# Årsberetning
2024

DATATILSYNET

# Datatilsynet

Årsberetning
2024

# Indhold

# Til Folketinget

Året 2024 var for Datatilsynets vedkommende endnu et år præget af et højt aktivitetsniveau med mange vigtige vejledningsinitiativer, større sagskomplekser og opgaver af international karakter. Der blev registreret 18.816 nyoprettede sager, hvilket er 754 flere sager end sidste år, som ellers var et rekordår med det hidtil højeste antal nyoprettede sager.

Datatilsynets arbejdsfelt er bredt og varierer, 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 endvidere aktivt i internationalt arbejde, herunder navnlig i EU.

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.

**Særlig indsats i forhold til kunstig intelligens**
Den internationale databeskyttelsesdag blev i januar 2024 markeret af Datatilsynet ved, at tilsynet inviterede til paneldebat om kunstig intelligens (AI). I debatten rettede Datatilsynet fokus mod to centrale områder inden for brug af AI. Panelet debatterede potentialet og udfordringerne ved AI i sundhedsvæsenet, herunder om AI kan understøtte et presset sundhedssystem. Samtidig diskuterede panelet de væsentligste gevinster og risici ved danske organisationers brug af generativ AI, som hastigt vinder indpas. Der var også mulighed for, at de ca. 250 deltagerne kunne stille spørgsmål til panelet.

I oktober 2023 offentliggjorde Datatilsynet en vejledning om offentlige myndigheders brug af AI, der kan benyttes ved udvikling og brug af kunstige intelligensløsninger, ligesom tilsynet foretog en kortlægning af brugen af AI på tværs af den offentlige sektor. Datatilsynet fortsatte i hele 2024 med at have et styrket fokus på brug af AI. Det skete bl.a. gennem etablering af en regulatorisk sandkasse for AI, hvor udvalgte virksomheder og myndigheder har fået mulighed for at få praksisnær rådgivning og vejledning af Datatilsynet om udvikling og brug af AI-løsninger. I maj 2024 offentliggjorde Datatilsynet også to skabeloner til gennemførelse af konsekvensanalyser, som virksomheder og myndigheder kan benytte sig af. Den ene skabelon vedrører AI-løsninger, og den anden er af mere generisk karakter.

**Børn og online spil**
På det nordiske møde i Helsinki i efteråret 2022 besluttede de nordiske datatilsyn på initiativ fra det danske datatilsyn at nedsætte en fælles nordisk arbejdsgruppe om børn og onlinespil. Datatilsynet har deltaget meget aktivt i arbejdsgruppen, som på det nordiske møde i Oslo i maj 2024 fik vedtaget et sæt fælles principper, som skal styrke databeskyttelse af børn i forbindelse med online spil. Principperne, der er udarbejdet på engelsk, blev offentliggjort i juni 2024 og er tilgængelige på bl.a. Datatilsynets hjemmeside.

**GDPR-univers til foreninger**
Et andet væsentligt vejledningsinitiativ i 2024 var lanceringen i juni af et nyt vejledningsunivers om databeskyttelsesforordningen (GDPR) til foreninger i Danmark. Vejledningsuniverset er opdelt i 3 hoved-kategorier af foreninger (boligforeninger, frivillige foreninger og nonprofitorganisationer) med henblik på at sikre, at det er nemt for hver af disse grupper af foreninger at navigere igennem informationer, konkrete råd og eksempler, der er skræddersyet til de udfordringer og krav, som de står overfor. Vejledningsuniverset blev udviklet i tæt samarbejde med en række foreninger, der repræsenterer målgruppen.

**Flere vejledningsområder ved brud på persondatasikkerheden**
I 2023 gennemførte og lancerede tilsynet 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. På baggrund af en løbende evaluering af dette projekt lykkedes det Datatilsynet i løbet af 2024 at optimere de interne procedurer i forbindelse med vejledningsindsatsen yderligere og fordoble antallet af vejledningsområder.

**Overførsel af personoplysninger til USA**
Datatilsynet spilede i 2024 også en særdeles aktiv rolle i forbindelse med EU-Kommissionens første evaluering af EU-U.S. Data Privacy Framework (DPF). En medarbejder fra Datatilsynet var med, da en europæisk delegation i juli 2024 var i Washington DC for at evaluere afgørelsen. Senere udarbejdede EU-Kommissionen en afsluttende rapport til EU-Parlamentet og Rådet, som konkluderede, at de fornødne procedurer er på plads for at sikre, at DPF-ordningen fungerer efter hensigten.

**Strategi for en data- og risikobaseret indsats mv.**
I løbet af 2024 har Datatilsynet også fulgt op på den opdaterede strategi for en data- og risikobaseret indsats, som tilsynet offentliggjorde i januar 2024. Der blev bl.a. etableret og implementeret processer for løbende monitering af datakvaliteten af Datatilsynets egne data, udviklet og idriftsat et internt datavarehus med relevante data og dataanalyser, ligesom der blev udarbejdet en ny model for udvælgelse af fokusområder.

Datatilsynet tilpassede i 2024 også tilsynets hjemmeside med henblik på at gøre det nemmere for brugerne – både borgere og dem, der behandler data – at finde relevant information og navigere lettere rundt.

Endvidere reorganiserede Datatilsynet i 2024 tilsynets telefonrådgivning, ligesom der var fokus på at sikre ordentlige fysiske rammer for telefonrådgivningen til gavn for ikke kun brugerne af telefonrådgivningen, men også de medarbejdere der betjener den.

Valby, maj 2025

Kristian Korfits Nielsen
Formand, Datarådet

Cristina Angela Gulisano
Direktør, Datatilsynet

## Om Datatilsynets årsberetning

Datatilsynets årsberetning for 2024 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 EØS-medlemslandenes nationale ret.

Årsberetningen indeholder omtale af væsentlige aktiviteter for Datatilsynet i 2024, 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.

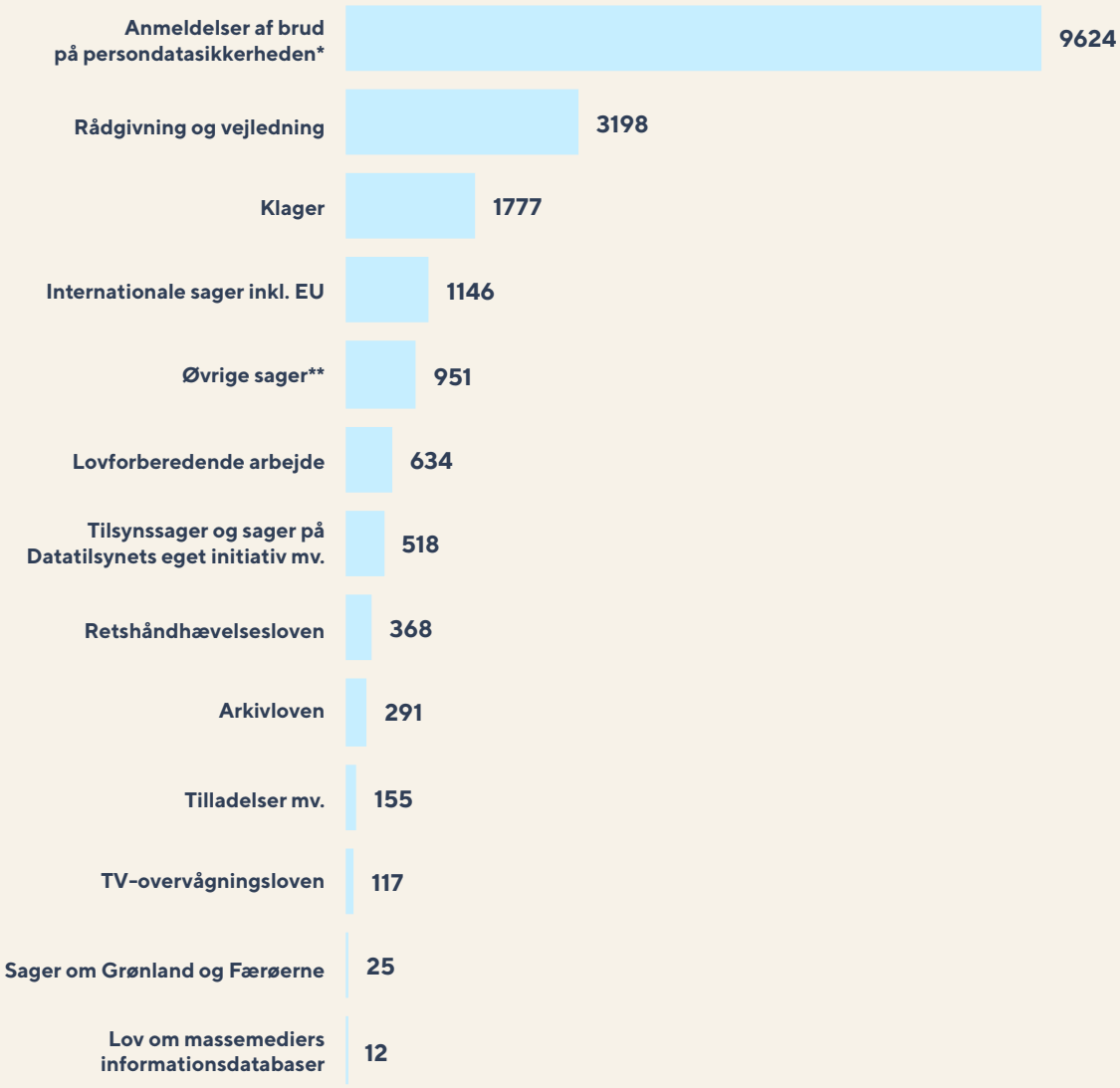
På Datatilsynets hjemmeside offentliggør tilsynet løbende udtalelser og afgørelser i sager, som vurderes at være af generel interesse. Datatilsynet kan således henvise til sin hjemmeside for yderligere oplysninger. Årsberetningen sendes endvidere til Europa-Kommissionen og Det Europæiske Databeskyttelsesråd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

På næste side findes oplysninger om antallet af nye sager, som er oprettet i Datatilsynets journalsystem i 2024.

En del af Datatilsynets sagsbehandling omfatter 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 **18.816** nye sager i 2024.

# Oprettede sager i 2024: 18.816




**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

**3.198** sager i alt

**2.068**
Sager vedr. private

**934**
Sager vedr. offentlige myndigheder

**196**
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, og at 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 2024 offentliggjort **16** nye eller opdaterede nationale vejledninger, hjemmesidetekster mv. om databeskyttelsesreglerne, som supplerer de 68 nationale vejledninger og vejledende tekster mv., som tilsynet har offentliggjort fra 2017 til 2023. De nye vejledningsinitiativer omfatter bl.a. en delvis opdatering af Datatilsynets vejledning om håndtering af brud på persondatasikkerheden, en justering af tilsynets vejledende tekst om Datatilsynets praksis i forhold til optagelse af telefonsamtaler og en ny vejledende tekst om kravene til underretning af registrerede. Endvidere er en af Datatilsynets mest populære vejledninger i form af vejledningen om overførsel af personoplysninger til tredjelande blevet opdateret.

Datatilsynet yder også en aktiv indsats på vejledningsområdet i europæiske sammenhænge og har i regi af Det Europæiske Databeskyttelsesråd bidraget til udarbejdelsen af **7** nye fælleseuropæiske vejledninger og udtalelser om databeskyttelsesforordningen og retshåndhævelsesdirektivet.

Alle de mange nævnte vejledninger, udtalelser og hjemmesidetekster 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 2024 f.eks. til stede med en stand på Digitaliseringsmessen, der er en af Danmarks største begivenheder om offentlig digitalisering, ligesom tilsynet deltog i konferencen Lærfest, der er den største fagmesse i Danmark om læremidler og god undervisning.

## Ny vejledning om 10 typiske brud på persondatasikkerheden

Datatilsynet modtager hver uge flere hundrede anmeldelser om brud på persondatasikkerheden. Mange af dem vedrører situationer, hvor der på forskellig vis utilsigtet gives adgang til eller videregives personoplysninger til uvedkommende. Det er ofte de samme typescenarier, der går igen, og mange af bruddene kunne formentlig være undgået, hvis organisationen havde haft de rette sikkerhedstiltag på plads.

Med udgangspunkt i 10 typiske brud offentliggjorde Datatilsynet derfor i januar 2024 en række gode råd til, hvilke sikkerhedstiltag der kan overvejes for at nedbringe risikoen for disse typer af brud. Sikkerhedstiltagene kan både være af teknisk og organisatorisk karakter, og i mange tilfælde er det relevant med begge dele. Et typisk brud er eksempelvis, hvor en medarbejder ved en fejl sender en mail med oplysninger, der er tiltænkt én modtager, til en anden modtager med samme eller forvekslelig navn, fordi navnene forveksles i selve afsendelsesøjeblikket. Det kan også være den situation, hvor der utilsigtet eksponeres oplysninger om en beskyttet adresse, fordi oplysningen om adressebeskyttelse på grund af dårligt design, kodefejl eller manglende tests ikke slår igennem fra ét it-system til et andet. Til hvert af de 10 typiske brud er der angivet forslag til relevante sikkerhedsmæssige tiltag, der kan overvejes, ligesom der også flere steder henvises til foranstaltninger fra Datatilsynets katalog over sikkerhedsforanstaltninger.

Vejledningen er især målrettet medarbejdere, der har mulighed for at påvirke organisationens regler, procedurer, undervisning og andre awareness-aktiviteter samt tekniske opsætninger i it-miljøer for derigennem at beskytte organisationen imod disse typiske brud på persondatasikkerheden. Alle, der ofte arbejder digitalt med personoplysninger, kan dog have gavn af et fokus på de beskrevne scenarier, da disse typer brud som nævnt tegner sig for en meget betragtelig andel af de brud, som anmeldes til Datatilsynet hver uge.

## Ny temaside til borgere om samtykke

Datatilsynet publicerede i februar 2024 på sin hjemmeside en ny temaside til borgere om samtykke. Det skyldtes, at der ofte er misforståelser omkring samtykke som værende det eneste behandlingsgrundlag. Det er således ikke altid nødvendigt for en myndighed eller virksomhed at indhente samtykke, før de må behandle personoplysninger, da samtykke kun er ét blandt flere lovlige hjemler.

På temasiden kan borgere også blive klogere på deres rettigheder og få hjælp til, hvordan de får indblik i, hvorfor en offentlig myndighed eller privat virksomhed behandler deres oplysninger. Endvidere findes der på siden en ordforklaring med de oftest anvendte ord inden for databeskyttelse, der kan være nyttige at kende, når man som borger er i kontakt med en myndighed eller virksomhed. Derudover indeholder temasiden en liste med ofte stillede spørgsmål vedrørende bl.a. sletning og ændring af oplysninger.

## Ændringer i Datatilsynets standarddatabehandleraftale

I marts 2024 foretog Datatilsynet to ændringer i tilsynets standarddatabehandleraftale vedrørende pligten til at indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs. Begge ændringer, der angik samme bestemmelse, bestod i:

- Bestemmelsen er nu blevet fremhævet som valgfri for den dataansvarlige og databehandleren at inkludere i databehandleraftalen.
- Bestemmelsens ordlyd er blevet ensrettet med ordlyden i den tilsvarende bestemmelse i EU-Kommissions standardkontraktbestemmelser for databehandleraftale af 4. juni 2021.

Forud for ændringerne havde Datatilsynet modtaget flere henvendelser om betydningen af den pågældende bestemmelse. Det blev bl.a. fremhævet, at bestemmelsen var udfordrende at arbejde med i praksis. Eftersom bestemmelsen ikke er et direkte krav efter databeskyttelsesforordningen, men har været et forsøg fra Datatilsynets side på at sikre, at den dataansvarlige forsat kan leve op til sine forpligtelser som dataansvarlig i tilfælde at databehandlerens konkurs, besluttede Datatilsynet at fremhæve, at bestemmelsen er valgfri. Tilsynet gjorde dog samtidig opmærksom på, at den dataansvarlige – uanset bestemmelsens indføjelse i databehandleraftalen eller ej – fortsat er ansvarlig for at sikre, at personoplysninger bliver tilstrækkelig beskyttet (slettet eller tilbageleveret) i tilfælde, hvor databehandleren er ophørt eller er gået konkurs.

Datatilsynets to ændringer blev forelagt Det Europæiske Databeskyttelsesråd (EDPB), som ikke havde indvendinger til ændringerne. Bestemmelserne – og de tilføjede ændringer – har derfor fortsat karakter af at være standardkontraktbestemmelser efter databeskyttelsesforordningens artikel 28, stk. 8.

Ændringerne i standarddatabehandleraftalen betyder i øvrigt ikke, at aftaler, der er indgået på den tidligere udgave af standarddatabehandleraftalen, bliver ugyldige. Datatilsynet forventer fortsat at acceptere sådanne databehandleraftaler, der er indgået ved brug af den tidligere udgave af standarden. Det forudsætter dog naturligvis, at ordlyden af aftalen ikke afviger fra standarden, og at standarden er udfyldt korrekt.

## Justering af praksis for optagelse af telefonsamtaler

I Datatilsynets vejledning fra november 2020 om optagelse af telefonsamtaler fremgik det, at medmindre der forelå særlige omstændigheder, krævede optagelse af telefonsamtaler til uddannelsesformål et samtykke. Derudover fremgik det, hvilke betingelser der skal være opfyldt for, at man kan optage telefonsamtaler til dokumentationsformål.

I april 2024 opdaterede Datatilsynet denne vejledning på baggrund af den seneste europæiske udvikling på området. Af den opdaterede vejledning fremgår det, at det nu er Datatilsynets opfattelse, at optagelse af telefonsamtaler til uddannelsesformål kan ske uden den registreredes samtykke, hvis den registrerede enten forud for opkaldet (ved tastetryk) eller i forbindelse med opkaldet kan frabede sig, at samtalen optages.

Der er ikke sket ændringer i muligheden for at optage telefonsamtaler til dokumentationsformål.

## Nye skabeloner til gennemførelse af konsekvensanalyser

Datatilsynet offentliggjorde i maj 2024 to nye skabeloner til gennemførelse af konsekvensanalyser, som myndigheder og virksomheder kan benytte sig af. Den ene skabelon vedrører AI-løsninger, og den anden er af mere generisk karakter.

En konsekvensanalyse er et værktøj, som gør det muligt at arbejde med de risici, som en behandlingsaktivitet kan indebære, på en systematisk måde. Analysen skal efter databeskyttelsesreglerne gennemføres, hvis en behandlingsaktivitet sandsynligvis vil indebære høje risici for de registrerede.

Datatilsynet har løbende kunnet konstatere, at virksomheder og myndigheder i mange tilfælde har udfordringer med at gennemføre konsekvensanalyser. Dette var f.eks. et af fundene i forbindelse med Datatilsynets kortlægning af brugen af kunstig intelligens i den offentlige sektor fra oktober 2023, og tilsynet har også truffet flere afgørelser vedrørende manglende eller utilstrækkelige konsekvensanalyser.

Formålet med skabelonerne er derfor at hjælpe virksomheder og myndigheder i deres arbejde med at gennemføre konsekvensanalyser. Skabelonen for AI indeholder bl.a. konkrete eksempler på risici og på foranstaltninger, som kan være relevante i arbejdet med at nedbringe disse risici.

## Nye tilføjelser til kataloget over sikkerhedsforanstaltninger

I 2023 offentliggjorde Datatilsynet som noget nyt et katalog over sikkerhedsforanstaltninger, som virksomheder og myndigheder kan bruge til at håndtere forskellige sikkerhedsrisici. Det er meningen, at foranstaltningskataloget løbende skal udbygges, og i 2024 blev yderligere 2 nye foranstaltninger tilføjet til kataloget.

### Softwaretest med fokus på sikkerhed

Foranstaltningen fokuserer på softwaretest med fokus på sikkerhed, som kan være med til at opdage sårbarheder i nyudviklet software.

Datatilsynet har en del praksis på dette område, og sagerne har ofte bund i erfaringer fra brud på persondatasikkerheden, som er sket på grund af bl.a. mangelfulde test.
Den nye foranstaltning begrænser sig ikke til sårbarheds- og penetreringstest, men beskriver mange typer af test, som kan være relevante at overveje. Når softwareudvikling ofte sker hos en leverandør, kan test eller krav til leverandørens test således være den eneste måde at sikre, at den nye software udvikles med fokus på sikkerhed.

Beskrivelsen af foranstaltningen berører også spørgsmålet om dokumentation, fordi dokumentation af test kan være afgørende for at kunne påvise, om man har gjort tilstrækkeligt for at undgå et brud på persondatasikkerheden.

### Styret og overvåget offentliggørelse af data

Foranstaltningen beskriver en række forebyggende tiltag, som kan mindske risikoen for utilsigtet offentliggørelse af personoplysninger. Foranstaltningen kommer også ind på en række korrigerende tiltag, der kan være med til at opdage allerede offentliggjorte personoplysninger.

Mange virksomheder og myndigheder offentliggør hyppigt dokumenter som led i deres arbejde, og Datatilsynet har set flere eksempler på brud på persondatasikkerheden i forhold til utilsigtet offentliggørelse af personoplysninger. Som dataansvarlig har man en forpligtelse til at beskytte personoplysninger mod utilsigtet offentliggørelse og sikre, at der føres passende kontrol med, at offentliggjort data ikke indeholder unødige personoplysninger.

## Ny praksis i forhold til indsigt i logfiler

Den 22. juni 2023 tog EU-Domstolen stilling til spørgsmålet om indsigt i logfiler. I EU-Domstolens dom fastslås det, at databeskyttelsesforordningens artikel 15, stk. 1, skal fortolkes således, at information vedrørende søgninger i en persons personoplysninger og vedrørende datoerne for og formålet med disse søgninger udgør information, som den berørte person i henhold til denne bestemmelse har ret til at få fra den dataansvarlige.

Samtidig fastslår EU-Domstolen dog, at bestemmelsen ikke giver ret til information om identiteten på de af den dataansvarliges ansatte, som har foretaget søgningerne under den dataansvarliges ledelse og efter instruks fra denne, medmindre denne information er nødvendig for, at den registrerede effektivt kan udøve sine rettigheder i henhold til denne forordning, og forudsat at de ansattes rettigheder og frihedsrettigheder iagttages.

Ovenstående vil derfor også være Datatilsynets praksis fremadrettet. Den nye praksis betyder, at man som dataansvarlig skal udlevere en kopi af de personoplysninger om en registreret, som man har registreret om vedkommende i sin log. Det vil f.eks. være oplysninger om søgninger i vedkommendes oplysninger og datoerne for (og formålet) med disse søgninger.

Man skal også oplyse om, hvem der har foretaget søgningen, hvis denne information – efter omstændighederne – er nødvendig for, at den registrerede effektivt kan udøve sine rettigheder. Det kan f.eks. være, hvis den registrerede mistænker, at der er foretaget uberettiget søgning på vedkommendes oplysninger. Man skal dog ikke udlevere navnet på den, som har foretaget søgninger, hvis man som dataansvarlig konkret vurderer, at udlevering af navnet vil kunne krænke dennes rettigheder.

Som tommelfingerregel gælder i den forbindelse efter Datatilsynets opfattelse, at hvis den registrerede alene har bedt om indsigt i loggen uden at angive et specifikt formål, vil hensynet til den, som har foretaget et opslag, ofte veje tungere end hensynet til den, som anmoder om indsigt i loggen. Hvis den registrerede derimod har brug for at vide, hvem der har slået op i loggen for at kunne kontrollere lovligheden af et opslag, f.eks. fordi den registrerede har grund til at mistænke, at der er sket uberettiget opslag, vil afvejningen i mange tilfælde falde ud til fordel for den, der anmoder om indsigt. I disse tilfælde skal man altså som udgangspunkt også oplyse om, hvem der har foretaget opslaget.

Der kan også stadigvæk gøres undtagelse til retten til indsigt efter databeskyttelsesforordningens artikel 15 i personoplysninger i en log, hvis et af de forhold, som fremgår af databeskyttelseslovens § 22 gør sig gældende.

For at kunne anvende databeskyttelseslovens § 22 er det dog et krav, at man foretager en konkret afvejning af de modstående interesser, som er nævnt i bestemmelsen – altså hensynet til den registrerede og det hensyn man påberåber sig for at gøre undtagelse til indsigtsretten. Det vil altså ikke være tilstrækkeligt blot at redegøre for indholdet i bestemmelsen som begrundelse for at afvise en anmodning om indsigt. Man vil heller ikke kunne bruge ressourcehensyn som begrundelse for at undlade at give indsigt, ligesom man heller ikke vil kunne henvise til, at man ikke kan bruge loggen til at kontrollere behandlingens lovlighed.

## GDPR-univers for små foreninger

I juni 2024 lancerede Datatilsynet et nyt vejledningsunivers om GDPR for små foreninger, der tilbyder gode råd og konkrete eksempler, der er skræddersyet til de udfordringer, som mindre foreninger står overfor.

Universet er bygget op omkring 7 trin, som foreninger kan følge for at overholde GDPR. Hvert trin indeholder konkrete eksempler og gode råd, som er kategoriseret efter forskellige typer af foreninger. Materialet består også af en omfattende FAQ såvel som jordnære beskrivelser af de grundlæggende begreber i GDPR.

GDPR-universet for små foreninger er udviklet i samarbejde med Andelsboligforeningernes Fællesrepræsentation (ABF), idrætsorganisationen DGI og Fonden for Socialt Ansvar som repræsentanter for denne målgruppe.

## Fælles nordiske principper om databeskyttelse i forbindelse med børn og online spil

De nordiske datatilsynsmyndigheder vedtog den 30. maj 2024 på det årlige nordiske møde et sæt fælles principper, som skal styrke databeskyttelsen af børn i forbindelse med online spil. Formålet er at gøre dataansvarlige spiludviklere opmærksom på nogle af de GDPR-relaterede overvejelser, de som minimum bør gøre sig for at fremme beskyttelsen af spillernes personoplysninger.

Arbejdsgruppen, der har udarbejdet principperne, blev nedsat på det nordiske møde i Helsinki i efteråret 2022 efter forslag fra det danske datatilsyn. Baggrunden for det danske initiativ var en rapport fra tænkehandletanken DataEthics og Ingeniørforeningen i Danmark (IDA) om den udbredte brug af online spil blandt børn og behovet for at styrke beskyttelsen af spillernes personoplysninger og privatliv.

## Vejledning i forbindelse med brud på persondatasikkerheden

De fleste brud på persondatasikkerheden anmeldes til Datatilsynet via virk.dk på en online-blanket, som hjælper med at sikre, at alle nødvendige oplysninger gives fra starten. Blanketten tilrettes løbende på baggrund af erfaringer og indgår dermed som en del af vejledningen til organisationer, der anmelder brud.

I tilfælde, hvor et brud på persondatasikkerheden kræver akut handling, tager Datatilsynet ofte direkte kontakt til anmelderen. Dette kan f.eks. være nødvendigt, hvis der er behov for at rydde op efter et brud, eller hvis personer, hvis oplysninger er blevet berørt, hurtigt skal underrettes. Denne direkte kontakt er samtidig en del af Datatilsynets målrettede vejledning.

Samtidig giver tilsynet i forbindelse med, at behandlingen af en anmeldelse af et brud på persondatasikkerheden afsluttes, anmelderen – så vidt muligt – links til relevante vejledninger, herunder materialer fra Datatilsynets foranstaltningskatalog. Vejledningerne er handlingsanvisende og indeholder både tekniske og organisatoriske foranstaltninger. De spænder bredt og omfatter ikke kun Datatilsynets egne materialer, men også vejledninger, der er udarbejdet i samarbejde med Sikkerdigital.dk og brancheorganisationer som Dansk Industri, Dansk Erhverv og SMV Danmark. Derudover henvises der også til vejledninger fra Center for Cybersikkerhed.

Den målrettede vejledningsindsats, der blev indledt i efteråret 2023, er i løbet af 2024 blevet forbedret yderligere, ligesom det er lykkes Datatilsynet at fordoble antallet af vejledningsområder. F.eks. vil Datatilsynet fremover automatisk – baseret på et CVR-opslag – henvise til GDPR-universet for små foreninger, når disse – uanset størrelse – anmelder et brud på persondatasikkerheden.

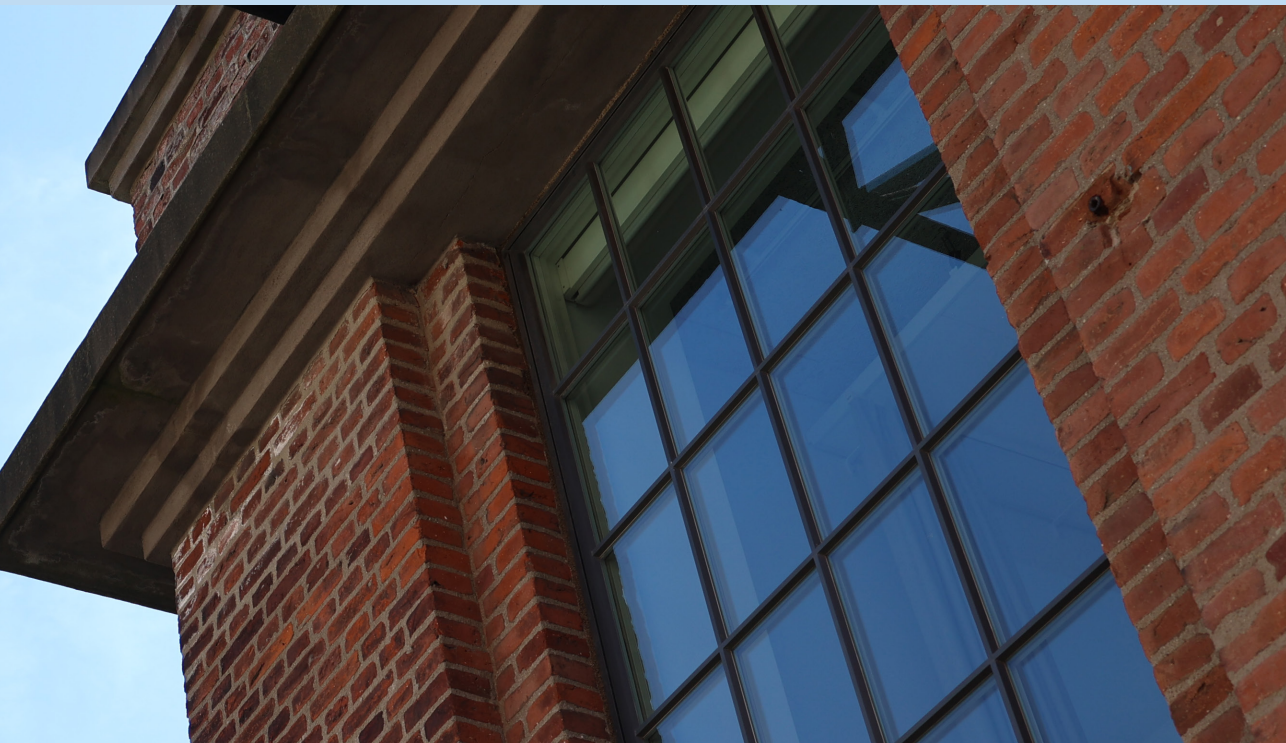
## Regulatorisk sandkasse for kunstig intelligens (AI)

Som led i regeringens digitaliseringsstrategi lancerede Datatilsynet i samarbejde med Digitaliseringsstyrelsen i marts 2024 en regulatorisk sandkasse for AI, hvor virksomheder og myndigheder kan få adgang til relevant ekspertise og vejledning i GDPR, når de udvikler eller anvender AI-løsninger.

Hensigten med den regulatoriske sandkasse er bl.a. at understøtte innovation og brugen af gode AI-løsninger gennem projekt- og praksisnær vejledning om GDPR og dermed bidrage til at sikre en ansvarlig og lovlig anvendelse af AI-løsninger. Formålet med den regulatoriske sandkasse er også at bidrage til at nedbringe tiden fra udvikling til drift og sikre, at færre projekter strander eller helt afsluttes på grund af usikkerhed om de regulatoriske rammer.

Længden af et sandkasseforløb afhænger af det konkrete projekts omfang og kompleksitet. Det er dog forventningen, at et typisk projektforløb vil være mellem 3 og 6 måneder. For hvert sandkasseforløb udarbejdes en individuel projektplan, der beskriver, hvad det enkelte sandkasseforløb vil bestