigsrevisionen i den forbindelse sikrer overholdelse af princippet om dataminimering.

Datatilsynet fandt, at Rigsrevisionen har hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, til at indhente personoplysninger, når Rigsrevisionen udfører sin revisionsvirksomhed, jf. reglerne i rigsrevisorloven, herunder lovens § 12, stk. 1.

Datatilsynet fandt endvidere, at Rigsrevisionens indhentelse af personoplysninger, når Rigsrevisionen udfører sin revisionsvirksomhed, sker inden for rammerne af databeskyttelsesforordningens artikel 5, stk. 1, litra c.

Datatilsynet lagde i den forbindelse vægt på bl.a., at ansatte i Rigsrevisionen er instrueret i at begrunde og dokumentere, hvis der skal indhentes personoplysninger. De ansatte er også instrueret i at gå i dialog med den reviderede myndighed for at sikre overholdelse af forpligtelsen til dataminimering, herunder undgå at modtage f.eks. cpr-oplysninger eller andre personhenførbare oplysninger hvis det ikke har betydning for revisionen.

Datatilsynet lagde endvidere vægt på bl.a., at beslutning om, hvorvidt regnskabsoplysninger mv. skal tilgås via terminaladgang, sker ud fra flere hensyn, herunder "databeskyttelse – i forbindelse med overførsel og opbevaring af data" og "princippet om dataminimering – dvs. at få så få data ind som muligt".

Tilsyn med kommuner om sikkerheden i AULA

I 2023 traf Datatilsynet afgørelse i fem tilsynssager vedrørende behandlingssikkerheden i AULA. Alle fem kommuner fik enten kritik eller alvorlig kritik i den del af sagerne, der omhandlede konsekvensanalyse. To af kommunerne fik alvorlig kritik for ikke at have udarbejdet en konsekvensanalyse. Datatilsynet meddelte endvidere disse to kommuner et påbud om at udarbejde en konsekvensanalyse inden for tre måneder. De tre øvrige kommuner havde udarbejdet konsekvensanalyser. Datatilsynet vurderede imidlertid, at ingen af dem opfyldte alle mindstekravene til en konsekvensanalyse.

Derudover havde Datatilsynet undersøgt tidspunktet for udarbejdelsen af konsekvensanalyserne og i den forbindelse taget i betragtning, at der havde været uklarhed om dataansvaret for behandlingen af personoplysninger i AULA. Alle tre kommuner havde først udarbejdet konsekvensanalyserne lang tid efter, at klarhed om dataansvaret for behandlingen af personoplysninger i AULA var etableret. To af kommunerne havde tilmed først udarbejdet konsekvensanalyser, efter at tilsynet havde anmodet om materialet i forbindelse med iværksættelsen af tilsynet, hvorfor Datatilsynet overfor disse to kommuner udtalte alvorlig kritik

Samtlige fem kommuner fik ligeledes enten kritik eller alvorlig kritik i forhold til den del af sagerne, der omhandlede kommunernes forudgående risikovurdering. Kritikken vedrørte dokumentationskravet for at kunne påvise, at de havde identificeret og nedbragt de risici, som behandlingen af personoplysninger i AULA udgør for de personer, oplysningerne vedrører, så der er sikret et passende sikkerhedsniveau. Derudover vedrørte kritikken manglende identifikation og implementering af relevante foranstaltninger for at sikre et passende sikkerhedsniveau.

Datatilsynet udtalte alvorlig kritik af to af kommunerne, da de ikke havde fremsendt egentlige risikovurderinger. De øvrige tre kommuner havde fremsendt risikovurderinger. Datatilsynet udtalte dog kritik til disse kommuner, da de ikke i fuldt tilstrækkeligt omgang havde påvist, at de havde sikret et passende sikkerhedsniveau.

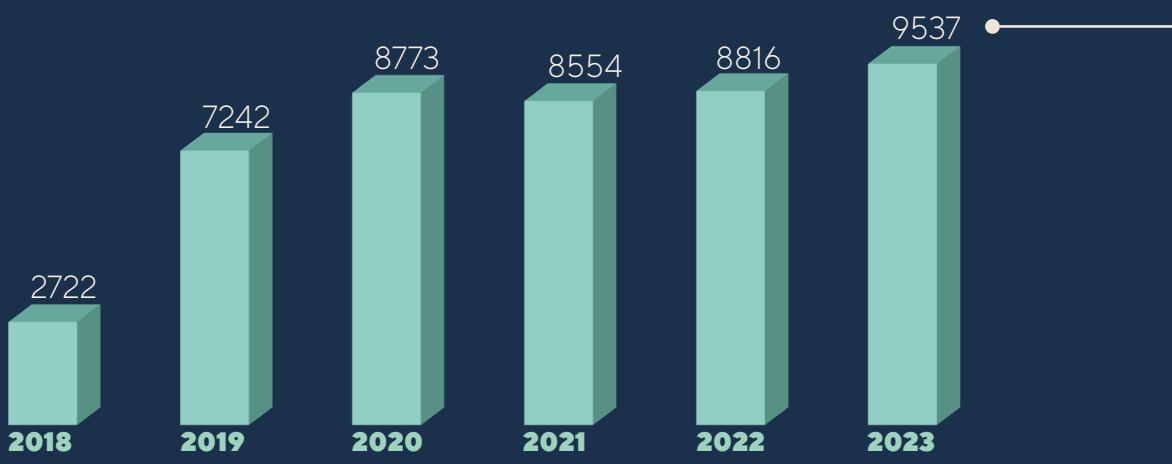
Datatilsynet fandt, at tilsynssagerne rejste nogle generelle databeskyttelsesretlige problemstillinger på tværs af kommunerne, som med fordel kunne håndteres samlet fremfor særskilt hos de enkelte kommuner.

På denne baggrund valgte Datatilsynet at orientere Kommunernes Landsforening (KL), Styrelsen for It og Læring og Kombit A/S (herefter KOMBIT) om tilsynets afgørelser, ligesom Datatilsynet også orienterede alle landets øvrige kommuner om afgørelserne. Datatilsynet opfordrede til, at det overvejes på tværs af kommunerne, eventuelt i samarbejde med KL og KOMBIT, at udarbejde en fælles konsekvensanalyse vedrørende kommunernes behandling af personoplysninger i AULA. Datatilsynet anbefalede endvidere, at KL, i samarbejde med kommunerne og eventuelt KOMBIT, overvejer muligheden for at udarbejde et adfærdskodeks i overensstemmelse med databeskyttelsesforordningens artikel 40 vedrørende kommunernes behandling af personoplysninger i AULA. På baggrund af en gennemgang af anmeldte brud på persondatasikkerheden fra kommuner relateret til AULA fandt Datatilsynet endvidere anledning til at anbefale, at KOMBIT sammen med de dataansvarlige kommuner foretager en undersøgelse af, om det er muligt at gennemføre en eller flere tekniske foranstaltninger for at mindske risikoen for fejlfremsendelse i AULA og en undersøgelse af mulighederne for at indrette beskedfunktionen på en måde, der mindsker en sådan risiko.

Anmeldelser af

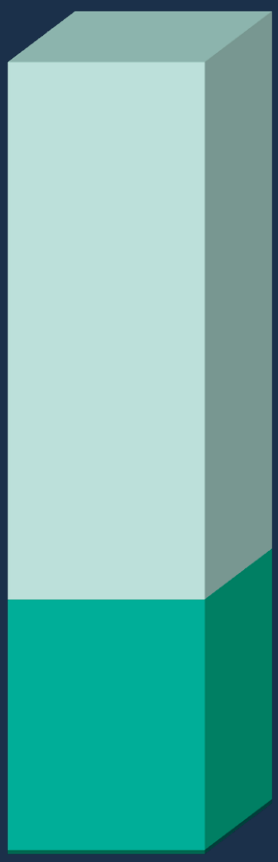
brud på persondatasikkerheden

*Datatilsynet modtager hvert år en stor mængde anmeldelser af brud på persondatasikkerheden. I 2023 blev der anmeldt **9.537** brud på persondatasikkerheden, hvilket er 721 flere anmeldelser end i 2022 og samtidig det hidtidig højeste antal, siden anmeldelsespligten blev indført i maj 2018.*



Fordelingen af anmeldelser af brud på persondatasikkerheden i 2023

9537 brud i alt*



6471 Anmeldelser fra offentlige myndigheder

3018 Anmeldelser fra private

48 Forskelligt

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

Mere videndeling om brud på persondatasikkerheden

Hvert år modtager Datatilsynet flere tusinde anmeldelser om brud på persondatasikkerheden. I marts 2023 lancerede tilsynet første version af et datavarehus, der skal bidrage til bedre videndeling om, hvilke brud der anmeldes og hvilke sektorer bruddene berører. Initiativet er et led i den Nationale Cyber- og Informationssikkerhedsstrategi. Datavarehuset er tilgængelig via Datatilsynets hjemmeside.

Denne viden er afgørende for Datatilsynet, fordi den gør det muligt bedre at vurdere, hvor der kan være behov for mere vejledning eller et tættere tilsyn. Initiativet gør det endvidere muligt for omverdenen at drage nytte af de mange data som led i forebyggelse af brud på persondatasikkerheden og opnå bedre databeskyttelse.

Datatilsynet har i forbindelse med etableringen af datavarehuset været i dialog med væsentlige interessenter om løsningen, herunder bl.a. Center for Cybersikkerhed og Erhvervsstyrelsen.

Nogle data kan dog ikke udstilles i den detaljegrad, som Datatilsynet egentlig har til rådighed. Det skyldes blandt andet, at statistikken af hensyn til sikkerhed og databeskyttelse ikke må vise noget, der går for tæt på de enkelte virksomheder eller brancher.

Det er dog tilsynets ambition, at detaljegraden løbende – inden for rammerne af disse hensyn – med tiden kan øges, herunder i relation til for eksempel geografisk fordeling. Datatilsynet har således allerede siden lanceringen forøget detaljegraden i forhold til de hændelsestyper, der vedrører utilsigtede hændelser, og som udgør størstedelen af de anmeldte sikkerhedsbrud.

Ny måde at kategorisere brud på persondatasikkerheden

Når Datatilsynet screener og visiterer de modtagne anmeldelser af brud på persondatasikkerheden, bliver hver enkelt anmeldelse - og dermed hver hændelse - kategoriseret som en eller flere hændelsestyper af tilsynets it-sikkerhedskonsulenter. På den måde kan tilsynet løbende bevare et overblik over, hvilke brud på persondatasikkerheden der anmeldes, og hvorfor de opstår.

Datatilsynet påbegyndte kategoriseringen af brud i hændelsestyper i april 2020. I forbindelse med udviklingen af Datatilsynets datavarehus udvidede Datatilsynet i januar 2023 taksonomien for kategorisering af brud. Den nye taksonomi bygger i vidt omfang på trusselstaksonomi fra 2016 fra Den Europæiske Unions Agentur for Cybersikkerheds (ENISA), og kategoriseringen indebærer derfor, at bruddene kategoriseres i hændelsestyper, der beskriver, hvilken type af trussel eller risiko der er relevant i forhold til bruddet. Datatilsynet valgte denne model, da statistikken primært har et forebyggende sigte.

Med den nye taksonomi udvider Datatilsynet antallet af hændelsestyper fra 10 til 64. Selvom ikke alle data af hensyn til sikkerhed og databeskyttelse kan udstilles i datavarehuset i den detaljegrad, som Datatilsynet egentlig har til rådighed, vil den nye kategorisering på sigt betyde, at Datatilsynet vil få et mere detaljeret indblik i, hvad der forårsager brud på persondatasikkerheden. Den nye kategorisering skal samtidigt gøre det muligt hurtigere at give målrettet vejledning til de dataansvarlige, efter et brud er anmeldt, jf. næste afsnit.

Vejledning i tilknytning til anmeldelse af brud på persondatasikkerheden

Datatilsynet lancerede i oktober 2023 en ny service kaldet "Ugens sikkerhedstip". Servicen går ud på, at Datatilsynet via tilsynets hjemmeside og LinkedIn-virksomhedsprofil løbende offentliggør aktuelle tips til, hvad man kan gøre for at undgå en række af de brud på persondatasikkerheden, som bliver anmeldt til tilsynet.

Oktober måned blev samtidig startskuddet til et mere omfattende vejledningsinitiativ, som indebærer, at Datatilsynet straks i forbindelse med den indledende sagsbehandling af de anmeldelser af brud på persondatasikkerheden, som tilsynet har modtaget, vurderer, om den dataansvarlige som følge af bruddet kan have behov for målrettet vejledning om specifikke tekniske og organisatoriske foranstaltninger, hvorefter sådan vejledning sendes til de dataansvarlige som en del af tilsynets kvitteringsbrev.

Målet er at sikre hurtig og anvendelig hjælp til de dataansvarlige, der oplever et brud på persondata-sikkerheden og nu skal overveje, hvordan de sikrer, at et lignende brud ikke sker igen. Alt efter persondatasikkerhedsbruddets karakter kan det både være Datatilsynets egne vejledninger og informationstekster eller vejledninger fra andre relevante myndigheder som f.eks. Center for Cybersikkerhed, som sendes ud til de dataansvarlige.

I næste afsnit følger en række eksempler på anmeldelser af brud på persondatasikkerheden, som Datatilsynet har behandlet i 2023.

Brugen af ”auto-complete” i e-mailprogrammer

Siden den 25. maj 2018, hvor pligten til at anmelde brud på persondatasikkerheden til Datatilsynet blev indført, har tilsynet modtaget et betydeligt antal anmeldelser om fejlfremsendelse af oplysninger til forkerte modtagere, hvoraf mange af dem kan henføres direkte til anvendelsen af funktionen ”auto-complete”.

Alene i 2022 var antallet af denne type brud over 100. Fejlfremsendelserne sker bl.a., når en e-mail skal sendes internt til en bestemt kollega, og man i stedet får sendt den til en forkert helt uvedkommende person. Der er eksempler på, at helt uvedkommende private borgere har fået tilsendt oplysninger, som de aldrig skulle have haft. Det har bl.a. haft som konsekvens, at kontaktoplysninger, personnumre, helbreds-oplysninger, herunder om mindreårige, og oplysninger om strafbare forhold er blevet sendt til uvedkommende modtagere.

Som følge af de mange brud besluttede Datatilsynet i august 2023 at præcisere og skærpe praksis i forhold til, hvilke forpligtelser der påhviler de dataansvarlige, når funktionen ”auto-complete” anvendes.

Datatilsynet har hidtil udtalt, at de dataansvarlige som minimum skal overveje at indføre tekniske og/eller organisatoriske foranstaltninger, der kan mindske risikoen ved brugen af auto-complete. I de anmeldelser af brud på persondatasikkerheden, som tilsynet har modtaget, har de dataansvarlige dog – til trods for denne vejledning – ofte alene peget på organisatoriske foranstaltninger i form af øget awareness, som tiltag til at imødegå yderligere brud.

Datatilsynet udtalte på den baggrund, at det fremadrettet vil være tilsynets opfattelse, at dataansvarlige, der i et vist systematisk omfang anvender e-mails til at sende fortrolige og/eller følsomme oplysninger, ikke kan nøjes med at gennemføre organisatoriske sikkerhedsforanstaltninger, f.eks. i form af retningslinjer om kommunikation og awareness herom. Disse dataansvarlige skal også gennemføre en eller flere tekniske foranstaltninger for at mindske risikoen for fejlforsendelse som følge af brugen af ”auto-complete”. Hvis det alene er dele af organisationen/myndigheden, der i et vist systematisk omfang anvender e-mails til at sende fortrolige og/eller følsomme oplysninger, kan de tekniske foranstaltninger dog eventuelt begrænses til at gælde for dem.

Datatilsynet besluttede samtidig, at der skulle gælde en overgangsperiode indtil den 1. marts 2024, hvor de dataansvarlige får lejlighed til at vurdere risikoen og foretage de fornødne sikkerhedsforanstaltninger i overensstemmelse med den skærpede praksis. Datatilsynet kom i den forbindelse med en række forslag til organisatoriske- og tekniske sikkerhedsforanstaltninger som med fordel kunne overvejes gennemført for at afhjælpe de afdækkede risici.

Manglende test og utilstrækkelig kontrol af brugeradgange

Datatilsynet traf i 2023 afgørelse i en sag, hvor Aalborg Universitet havde anmeldt et brud på persondatasikkerheden til tilsynet. Aalborg Universitet konstaterede, at det i flere år – sandsynligvis siden 2020 og frem til august 2022 – havde været muligt for alle med en AAU-brugerprofil (studerende, medarbejdere og gæstemedarbejdere) at tilgå ikke-følsomme oplysninger om universitetets medarbejdere i et system. Systemet havde således ikke haft den nødvendige adgangsbegrænsning, da det kun var IT-medarbejdere på universitetet, der havde behov for at anvende systemet i deres daglige arbejde.

Aalborg Universitet oplyste, at der i forbindelse med migrering til ny server og omskrivning af kode i systemet i sommeren 2020 højst sandsynligt var sket en menneskelig fejl, idet der ikke var foretaget testning af adgangskontrol i systemet efterfølgende. I den forbindelse har Aalborg Universitet oplyst, at universitetets retningslinjer ikke var blevet fulgt.

Datatilsynet udtalte, at det er tilsynets opfattelse, at kravet om passende sikkerhed normalt vil indebære, at når der foretages migrering til ny server og omskrivning af kode i et system, der behandler personoplysninger, skal ændringerne ske efter fastsatte procedurer, hvorved de mulige konsekvenser ved ændringerne overvejes. I den forbindelse udtalte tilsynet, at kravet endvidere vil indebære, at der skal planlægges test, der kan verificere, at de fastsatte sikkerhedskrav, herunder adgangsbegrænsning, fortsat er opfyldt efter, at ændringerne er gennemført.

Derudover udtalte Datatilsynet, at det er tilsynets opfattelse, at kravet om passende sikkerhed normalt vil indebære, at den dataansvarlige løbende kontrollerer, om brugeradgange til systemer med personoplysninger er begrænset til de brugere, der har et sagligt behov for adgang til oplysningerne i systemet.

Datatilsynet fandt, at der var grundlag for at udtale kritik af, at Aalborg Universitets behandling af personoplysninger ikke var sket i overensstemmelse med kravet om passende sikkerhed i databeskyttelsesforordningens artikel 32. Datatilsynet lagde vægt på, at det er en forudsætning, at der foretages test efter en ændring eller opdatering af et system for at sikre, at de fastsatte sikkerhedskrav i et system fortsat er implementeret efter ændringen eller opdateringen. Derudover lagde Datatilsynet vægt på, at uvedkommende havde haft adgang til systemet i flere år, og at der dermed ikke havde været foretaget tilstrækkelig løbende kontrol af brugeradgange i systemet.

Mangelfuld rettighedsstyring

Datatilsynet udtalte i 2023 kritik af Hovedstadens Beredskab i en sag, hvor Hovedstadens Beredskab havde anmeldt et brud på persondatasikkerheden til tilsynet. Hovedstadens Beredskab havde konstateret, at alle brugere af Hovedstadens Beredskabs ESDH-system havde haft adgang til kontaktoplysninger, herunder personnumre og beskyttede adresser, om tidligere og nuværende medarbejdere, siden systemet blev taget i brug i maj 2022.

Hovedstadens Beredskab oplyste i sagen, at kontaktoplysningerne blev anvendt i forbindelse med journalisering af personalesager. Adgangen til de pågældende oplysninger burde ifølge Hovedstadens Beredskab have været differentieret således, at de kunne udpege, hvilke medarbejdere der havde et arbejdsbetinget behov for at arbejde med oplysningerne, og således at det alene var disse medarbejdere, der blev tildelt adgang til dem. Hovedstadens Beredskab og deres leverandør havde imidlertid ikke været opmærksomme på den manglende mulighed for at differentiere i adgangsrettigheder til de pågældende oplysninger.

Datatilsynet udtalte, at det er tilsynets opfattelse, at kravet om passende sikkerhed i databeskyttelsesforordningens artikel 32 normalt vil indebære, at brugeradgange til systemer er begrænset til de personoplysninger, som er nødvendige for de pågældende brugeres arbejdsbetingede behov.

Datatilsynet fandt, at Hovedstadens Beredskab ikke havde levet op til reglerne om behandlingssikkerhed, da Hovedstadens Beredskab ikke havde sikret differentieret brugeradgange til tidligere og nuværende medarbejderes kontaktoplysninger i systemet.

Datatilsynet lagde i sin afgørelse særligt vægt på, at alle brugere af ESDH-systemet, siden systemet blev taget i brug, havde haft adgang til kontaktoplysninger, som også indeholdt fortrolige oplysninger om beskyttede adresser og personnumre, om 2.029 nuværende og tidligere medarbejdere, selvom det kun var medarbejdere i Hovedstadens Beredskabs HR-afdeling, der havde behov for adgang til disse oplysninger.

Utilstrækkelig sikkerhed i forbindelse med login med MitID

Datatilsynet udtalte i juni 2023 alvorlig kritik af både Digitaliseringsstyrelsen og Signaturgruppen i en sag, hvor begge parter havde ansvar for utilstrækkelig sikkerhed i forbindelse med login med MitID.

I januar 2022 kom flere borgere ud for, at de ved login i deres netbank via MitID fik adgang til andre borgeres konti. Dette blev anmeldt til Datatilsynet som brud på persondatasikkerheden af tre pengeinstitutter. Datatilsynet tog på den baggrund en sag op af egen drift for at undersøge det bagvedliggende problem.

Fejlen viste sig at skyldes, at login-anmodninger til samme netbank inden for millisekunder i særlige tilfælde kunne medføre, at MitID udstedte et såkaldt token til en anden session. Denne fejl kunne være undgået, hvis brokeren (den virksomhed, der formidler autentifikationssvaret - i dette tilfælde Signaturgruppen) havde valideret borgernes login med en teknologi, som kaldes Broker Security Context. Digitaliseringsstyrelsen, som er dataansvarlig for MitID, havde anbefalet dette, men ikke stillet det som et krav.

Datatilsynet fandt, at anvendelsen af Broker Security Context burde have været et krav og konkluderede, at Digitaliseringsstyrelsen ikke havde haft tilstrækkelige foranstaltninger for at opnå et sikkerhedsniveau, der passede til de risici, der var for borgerne. Samtidig var det Datatilsynets opfattelse, at Signaturgruppen – som dataansvarlig for brokerløsningen – heller ikke havde haft passende sikkerhedsforanstaltninger, fordi de benyttede Broker Security Context på en anden måde end beskrevet i anbefalingen.

Datatilsynet lagde ved valg af reaktion bl.a. vægt på, at overtrædelsen medførte, at der havde været utilsigtet adgang til personoplysninger, i hvert fald om økonomiske oplysninger, og at denne adgang sandsynligvis havde indebåret en ikke ubetydelig risiko for de registreredes rettigheder og frihedsrettigheder. Tilsynet lagde endvidere vægt på, at der er tale om en landsdækkende løsning, hvis primære formål er at validere identifikation af enkeltpersoner med henblik på at give adgang til alene de oplysninger, som vedkommende er berettiget til at få adgang til, herunder personoplysninger, og som anvendes som digitalt ID til en række centrale private og offentlige selvbetjeningsløsninger mv.

Manglende adgangskontrol og logning

I en sag vedrørende Region Sjælland fandt Datatilsynet, at der på sundhedsområdet – i visse tilfælde – kan være behov for en bredere adgang til personoplysninger. Denne adgang skal dog begrænses til de medarbejdere, hvor der er et konkret arbejdsbetinget behov og kun i de arbejdssituationer, hvor det er relevant. Behovet for denne bredere adgang skal altid afvejes mod de kendte risikoscenarier.

Datatilsynet udtalte alvorlig kritik af Region Sjælland for at give alle autoriserede brugere adgang til patientlister med personoplysninger på samtlige af Regionens hospitalsafdelinger - uden tilstrækkelige sikkerhedsforanstaltninger.

Endvidere fandt Datatilsynet, at Region Sjællands logningspraksis ikke kunne skabe en sammenhæng mellem et opslag og de konkrete personoplysninger, som blev tilgået gennem patientlisten. Regionen kunne derfor ikke dokumentere og følge op på et eventuelt misbrug af den omfattende brugeradgang til persondata og havde på den baggrund ikke overholdt kravet om passende sikkerhed i databeskyttelsesforordningens artikel 32.

Autoriserede brugeres uretmæssige adgang til personoplysninger udgør en betydelig risiko, som alle dataansvarlige efter Datatilsynets opfattelse skal forholde sig til. Det er ikke altid tilstrækkeligt – alene at have tavshedsregler – til at beskytte de registreredes rettigheder.

Adgang til personoplysninger bør kun gives til en bruger efter en dokumenteret vurdering af den dataansvarlige, ligesom brugeren kun bør have adgang til personoplysninger, som vedkommende har et (arbejdsbetinget) behov for at tilgå. Den dataansvarlige skal reducere risikoen ved adgang til personoplysninger og implementere passende kontrolforanstaltninger.

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

Databehandler fik kritik for manglende sikkerhed

Datatilsynet udtalte kritik i en sag, hvor Mindworking A/S, som databehandler og leverandør af en platform til ejendomshandler, ikke havde sikret sig mod, at uvedkommende – ved inspektion af kildekoden (XML-koden) – kunne tilgå personoplysninger på platformen.

De oplysninger, der kunne tilgås på platformen, var de oplysninger, som den enkelte ejendomsmægler havde knyttet til en konkret ejendom, der var til salg. Der var bl.a. tale om navne på potentielle købere og den pris, de havde tilbudt for ejendommen, samt dokumenter med personoplysninger. Det var f.eks. udkast til købsaftaler, der – udover diverse identitetsoplysninger – i enkelte tilfælde også indeholdt cpr-numre. Enkelte af personoplysningerne var allerede offentliggjorte oplysninger fra tinglysningsportaler.

Oplysningerne kunne tilgås af brugere, der var tilknyttet konkrete salgssager, og efter de var logget ind med et brugernavn og adgangskode. Brugeren kunne få adgang til oplysningerne ved at trykke på en funktionstast og aktivere såkaldte ”Dev tools”, der er en forkortelse for ”Developer Tools” eller ”Web development tools”, og som er et webværktøj/en række programmer, der kan bruges til fx at teste og fejlfinde koder.

Datatilsynet slog i afgørelsen fast, at der generelt ikke i kildekoden eller i visningslagets kommentarfelter skal fremgå personoplysninger. Dette gælder også for oplysninger, der ikke er personoplysninger, men som vil kunne kompromittere behandlingssikkerheden - f.eks. hvis det er muligt i klar tekst at se styringsparametre på services, certifikater eller lignende.

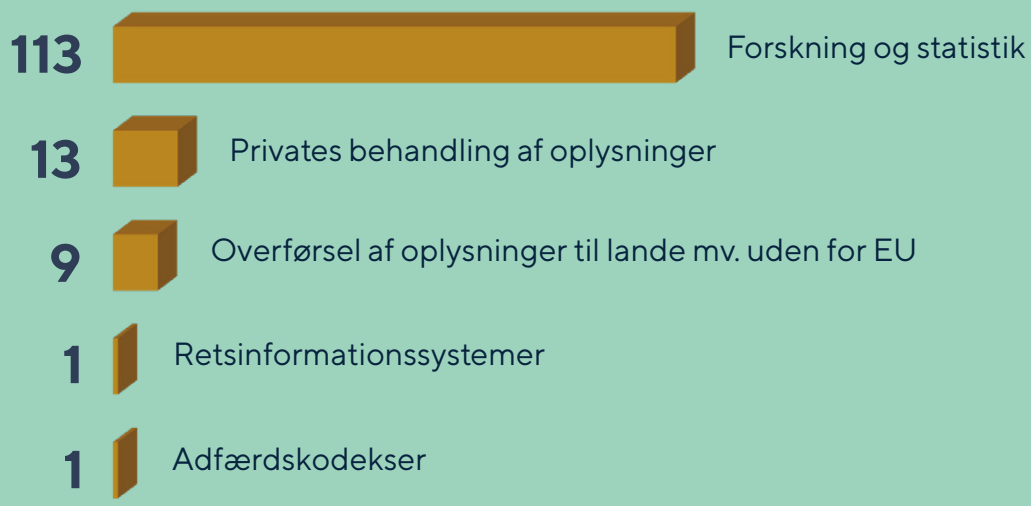
Datatilsynet slog endvidere fast, at det ikke var at betragte som en sikkerhedsforanstaltning, at adgang til oplysningerne krævede, at den enkelte bruger skulle aktivere ”Dev Tools” i browseren.

Det er Datatilsynets opfattelse, at funktionaliteten ved at benytte den pågældende funktionstast er en almindelig kendt proces for inspiceringen af kildekoden, der ikke kræver særlige kompetencer inden for it-sikkerhed.

Datatilsynet konkluderede, at databehandleren burde have gennemført relevante tests af platformen før ibrugtagningen, da der var tale om en kendt og elementær fejl, som let kunne og burde være undgået. Dermed havde Mindworking A/S overtrådt forordningens artikel 32 ved ikke at have truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passede til de risici, der var ved behandlingen af personoplysningerne.

Tilladelser mv.

137 sager i alt



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. På næste side omtales et eksempel på en af de tilladelsessager, som Datatilsynet har behandlet i 2023.

Præcisering af regler for sletning af personoplysninger ved afslutning af forskningsprojekter

Med virkning fra den 1. januar 2023 blev videregivelsesbekendtgørelsen ændret. Videregivelses-bekendtgørelsen angiver vilkårene for videregivelse af personoplysninger fra statistiske eller videnskabelige undersøgelser efter databeskyttelseslovens § 10.

Af videregivelsesbekendtgørelsen havde det hidtil fremgået bl.a., at personoplysninger ved undersøgelsens afslutning skulle slettes, anonymiseres, tilintetgøres eller tilbageleveres, således at det ikke efterfølgende var muligt at identificere fysiske personer ud fra oplysningerne eller i kombination med andre oplysninger.

Med henblik på at tydeliggøre, at dataansvarlige kan have et berettiget behov for at behandle oplysninger i en periode efter undersøgelsens afslutning – f.eks. med henblik på peer review eller imødegåelse af anklager om videnskabelig uredelighed – er bekendtgørelsen ændret.

Det fremgår derfor nu af bekendtgørelsen, at når formålet med behandling af personoplysninger er ophørt, skal oplysningerne slettes, anonymiseres, tilintetgøres eller tilbageleveres, således at det efterfølgende ikke er muligt at identificere fysiske personer ud fra oplysningerne eller i kombination med andre oplysninger. Alternativt kan personoplysningerne overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Ændringen skyldes, at dataansvarlige ofte vil være underlagt krav om i en periode efter afslutningen af deres undersøgelse at kunne bevise, at undersøgelsen ikke er baseret på falske oplysninger, eller at andre forskere skal kunne genskabe resultaterne. Derudover arbejdes der på nogle forskningsområder i højere grad med løbende afdækning af forskningsfelter, løbende opbygning af relationer eller løbende opbygning af datamateriale, hvor det ikke er meningsfuldt at tale om, at et projekt ”afsluttes”.

Dataansvarlige bør imidlertid være opmærksomme på, om formålet med behandlingen af personoplysninger efter undersøgelsens afslutning kan opnås ved at behandle oplysningerne i en anden – eksempelvis anonymiseret – form i overensstemmelse med det grundlæggende databeskyttelsesretlige princip om dataminimering.

Endelig skal dataansvarlige være opmærksomme på, at tilladelser til videregivelser meddelt af Datatilsynet før ændringen af bekendtgørelsen bør fortolkes i overensstemmelse med ovenstående.

Brøndby IF's anmodning om udvidet brug af ansigtsgenkendelse

Datatilsynet gav i 2019 – i henhold til databeskyttelseslovens § 7, stk. 4 – Brøndby IF tilladelse til behandling af følsomme personoplysninger omfattet af databeskyttelsesforordningens 9. Det drejer sig om biometriske data med det formål entydigt at identificere en fysisk person – i forbindelse med etableringen af automatisk ansigtsgenkendelse som led i adgangskontrol ved indgangene til Brøndby Stadion.

Datatilsynet behandlede i forlængelse heraf i 2023 en anmodning fra Brøndby IF om udvidet brug af ansigtsgenkendelse. Nærmere bestemt anmodede Brøndby IF om, at fodboldklubben kan anvende automatisk ansigtsgenkendelse ved kampe på andre stadions end Brøndby Stadion. Brøndby IF anmodede også om en vis udvidet adgang til at bruge automatisk ansigtsgenkendelse på Brøndby Stadion.

Som begrundelse for anmodningen oplyste Brøndby IF, at erfaringerne med anvendelsen af automatisk ansigtsgenkendelse generelt havde været gode.

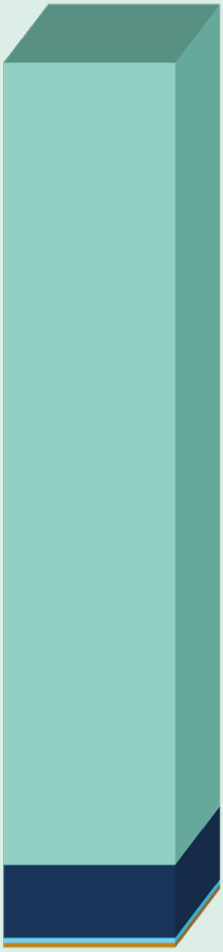
Brøndby IF havde imidlertid konstateret, at personer, der med baggrund i ordensreglementet for Brøndby Stadion var meddelt forbud mod tilstedeværelse til fodboldkampe med deltagelse af Brøndby IF – uanset hvor disse kampe spilles – havde formået at opnå adgang til kampe på andre stadions, hvor de havde udvist en adfærd svarende til den, der førte til, at de blev meddelt forbud mod tilstedeværelse til kampe med deltagelse af Brøndby IF, herunder udøvelse af vold og hærværk samt anden utryghedsskabende adfærd – såvel inde på stadion som i området omkring stadion og på rejsestrækningen til og fra stadion.

Efter at spørgsmålet havde været behandlet på et møde i Datarådet, fik Brøndby IF lov til den udvidede brug af ansigtsgenkendelse.

Datatilsynet lagde blandt andet vægt på, at de forhold, som begrundede, at tilsynet meddelte tilladelse til den omhandlede behandling i forbindelse med brugen af automatisk ansigtsgenkendelse som led i adgangskontrol ved indgangene til Brøndby Stadion, også må anses for at gøre sig gældende i forhold til Brøndby IF's udebanekampe, dvs. kampe på andre stadions end Brøndby Stadion.

Det var endvidere Datatilsynets vurdering, at Brøndby IF – inden for rammerne af den (oprindeligt) meddelte tilladelse – kunne anvende billeder fra overvågningskameraer på stadion som grundlag for i systemet til automatisk ansigtsgenkendelse at registrere personer, der overtræder ordensreglementet.

Internationalt arbejde



974 sager i alt

883 EU-sager

80 Forespørgsler om lovgivning til/fra udlandet (ikke særlig EU-procedure)

5 Nordisk tilsynssamarbejde

6 Forskelligt

Databeskyttelsesområdet er nu i langt højere omfang reguleret på EU-niveau, ligesom der med forordningen er etableret et ganske formaliseret samarbejde mellem de europæiske tilsyns-myndigheder. 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 tilsynet 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 Det Europæiske Databeskyttelsesråd (EDPB) og på den måde få gjort danske synspunkter gældende i rette tid og på rette sted.

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.

Fordeling af EU-sager

725 One-stop-shop-mekanismen

27 EDPB

28 Fælleseuropæiske systemer mv.

103 Forskelligt

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 Europa-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 Europa-Kommissionen om ethvert spørgsmål om beskyttelse af personoplysninger i EU.

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

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

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

Udtalelse om forslag til nye procedureregler for grænseoverskridende sager

Den 4. juli 2023 fremsatte Europa-Kommissionen et forslag til supplerende procedureregler for håndhævelse af databeskyttelsesforordningen. Forslaget skal supplere databeskyttelsesforordningen ved at fastsætte procedureregler for tilsynsmyndighedernes behandling af klager og gennemførelse af undersøgelser i grænseoverskridende sager.

EDPB afgav i september 2023 sammen med EDPS en udtalelse til Europa-Kommissionens forslag. EDPB og EDPS bød bl.a. i udtalelsen forslaget om at harmonisere, hvilke oplysninger en grænseoverskridende klage skal indeholde, før den kan antages til behandling, velkomment, men foreslog, at også de formelle betingelser, såsom forældelsesfrister, harmoniseres. Endvidere foreslog EDPB og EDPS, at bestemmelserne i forslaget, der vedrører opnåelse af enighed blandt tilsynsmyndighederne, forbedres yderligere ved at sikre, at de berørte tilsynsmyndigheder inddrages mere og tidligere under samarbejdsproceduren med henblik på at undgå uenigheder om, hvordan en sag skal håndteres senere i sagsforløbet.

Fælleseuropæiske bindende afgørelser

I løbet af 2023 traf EDPB tre bindende afgørelser i såkaldte tvistbilæggelsessager efter procedurerne i databeskyttelsesforordningens artikel 65 og 66.

Bindende afgørelse om Meta Irlands overførsel af personoplysninger til USA

Den første bindende afgørelse i 2023 efter tvistbilæggelsesproceduren i databeskyttelsesforordningens artikel 65 blev vedtaget af EDPB i april. I sagen, der vedrørte Meta Irlands overførsel af personoplysninger om Facebook-brugere til USA, havde det irske datatilsyn som ledende tilsynsmyndighed udarbejdet et udkast til en afgørelse i sagen, som flere europæiske tilsynsmyndigheder havde gjort indsigelser mod.

I sin bindende afgørelse erklærede EDPB sig enig med det irske tilsyn i, at Meta Irland ikke havde kunnet sikre et tilstrækkeligt beskyttelsesniveau for de personoplysninger, der blev overført til USA. EDPB fandt endvidere grundlag for, at det irske datatilsyn skulle instrueres i at udstede en bøde til Meta Irland for overtrædelsen af databeskyttelsesforordningen. EDPB lagde i den forbindelse bl.a. vægt på den høje grad af alvorlighed af overtrædelsen og antallet af registrerede omfattet af overtrædelsen. Herudover instruerede EDPB det irske datatilsyn i at meddele Meta Irland påbud om at bringe sine behandlingsaktiviteter i overensstemmelse med databeskyttelsesforordningen inden seks måneder fra det irske datatilsyns afgørelse.

På baggrund af EDPB's bindende afgørelse traf det irske datatilsyn sin endelige afgørelse i sagen den 22. maj 2023. I sin afgørelse udstedte det irske tilsyn en bøde på 1,2 milliarder euro (svarende til næsten 9 milliarder danske kroner) for overtrædelsen af databeskyttelsesforordningen. Dette er den største bøde, der hidtil er udstedt efter forordningen. Det irske datatilsyn meddelte endvidere Meta Irland et påbud om at bringe sine behandlingsaktiviteter i overensstemmelse med forordningen inden seks måneder.

Datatilsynet var, ligesom de øvrige europæiske datatilsyn, berørt tilsynsmyndighed i sagen, og – som en del af EDPB – var tilsynet også involveret i udarbejdelsen af EDPB's bindende afgørelse.

Bindende afgørelse om TikToks behandling af personoplysninger om børn

Den 2. august 2023 vedtog EDPB endnu en bindende afgørelse efter tvistbilæggelsesproceduren i databeskyttelsesforordningens artikel 65. Afgørelsen vedrørte TikToks behandling af personoplysninger om børn og blev truffet efter anmodning fra det irske datatilsyn som ledende tilsynsmyndighed i sagen.

I sin bindende afgørelse adresserede EDPB flere indsigelser fra berørte tilsynsmyndigheder mod det irske datatilsyns forslag til afgørelse i sagen. Indsigelserne omhandlede bl.a. TikToks overtrædelse af reglerne om databeskyttelse gennem design og standardindstillinger i forhold til aldersverifikation, og om der også var sket en overtrædelse af princippet om rimelighed.

I afgørelsen tog EDPB stilling til TikToks designpraksis vedrørende to konkrete pop-up notifikationer (én når man registrerede sig som bruger, og én når man postede en video), der blev vist til børn i alderen 13-17 år.

EDPB fandt, at ingen af disse notifikationer præsenterede valgmuligheder til brugeren på en objektiv og neutral måde. På den baggrund fandt EDPB, at TikTok overtrådte princippet om rimelighed i databeskyttelsesforordningen, jf. artikel 5. EDPB udtalte i den forbindelse, at dataansvarlige ikke bør gøre det svært for registrerede at justere deres privatlivsindstillinger og begrænse behandlingen af deres personoplysninger. Det irske tilsyn blev herefter instrueret i at inkludere denne overtrædelse i sin endelige afgørelse og i at meddele påbud til TikTok om at bringe denne praksis i overensstemmelse med forordningen.

Endvidere fandt EDPB grundlag for at udtrykke alvorlig tvivl om, hvorvidt TikToks foranstaltninger vedrørende aldersverifikation var tilstrækkeligt effektive, særligt fordi disse nemt ville kunne omgås.

Det irske datatilsyn inddrog EDPB's konklusioner i sin endelige afgørelse og fandt endvidere, at TikToks 'public by default' indstillinger var i strid med databeskyttelsesforordningens regler om databeskyttelse gennem design og standardindstillinger samt principperne om dataminimering og gennemsigtighed. Ud over kritik og et påbud udstedte det irske datatilsyn en bøde til TikTok på 345 millioner euro, svarende til ca. 2,6 milliarder kroner.

Datatilsynet deltog som medlem i EDPB i udarbejdelsen af den bindende afgørelse, og den irske sag blev bl.a. rejst på baggrund af en sag, som Datatilsynet havde påbegyndt, men som i 2021 blev oversendt til det irske datatilsyn, da TikTok i mellemtiden havde etableret sit europæiske hovedkontor i Irland.

Bindende afgørelse vedrørende Meta Irlands adfærdsbaserede markedsføring

I oktober 2023 traf EDPB en såkaldt 'hurtig bindende afgørelse' i overensstemmelse med databeskyttelsesforordningens artikel 66, stk. 2.

Sagen opstod på baggrund af tre bindende afgørelser, som EDPB vedtog den 6. december 2022. I afgørelserne fandt EDPB, at Meta Irland ikke kunne basere sin behandling af personoplysninger til brug for adfærdsbaseret markedsføring på nødvendigheden for opfyldelse af en kontrakt med den registrerede. Det irske datatilsyn traf herefter sin endelige afgørelse den 31. december 2022, hvori tilsynet fandt, at Meta Irland ikke havde lovligt grundlag for at behandle personoplysninger til brug for adfærdsbaseret markedsføring. Meta Irland fik – foruden en bøde – påbud om at bringe behandlingen i overensstemmelse med databeskyttelses-forordningen ved at identificere et passende lovligt grundlag for behandlingen af personoplysninger til brug for adfærdsbaseret markedsføring inden for en frist på tre måneder. Sagerne er omtalt i Datatilsynets årsberetning fra 2022.

I april 2023 besluttede Meta Irland imidlertid at basere sin behandling af personoplysninger til adfærdsbaseret markedsføring på Meta Irlands legitime interesse i at behandle oplysningerne til dette formål, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Den 14. juli 2023 udstedte det norske datatilsyn et midlertidigt forbud herimod og forbød dermed Meta Irland at behandle personoplysninger om norske borgere til brug for adfærdsbaseret markedsføring baseret på enten kontraktforhold eller legitim interesse. Dette skyldtes, at det norske tilsyn mente, at en legitim interesse ikke kunne udgøre et lovligt grundlag for behandlingen, og at Meta Irland derfor ikke havde levet op til det påbud, virksomheden fik den 31. december 2022. I overensstemmelse med artikel 66, stk. 1 i databeskyttelsesforordningen var forbuddet geografisk afgrænset til kun at gælde i Norge og var tidsbegrænset til tre måneder.

Den 26. september 2023 anmodede det norske datatilsyn EDPB om at træffe endelige foranstaltninger mod Meta Irland. Det norske tilsyn anmodede specifikt EDPB om at træffe en 'hurtig bindende afgørelse' efter artikel 66, stk. 2 i databeskyttelsesforordningen for at gøre forbuddet mod Meta Irland tidsubegrænset og gældende i hele EØS.

Den 27. oktober 2023 traf EDPB sin endelige afgørelse. I afgørelsen fandt EDPB, at Meta Irland overtrådte artikel 6, stk. 1, i databeskyttelsesforordningen, idet virksomheden uberettiget havde behandlet personoplysninger til adfærdsbaseret markedsføring på baggrund af henholdsvis kontraktforhold og legitim interesse. Herudover fandt EDPB, at Meta Irland havde overtrådt sin forpligtelse til at efterkomme det irske datatilsyns afgørelse af 31. december 2022. I lyset af risikoen for alvorlig og uoprettelig skade for de registrerede fandt EDPB endvidere, at sagen var af så hastende karakter, at den almindelige samarbejdsmekanisme ikke kunne bruges i sagen.

På den baggrund fandt EDPB slutteligt, at der omgående skulle træffes endelige foranstaltninger overfor Meta Irland, hvorfor det irske datatilsyn blev instrueret i at udstede forbud mod Meta Irlands behandling af personoplysninger til brug for adfærdsbaseret markedsføring baseret på bestemmelsen om kontraktforhold og legitim interesse. Det irske datatilsyn traf afgørelse i sagen den 10. november 2023, hvorefter forbuddet trådte i kraft.

Efterfølgende har Meta Irland introduceret en ny samtykkebaseret løsningsmodel ved brug af Facebook og Instagram, hvor brugerne kan vælge mellem en gratis udgave, der fortsat indeholder adfærdsbaseret markedsføring, og en betalingsversion uden denne form for markedsføring. Det irske datatilsyn er på nuværende tidspunkt ved at se nærmere på lovligheden af denne løsningsmodel. EDPB, og Datatilsynet følger udviklingen i sagen tæt.

Fælles koordineret håndhævelsesramme (CEF)

I oktober 2020 etablerede EDPB den fælles koordinerede håndhævelsesramme, også kaldet CEF (Coordinated Enforcement Framework). Initiativet har til formål at koordinere fælles aktiviteter mellem de europæiske tilsynsmyndigheder og derved harmonisere og styrke håndhævelsen af databeskyttelses-forordningen.

I januar 2023 vedtog EDPB en rapport om offentlige myndigheders brug af cloudservices. Rapporten er den første, som er blevet vedtaget som led i den fælles koordinerede håndhævelsesramme. Datatilsynet deltog aktivt i udarbejdelsen af de generelle betragtninger og konklusioner i den offentliggjorte rapport samt rapportens anbefalinger.

I rapporten understreger EDPB behovet for, at offentlige myndigheder handler i fuld overensstemmelse med databeskyttelsesforordningen, når de bruger cloudbaserede produkter eller tjenester, og giver i tillæg hertil en række anbefalinger til, hvordan myndighederne kan leve op til de gældende krav.

Derudover indeholder rapporten en generel oversigt over sager (afgørelser, udtalelser mv.), som de europæiske tilsynsmyndigheder har behandlet om brugen af cloudservices de seneste år ud over den koordinerede indsats.

Ny tilstrækkelighedsafgørelse vedrørende USA

Europa-Kommissionen vedtog den 10. juli 2023 en tilstrækkelighedsafgørelse vedrørende det nye EU-U.S. Data Privacy Framework (EU-U.S. DPF). Som følge af afgørelsen kan man nu overføre personoplysninger fra EU/EØS til organisationer i USA, som har certificeret sig under EU-U.S. DPF.

EU-U.S. DPF er en certificeringsordning bestående af en række databeskyttelsesretlige principper, som er udviklet i et samarbejde mellem EU og USA. En virksomhed, som vælger at certificere sig under ordningen, bliver retligt forpligtet til at overholde principperne.

EU-U.S. DPF administreres af det amerikanske handelsministerium, og en opdateret liste over certificerede virksomheder er tilgængelig på ministeriets hjemmeside.

Med den nye tilstrækkelighedsafgørelse har Europa-Kommissionen vurderet, at EU-U.S. DPF sammen med en række nye retssikkerhedsgarantier i amerikansk lovgivning – herunder etableringen af en særlig klagemekanisme for EU/EØS-registrerede – sikrer et niveau for beskyttelse af personoplysninger, som i det væsentlige svarer til niveauet inden for EU/EØS. Dette betyder, at man kan overføre personoplysninger til EU-U.S. DPF-certificerede virksomheder uden at skulle anvende et overførselsgrundlag i databeskyttelsesforordningens artikel 46. Det er tilstrækkeligt at henvise til tilstrækkelighedsafgørelsen som grundlag for overførslen.

Den nye tilstrækkelighedsafgørelse og ændringerne i amerikansk lovgivning er resultatet af næsten tre års forhandlinger mellem EU og USA, efter den såkaldte EU-U.S. Privacy Shield-ordning blev kendt ugyldig af EU-Domstolen i 2020 (Schrems II-dommen).

Det Europæiske Databeskyttelsesråd (EDPB) vedtog den 28. februar 2023 en udtalelse om Europa-Kommissionens udkast til tilstrækkelighedsafgørelsen, og EDPB vil også deltage i den første evaluering af tilstrækkelighedsafgørelsen i 2024.

Informationsnote fra EDPB om overførsler til USA

EDPB vedtog den 18. juli 2023 en informationsnote om overførsel af personoplysninger til USA efter vedtagelsen af den nye tilstrækkelighedsafgørelse vedrørende EU-U.S. Data Privacy Framework (EU-U.S. DPF). Informationsnoten blev udfærdiget med henblik på at besvare en række spørgsmål om konsekvenserne af tilstrækkelighedsafgørelsen for registrerede i EU/EØS og for dataeksportører, som overfører personoplysninger fra EU/EØS til USA. I korte træk fremhæves følgende:

- Med tilstrækkelighedsafgørelsens ikrafttræden den 10. juli 2023 kan man frit overføre personoplysninger fra EU/EØS til virksomheder i USA, der er certificeret under EU-U.S. DPF. Det er ikke nødvendigt at tilvejebringe et overførselsgrundlag i databeskyttelsesforordningens artikel 46 eller fastsætte effektive supplerende foranstaltninger for sådanne overførsler.
- Hvis organisationen i USA ikke er certificeret under EU-U.S. DPF, kan tilstrækkelighedsafgørelsen ikke anvendes som overførselsgrundlag. Der vil da stadig skulle tilvejebringes et overførselsgrundlag og eventuelt fastsættes effektive supplerende foranstaltninger for at opnå et beskyttelsesniveau svarende til det inden for EU/EØS.
- De retssikkerhedsgarantier, som den amerikanske regering har indført i forbindelse med amerikanske efterretningstjenesters adgang til og brug af personoplysninger overført fra EU/EØS, gælder for alle overførsler til USA uanset valg af overførselsgrundlag. Ved vurderingen af, om det valgte overførselsgrundlag sikrer en effektiv beskyttelse, kan dataeksportører inddrage Europa-Kommissionens analyse af amerikansk lovgivning og praksis i tilstrækkelighedsafgørelsen.
- Der findes en række forskellige klagemuligheder for EU/EØS-registrerede, som mener, at en certificeret virksomhed behandler deres oplysninger i strid med principperne i EU-U.S. DPF.
- Ønsker man at klage over de amerikanske efterretningstjenesters behandling af ens personoplysninger, kan man benytte sig af den nyetablerede klagemekanisme til dette formål. Klagen skal indgives til det nationale datatilsyn i ens egen medlemsstat. Det pågældende datatilsyn videreformidler klagen til EDPB, som sender den videre til klageinstansen i USA. Man behøver ikke kunne påvise, at amerikanske efterretningstjenester rent faktisk har indsamlet personoplysningerne.
- Tilstrækkelighedsafgørelsen vil blive evalueret første gang et år efter ikrafttrædelsen. Det vil i den forbindelse blive kontrolleret, om alle relevante elementer i afgørelsen er blevet implementeret fuldt ud og fungerer i praksis.

Særlige internationale tilsynsforpligtelser

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

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

SIS (Schengen-informationssystemet)

Som en del af Schengen-samarbejdet om et fælles område uden indre grænser samarbejder medlemsstater 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.

Den 7. marts 2023 trådte tre nye SIS-forordninger i kraft. Forordningerne erstatter de tidligere SIS II-forordninger samt Rådets afgørelse om SIS II. De nye forordninger har til formål at styrke SIS særligt i lyset af EU's migrationsudforinger. Med de nye regler er håndhævelsen og effektiviteten af EU's politik for tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold blevet styrket og samarbejdet mellem politi og juridiske myndigheder er blevet både udvidet og forbedret.

Datatilsynet deltager på EU-niveau i en koordinationsgruppe for tilsynet med SIS (SIS CSC), hvor de nationale datatilsyn i EU-medlemsstaterne, Island, Norge, Liechtenstein og Schweiz sammen med Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) sikrer et koordineret tilsyn med behandlingen af personoplysninger i SIS. 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. Der har i 2023 været afholdt fire møder i SIS CSC.

Endvidere deltog Datatilsynet i efteråret 2022 i den såkaldte 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 de andre medlemsstaters datatilsyn, Europa-Kommissionen og EDPS. 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 medlemsstaterne, samtidig med at der opretholdes et højt niveau af gensidig tillid mellem medlemsstaterne.

Datatilsynet har i 2023 samarbejdet med evalueringsholdet om opfølgningen på evalueringen. Det forventes, at den endelige evalueringsrapport bliver vedtaget i løbet af 2024. Datatilsynet skal herefter følge op på evalueringsholdets anbefalinger og bemærkninger.

VIS (Visuminformationssystemet)

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

Som led i tilsynet med behandling af personoplysninger i VIS deltager Datatilsynet endvidere i en koordinationsgruppe for tilsynet med visuminformationssystemet (VIS SCG).

Der har i 2023 været afholdt to møder, hvor der bl.a. blev drøftet følgende emner:

- Lovforslag om digitale VISA.
- Arbejdet med en fælles tilsynsplan til brug for nationale tilsynsmyndigheders tilsyn med VIS.
- Udarbejdelse af et arbejdsdokument vedrørende sletning af oplysninger i VIS før tid.

Eurodac

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

Som led i tilsynet med Eurodac deltager Datatilsynet endvidere i en koordinationsgruppe for tilsynet med Eurodac (Eurodac SCG). I 2023 har der været afholdt to møder, hvor gruppen bl.a. har haft besøg af repræsentanter for eu-LISA med henblik på orienteringer om den seneste udvikling på området og drøftelser af de aktuelle databeskyttelsesretlige problemstillinger. Herudover har Europa-Kommissionen givet skriftlige opdateringer på området, herunder status for Europa-Kommissionens forslag til en ny Eurodac-forordning. Endvidere har gruppen bl.a. drøftet følgende emner:

- Tilsyn med retshåndhævende myndigheders adgang til Eurodac
- Vedtagelse af Koordinationsgruppens aktivitetsrapport 2020-2021
- Prioritering af emner i gruppens arbejdsprogram for 2022-2024

CIS (Toldinformationssystemet)

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 told-administration.

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 i en koordinationsgruppe for tilsynet med CIS (CIS SCG). Der har i 2023 været afholdt ét møde i CIS SCG.

IMI (Informationssystemet for det indre marked)

Informationssystemet for det indre marked (IMI), som er oprettet af Europa-Kommissionen, har overordnet til formål at lette europæiske myndigheders grænseoverskridende samarbejde og sagsbehandling. Datatilsynet fører tilsyn med behandlingen af personoplysninger i den danske del af systemet.

På EU-niveau deltager Datatilsynet i en koordinationsgruppe for tilsynet med IMI (IMI SCG). Der har i 2023 været afholdt fire møder, hvor man bl.a. arbejder på et sæt anbefalinger til nationale myndigheder om iagttagelse af oplysningspligten, når personoplysninger behandles i IMI.

Tilsyn med Rigspolitiets søgning i EU-informationssystemer

Som led i Datatilsynets internationale tilsynsforpligtelser har tilsynet i 2023 først tilsyn med Rigspolitiets søgning i EU-informationssystemer til retshåndhævende formål.

Datatilsynet fandt, at Rigspolitiet ikke havde overholdt de retlige betingelser for søgninger i henholdsvis Visuminformationssystemet og Eurodac-systemet. Rigspolitiet har, under visse betingelser, mulighed for at søge i de pågældende systemer til retshåndhævende formål på baggrund af en anmodning fra politikredsene. Det er i den sammenhæng påkrævet, at Rigspolitiet foretager en kontrol af, om politikredsene har overholdt betingelserne for søgning i systemerne.

I forhold til Visuminformationssystemet fandt Datatilsynet, at den nødvendige kontrol i ét tilfælde ikke var blevet foretaget, og i et andet tilfælde ikke var foretaget i tilstrækkelig grad.

Datatilsynet fandt endvidere, at Rigspolitiet i ét tilfælde ikke havde foretaget en forudgående søgning i Visuminformationssystemet, inden Rigspolitiet foretog en søgning i Eurodac-systemet. Rigspolitiet har også her, under visse betingelser, mulighed for at foretage en søgning til retshåndhævende formål. Det er bl.a. en betingelse herfor, at der er foretaget en forudgående søgning i Visuminformationssystemet uden resultat.

Datatilsynet udtalte på den baggrund kritik af Rigspolitiets manglende kontrol af søgningskriterierne i Visuminformationssystemet og Eurodac-systemet.

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 2023.

Den internationale arbejdsgruppe om databeskyttelse i teknologi

Den såkaldte Berlin-gruppe, der har skiftet navn til International Working Group on Data Protection in Technology, har i 2023 afholdt to møder i Rom og Ottawa.

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

I 2023 har gruppens fokus på privatliv og sikkerhed vedrørt følgende Working Papers:

- Smarte byer: Vedrører brugen af personoplysninger opsamlet fra de enheder, beboerne i byen benytter i deres dagligdag og den interaktion, der kan skabes ved brug af de såkaldte beacons (antenner, der opsamler oplysninger direkte når en enhed passerer forbi).
- Ansigtsgenkendelse: Vedrører brugen af ansigtsgenkendelse, både i forhold til selve indsamlingen af oplysninger, men også for så vidt angår brugen af disse i forhold til overvågning, biometrisk genkendelse samt forholdet til retshåndhævelse.
- Telemetri og diagnostiske data: Forholder sig til indsamling og behandlingen af denne type oplysninger ved brug af applikationer, software og hardware. Der er i dokumentet fokus på den ugennemsigtige informationsindsamling hos den enkelte og det faktum, at den registrerede ikke har nogen eller kun ringe sikkerhed for, hvordan oplysningerne benyttes. Gruppens mål har været at få lavet beskrivelser og oplæg til at adressere de pågældende problemstillinger.

I årets løb har gruppen i øvrigt arbejdet med aktuelle emner, som indeholder problemstillinger med hensyn til databeskyttelse og beskyttelse af privatliv, eksempelvis, blockchain, digitale penge, quantum computing, neuroteknologi, generativ AI, biometri i elektronisk online autentifikation, ISO-standardisering, privatlivsbeskyttelse ved ICANN's RDS (Registration Directory Services) for internettet og forhold omkring forfølgelse og uønsket opmærksomhed i digital forstand (såkaldt cyber bullying og stalking).

Nordisk samarbejde

Der er en stærk tradition for samarbejde på det databeskyttelsesretlige område mellem de nordiske lande.

De nordiske datatilsyn er derfor i jævnlig kontakt om såvel konkrete som generelle emner og drøfter også spørgsmål af fælles interesse i forbindelse med deltagelse i møder i Det Europæiske Databeskyttelsesråd og dets ekspertarbejdsgrupper.

Det kom også til udtryk i 2023 – både på formelle møder og gennem sparring og videndeling på ad hoc-basis.
Hvert år afholdes der således et officielt nordisk møde, hvor alle de nordiske datatilsyn samles for at drøfte aktuelle spørgsmål på databeskyttelsesområdet. I 2023 fandt mødet sted i maj i Reykjavík, og her drøftede tilsynsmyndighederne bl.a. det værdifællesskab, der kendetegner de nordiske lande, og de fordele, der derfor kan drages ved et endnu tættere samarbejde. Traditionen tro vedtog tilsynene en erklæring på mødet. Et af målene i "Reykjavík-erklæringen" drejer sig om fortsat at udforske mulighederne for en mere data- og risikobaseret proces i udvælgelsen af, hvor der skal føres tilsyn. I den forbindelse aftalte landene endvidere at arbejde for større vidensdeling på europæisk niveau.

Endvidere havde Datatilsynet i september 2023 besøg af kolleger fra de norske og islandske datatilsyn, der gerne ville lære mere om Datatilsynets arbejde med at effektivisere sagsbehandlingen. Datatilsynet præsenterede i den forbindelse sit system for sagsbehandling og for behandling af brud på persondatasikkerheden.

Herudover var Datatilsynet i oktober 2023 vært for et besøg fra det svenske datatilsyn. Nogle af de erfaringer, som de danske repræsentanter kunne dele med de svenske kollegaer, vedrørte visiteringen af anmeldelser af brud på persondatasikkerheden, erfaringsindsamling og målrettet vejledning på baggrund af tendenserne i bruddene.

Den europæiske konference

Den europæiske konference for databeskyttelsesmyndigheder, også kaldet Forårskonferencen, afholdes en gang årligt. Datatilsynet var repræsenteret på konferencen i 2023, som blev afholdt i Budapest.

På konferencen blev bl.a. nye teknologiers indvirkning på vores tænkning, vores menneskelige relationer, vores sprog og på den måde, samfundet fungerer på, drøftet. Derudover blev de indbyrdes forbindelser mellem konkurrence- og databeskyttelseslovgivningen drøftet. Der blev bl.a. set nærmere på, hvordan disse to retsområder og tilsynsmyndighederne på området kan støtte og lære af hinanden.

For første gang var der også arrangeret en åben del på konferencen, som andre aktører end databeskyttelsesmyndigheder kunne deltage i. Emnet for den åbne del var databeskyttelsesrådgivere, hvor betydningen af veludviklede DPO-netværk og databeskyttelsesrådgiverens rolle internt i en organisation blev drøftet.

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 rapporter og resolutioner mv. om aktuelle databeskyttelsesemner. Udkast til rapporter og resolutioner forberedes inden konferencen i en række arbejdsgrupper bestående af repræsentanter fra de nationale databeskyttelsesmyndigheder. Datatilsynet deltager i bl.a. den såkaldte Berlin-gruppe, der har skiftet navn til International Working Group on Data Protection in Technology.

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 2023 i Bermuda, som Datatilsynet ikke deltog i, vedtog GPA en række resolutioner. Der blev bl.a. vedtaget en resolution om kunstig intelligens i forbindelse med ansættelse og en resolution om behandling af sundhedsdata til forskningsformål samt en resolution om GPA's strategiske fokusområder for 2023-2025, hvor der bl.a. vil være fokus på de registreredes rettigheder og styrkelse af databeskyttelsesmyndigheders kapacitet.

Grønland og Færøerne

49 sager i alt

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.

Den 1. juli 2023 blev retshåndhævelsesloven sat i kraft for Grønland for så vidt angår den behandling af personoplysninger, der foretages af politi og anklagemyndighed, ligesom justitsministeren kan fastsætte tidspunktet for reglernes virkning for kriminalforsorgen og domstolene.

Persondataloven er med virkning fra den 1. juli 2017 sat i kraft for rigsmyndighedernes behandling af oplysninger på Færøerne. Endvidere er pr. 1. juli 2022 retshåndhævelsesloven sat i kraft for de retshåndhævende myndigheder 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 2023 i lighed med foregående år kun modtaget få henvendelser om behandling af personoplysninger i Grønland eller ved rigsmyndighederne på Færøerne og har ikke behandlet mere principielle sager herom.

Tilsynet har dog modtaget flere 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.

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 2023 har Datatilsynet på retshåndhævelsesområdet bl.a. behandlet klagesager, forespørgsler samt anmeldelser om brud på persondatasikkerheden.

Ny vejledning om overførsel af personoplysninger til tredjelande på retshåndhævelsesområdet

Det Europæiske Databeskyttelsesråd (EDPB) vedtog i september 2023 en ny vejledning om rets-håndhævelsesdirektivets artikel 37 om overførsler til tredjelande omfattet af fornødne garantier.

Vejledningen indeholder bl.a. en beskrivelse af, hvad der skal forstås ved sådanne fornødne garantier, og hvilke retlige krav der stilles til garantierne. Derudover har vejledningen fokus på fortolkningen og anvendelsen af de to konkrete overførselsgrundlag i retshåndhævelsesdirektivets artikel 37, stk. 1, litra a og b, samt dokumentations- og underretningsforpligtelserne i artikel 37, stk. 2 og 3.

Vejledningen indeholder endvidere en liste over elementer, der bør indgå i et retligt bindende instrument, der anvendes som overførselsgrundlag. Den giver også eksempler på, hvordan man kan vurdere alle omstændighederne ved en overførsel. I vejledningen fremhæves bl.a.:

- at retshåndhævelsesdirektivets artikel 37 skal anvendes i lyset af princippet om, at beskyttelses-niveauet i EU/EØS ikke må undermineres ved overførsel af personoplysninger til et tredjeland,
- at anvendelse af et retligt bindende instrument i henhold til retshåndhævelsesdirektivets artikel 37, stk. 1, litra a, bør have forrang frem for en vurdering efter artikel 37, stk. 1, litra b, og
- at anvendelse af retshåndhævelsesdirektivets artikel 37, stk. 1, litra b, kun kan ske på grundlag af en nøje analyse af relevant lovgivning og praksis i modtagerlandet, som viser, at der findes de fornødne garantier for den konkrete overførsel.

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 (og retterne).

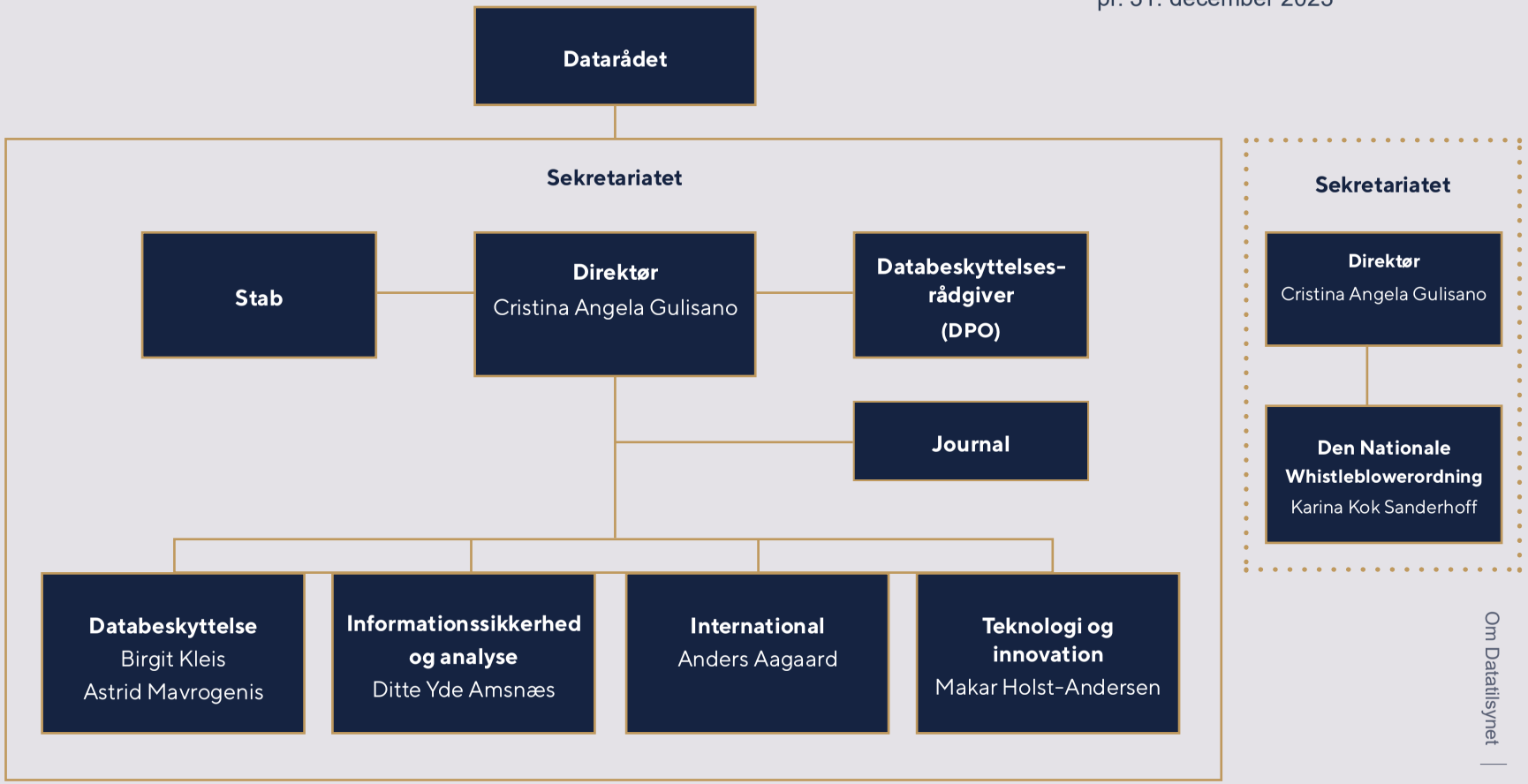
Datatilsynets organisation

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

pr. 31. december 2023



Datatilsynets opgaver

Tilsynet med databeskyttelsesområdet indebærer et stort antal forskelligartede opgaver. Datatilsynet har i 2023 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.

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. Udpegningen sker på baggrund af medlemmernes faglige kvalifikationer. De er således ikke repræsentanter for bestemte interesseorganisationer eller lignende.

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

Datarådets medlemmer (pr. 31. december 2023)

Formand
Kristian Korfits Nielsen, højesteretsdommer (udnævnt af justitsministeren)

Medlemmer
Henrik Udsen., dr.jur., Københavns Universitet (udnævnt af justitsministeren)
Pia Kirstine Voldmester, advokat og partner, Kromann & Reumert (udnævnt af justitsministeren)
Henning Mortensen, formand for Rådet for Digital Sikkerhed (udnævnt af justitsministeren)
Pernille Christensen. juridisk chef i KL (udnævnt af justitsministeren)
Uffe Rabe Krag, politisk chef i Forbrugerrådet Tænk (udnævnt af justitsministeren)
Svend Hartling, fhv. sundhedsdirektør i Region Hovedstaden (udnævnt af finansministeren)

Det syvende medlem til rådet forventes at falde på plads i 1. halvår af 2024.

Sekretariatet

Tilsynets sekretariat består af ca. 78 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 2023, der kan findes på undersiden "Årsberetninger og årsrapporter" på Datatilsynets hjemmeside. *Oversigten viser antallet af medarbejdere og ikke antallet af årsværk. Der kan derfor være visse afvigelser i forhold til den økonomiske årsrapport for 2023.

Sekretariatets medarbejdere (pr. 31. december 2023)*

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 Holst-Andersen
Chefkonsulent, cand.jur. Morten Juul Gjermundbo
Chefkonsulent, cand.jur. Vibeke Dyssemark Thomsen
Specialkonsulent, cand.jur. Andreas Droob Kristensen
Specialkonsulent, cand.soc. Gry Wad
Specialkonsulent, cand.jur. Lise Fredskov
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.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. Anne Elisabeth Tinten
Fuldmægtig, cand.jur. Anne-Sofie Bruunsgaard Secher
Fuldmægtig, cand.jur. Camilla von Köller
Fuldmægtig, cand.jur. Caroline Lindstrøm (orlov)
Fuldmægtig, cand.jur. Charlotte Svane Guglielmetti
Fuldmægtig, cand.jur. Delaram Ostadian Lam (orlov)
Fuldmægtig, cand.jur. Frederik Vahlgren
Fuldmægtig, cand.jur. Janani Parameswaran
Fuldmægtig, cand.jur. Jane Mindstrup Hagelin

Fuldmægtig, cand.jur. Josefine Grue
Fuldmægtig, cand.jur. Kamilla Bay Christensen
Fuldmægtig, cand.jur. Kamille Frølund Thomsen
Fuldmægtig, cand.jur. Kasper Folmar
Fuldmægtig, cand.jur. Line Hedemann Jacobsen
Fuldmægtig, cand.jur. Line Sørensen (orlov)
Fuldmægtig, cand.jur. Louise Lunddahl Nielen
Fuldmægtig, cand.jur. Mads Nordstrøm Kjær
Fuldmægtig, cand.jur. Majbrit Marie Hansen
Fuldmægtig, cand.jur. Malene Højbjerg
Fuldmægtig, cand.merc. jur. Miriem Naima Johansson (orlov)
Fuldmægtig, cand.merc.jur. Nicolai Philip van Hauen
Fuldmægtig, cand.jur. Rasha Suhiela Said Eleish
Fuldmægtig, cand.jur. Rikke Madsen
Fuldmægtig, cand.jur. Rumaisa Hajaj
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, cand.polyt., Ph.d. Martin Mehl Lauridsen Schadegg
It-sikkerhedskonsulent, politiassistent Poul Erik Høj Weidick
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
Dataspecialist, cand.soc. Lasse Overgaard Frandsen
Dataspecialist, cand.mag. Morten Engberg Helmstedt
Stabskonsulent, cand.soc. Anne Bech
HR-jurist, cand.jur. Mette Odel Spliid
Kommunikationskonsulent, cand.mag. Anders Due
Kommunikationsfuldmægtig, cand.mag. Natascha Helverskov Jørgensen (orlov)
Kommunikationsfuldmægtig, cand.mag. Hisar Sindi
Kommunikationsfuldmægtig, cand.comm. Stine Eimerdal
Controller, cand.merc.aud. Yimin Huang Nielsen
Kontorfunktionær Anette Sørensen
Kontorfunktionær Anne-Marie Müller
Kontorfunktionær Camilla Knutsdotter Hallingby
Kontorfunktionær Cathrine Bartels Thing
Kontorfunktionær Mette-Maj Aner Leilund
Kontorfunktionær Pernille Jensen
Informationssikkerhedskoordinator, Sune Lund Hansen
It-driftskoordinator, Søren Heine Sørensen
It-supporter, Poul Hansen
Stud.jur. Ahmad Wasfi Abd-Albaqi
Stud.it. Bjørn Alexander Wade Patterson
Stud.scient.pol. Emily Christine Reither
Stud.jur. Johan Daugaard Jacobsen
Stud.jur. Nanna Stig Pedersen

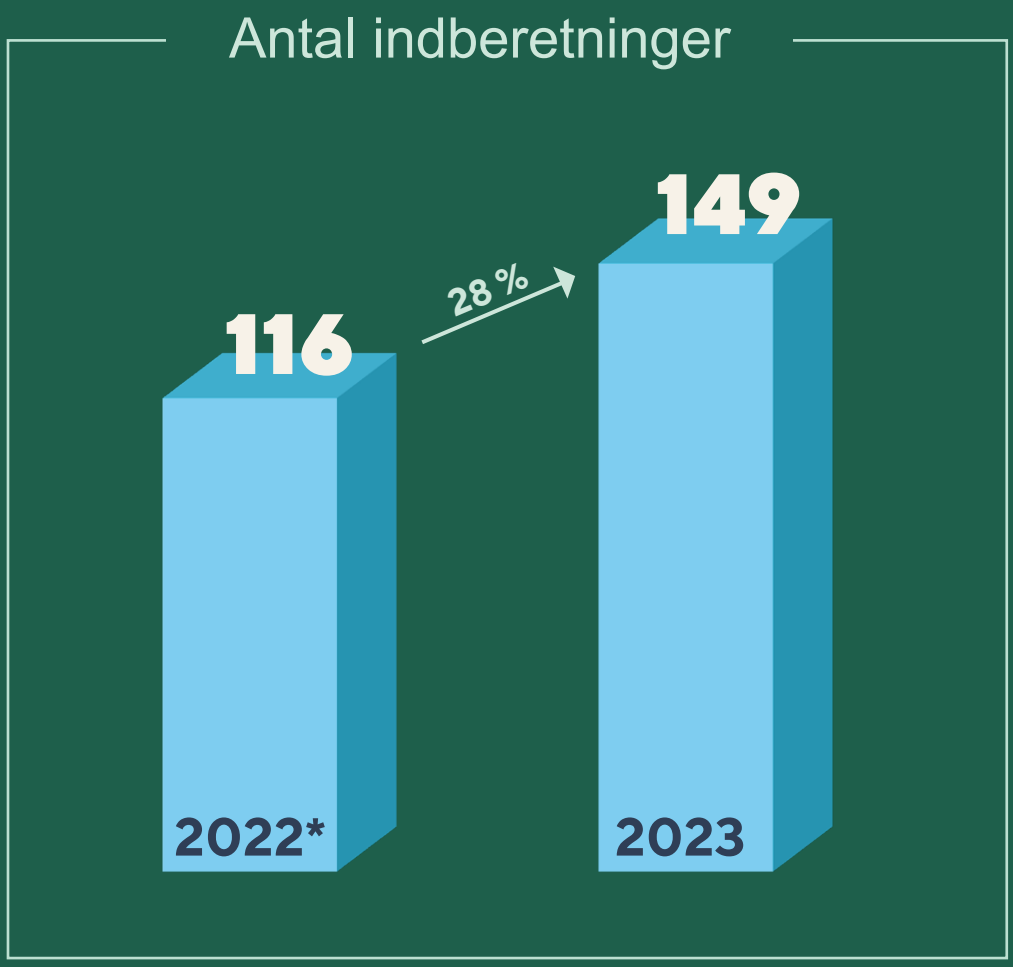
Den interne whistleblowerordning i Datatilsynet

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 og 2023 ikke modtaget nogle indberetninger.

Indberetninger til Den Nationale Whistleblowerordning



* I forbindelse med rapporteringen fra 2022 besluttede Den Nationalewhistleblowerordning at lave opgørelsen for periodem fra lovens ikrafttrædem dem 17. december 2021 til og med den 21. december 2022.

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

Som supplement til de interne whistleblowerordninger blev det endvidere besluttet, at Datatilsynet skulle etablere en ekstern whistleblowerordning til modtagelse og behandling af indberetninger vedrørende overtrædelser af 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.

Tallene for whistleblowerordningens første år viste, at mange forbandt ordningen med databeskyttelse – formentlig fordi ordningen er etableret i Datatilsynet – og derfor skiftede ordningen i 2023 navn til Den Nationale Whistleblowerordning. Herved blev det tydeligere signaleret 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.

I 2023 gennemførte Datatilsynet også en oplysningskampagne for at øge kendskabet til Den Nationale Whistleblowerordning bl.a. gennem annoncer i fagforeningsblade.

Den Nationale Whistleblowerordning fungerer uafhængigt og selvstændigt i forhold til Datatilsynets øvrige virksomhed. I 2023 var 10 medarbejdere tilknyttet whistleblowerordningen. Medarbejderne er alle 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 i forhold til deres arbejde.

I henhold til whistleblowerlovens § 27 skal myndigheder m.v. omfattet af reglerne om aktindsigt i offentlighedsloven mindst én gang årligt offentliggøre oplysninger om deres virksomhed efter whistleblowerloven.

Om indberetningerne i 2023

Den Nationale Whistleblowerordning modtog i perioden fra den 1. januar 2023 til og med den 31. december 2023 i alt 149 indberetninger. Det var 33 flere indberetninger end året før (svarende til en stigning på 28 %).

I samme periode færdigbehandlede Den Nationale Whistleblowerordning 147 indberetninger. Hovedparten af de 147 indberetninger var modtaget i 2023, men enkelte var indberetninger, som var modtaget ved udgangen af 2022.

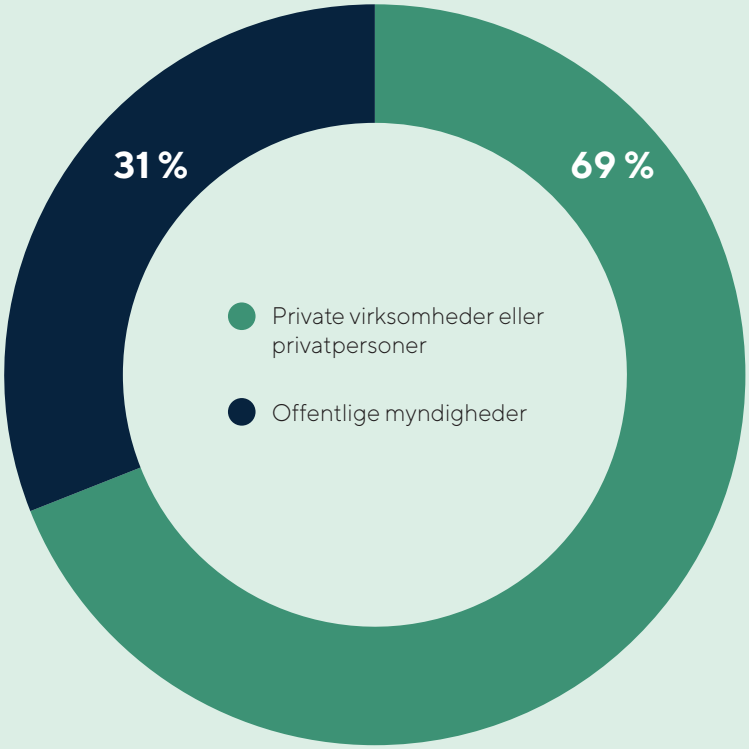
Af de 147 færdigbehandlede indberetninger vedrørte 102 indberetninger forhold hos private virksomheder eller privatpersoner, og 45 indberetninger vedrørte forhold hos offentlige myndigheder.

I 2023 havde Den Nationale Whistleblowerordning særligt fokus på at gøre opmærksom på ordningens brede anvendelsesområde, da 66 % af de modtagne indberetninger i 2022 vedrørte databeskyttelsesretlige forhold.

Bl.a. skiftede ordningen som nævnt ovenfor i begyndelsen af året navn til Den Nationale Whistleblowerordning. I 2023 var andelen af indberetninger, som handlede om databeskyttelsesretlige forhold, faldet til 35 %. Ligesom i 2022 drejede det sig navnlig om utilstrækkelig behandlingssikkerhed og overvågning af ansatte.

For de resterende sager vedrørte disse bl.a. særligt problemer med det psykiske arbejdsmiljø på arbejdspladsen, og 3 % omhandlede egentlig chikane. Herudover fyldte også for-

Hvem blev der indberettet om?



hold relateret til social- og sundhedsarbejde og sager om mulig økonomisk svindel.

Af de 147 færdigbehandlede indberetninger i 2023 fandt Den Nationale Whistleblowerordning i 48 sager grundlag for at videregive oplysninger om et eller flere forhold i indberetningerne til videre foranstaltning hos relevante myndigheder, herunder to sager til politiet. Det svarede til 33 % af de færdigbehandlede indberetninger i 2023 og var en stigning i forhold til 2022, hvor 26 % af sagerne blev videregivet.

24 indberetninger blev efter endt undersøgelse vurderet til at omhandle forhold, som ikke krævede yderligere opfølgning, jf. whistleblowerlovens § 21.

12 indberetninger blev afsluttet, fordi det ikke var muligt at få tilstrækkelige oplysninger til, at Den Nationale Whistleblowerordning kunne træffe afgørelse i sagerne.

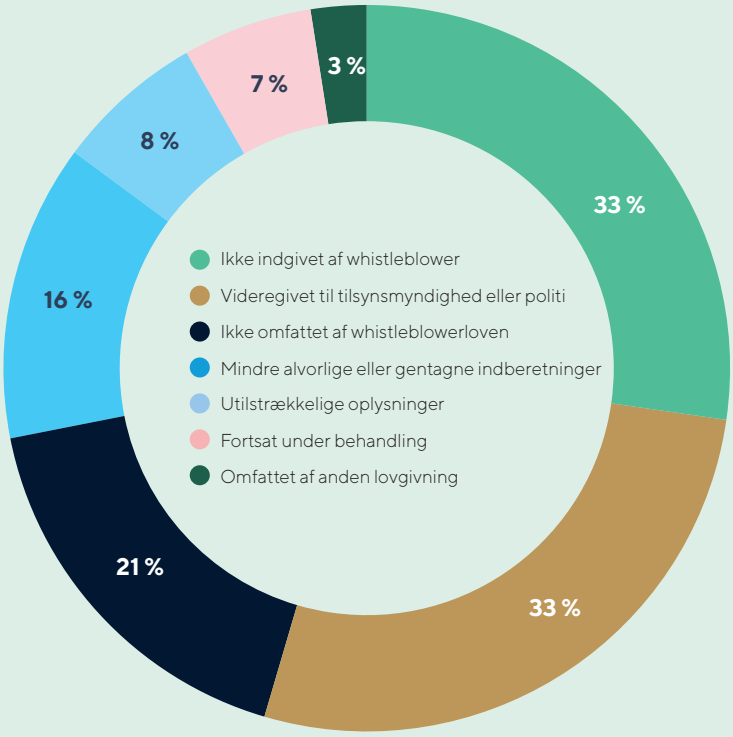
31 indberetninger faldt uden for whistleblowerlovens anvendelsesområde, og 48 indberetninger var indgivet af personer, som ikke var whistleblowere i lovens forstand. Disse personer blev i stedet – så vidt muligt – vejledt om mulighederne for at kontakte andre instanser.

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

11 indberetninger var fortsat under behandling pr. 31. december 2023.

Alle sager afsluttet i 2023 blev færdigbehandlet inden for tre måneder og dermed inden for fristerne i whistleblowerlovens § 20, stk. 2. Den gennemsnitlige sagsbehandlingstid var 23 dage.

Udfald af indberetningerne



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 med senere ændringer 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 med senere ændringer om retshåndhævende myndigheders behandling af personoplysninger.
- Tv-overvågningsloven
- Lovbekendtgørelse nr. 1190 af 11. oktober 2007 med senere ændringer 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 Efter- forskningsstøttedatabase (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 For- svarets internationale operative virke.
- 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 med senere ændringer 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 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 standard- indstillinger
- Vejledning af juli 2018 om de registreredes rettigheder
  - Tidsfrister og krav (særligt målrettet mindre virksomheder)
  - Retten til sletning (særligt målrettet mindre virksomheder)
  - Retten til indsigt (særligt målrettet mindre virksomheder)
  - Oplysningspligt (særligt målrettet mindre virksomheder)
- 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 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 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
- Vejledende tjekliste af januar 2023 ved skolers brug af billeder og video
- Vejledning af marts 2023 om databeskyttelse i ansættelsesforhold
- Vejledning af marts 2023 om udmåling af bøder til fysiske personer
- Vejledning af juni 2023 om direkte markedsføring
- Vejledning af juni 2023 om adfærdskodekser
- Vejledning af juni 2023 om tv-overvågning – private virksomheder
- Vejledning af juli 2023 om rollefordeling i forskningsprojekter
- Vejledning af oktober 2023 om offentlige myndigheders brug af kunstig intelligens – Inden I går i gang
- Vejledning af november 2023 om tv-overvågning – offentlige myndigheder
- Vejledning af december 2023 om tv-overvågning – boligorganisationer
- Vejledning af december 2023 om adgangsrettigheder

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 per- sonoplysninger.
- 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 radikalise- ring 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 (Vejledning 1/2019)
- Adfærdskodekser som redskab til overførsler (Vejledning 4/2021)
- Akkreditering (Vejledning 4/2018)
- Anvendelsen af databeskyttelsesforordningens artikel 65, stk. 1, litra a (Vejledning 3/2021)
- Art. 6, stk. 1, litra b, i databeskyttelsesforordningen som behandlingshjemmel ved udbud af online tjenester (Vejledning 2/2019)
- Anmeldelse af brud på persondatasikkerheden (Vejledning 9/2022)
- Ansigtsgenkendelsesteknologi på retshåndhævelsesområdet (Vejledning 05/2022)
- Anvendelse af lokaliseringsdata og kontaktopsporingsværktøjer i forbindelse med Covid-19-ud- bruddet (Vejledning 4/2020)
- Anvendelse og fastsættelse af administrative bøder i henhold til databeskyttelsesforordningen (wp253)
- Automatiske individuelle afgørelser og profilering (wp251)
- Behandling af personoplysninger i forbindelse med forbundne køretøjer og mobilitetsrelaterede applikationer (Vejledning 1/2020)

- Behandling af sundhedsdata med henblik på videnskabelig forskning i forbindelse med Covid-19-udbruddet (Vejledning 3/2020)
- Beregning af administrative bøder under databeskyttelsesforordningen (Vejledning 04/2022)
- Bindende virksomhedsregler (BCR) for dataansvarlige, standardansøgning samt elementer og principper, der skal være indeholdt (Anbefalinger 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)
- Certificering (Vejledning 1/2018)
- Certificering som et redskab til overførsler (Vejledning 07/2022)
- Dataansvarlig og databehandler (Vejledning 7/2020)
- Dataportabilitet, retten til (wp242)
- Databeskyttelsesrådgivere, DPO'er (wp243)
- Det juridiske grundlag for lagring af kreditkortdata med det ene formål at lette yderligere onlinetransaktioner (Anbefaling 2/2021)
- Eksempler på meddelelse om brud på persondatasikkerheden (Vejledning 1/2021)
- 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 08/2022)
- Målrettet markedsføring i forhold til brugere af sociale medier (Vejledning 8/2020)
- Relevant og begrundet indsigelse i henhold til databeskyttelsesforordningen (Vejledning 9/2020)
- Restriktioner i henhold til artikel 23 i databeskyttelsesforordningen (Vejledning 10/2020)
- Retten til indsigt (Vejledning 01/2022)
- Samtykke i henhold til databeskyttelsesforordningen (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)
- Teknisk anvendelsesområde for artikel 5, stk. 3, i ePrivacy-direktivet (Vejledning 2/2023)
- Territorialt anvendelsesområde for databeskyttelsesforordningen (Vejledning 3/2018)
- Tredjelandsoverførsler, artikel 37 i retshåndhævelsesdirektivet (Vejledning 01/2023)
- Tredjelandsoverførsler, overførsel af personoplysninger mellem offentlige myndigheder (Vejledning 2/2020)
- Tredjelandsoverførsler, supplerende foranstaltninger for at sikre et tilstrækkeligt beskyttelsesniveau (Anbefaling 1/2020)
- Tredjelandsoverførsler, tilstrækkeligt databeskyttelsesniveau (wp254)
- Tredjelandsoverførsler, undtagelser i særlige situationer (Vejledning 2/2018)
- Tredjelandsoverførsler, tilstrækkeligt databeskyttelsesniveau i henhold til retshåndhævelsesdirektivet (Anbefaling 1/2021)
- Virtuelle stemmeassistenter (Vejledning 2/2021)
- Vildledende designs på sociale medier (Vejledning 03/2022)

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

Telefon: 33 19 32 00
Mail: dt@datatilsynet.dk
Hjemmeside: datatilsynet.dk

Foto og layout: Datatilsynet
Tryk: Prinfo

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

DATATILSYNET

Ansvarlig anvendelse af borgernes data i et digitaliseret samfund

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby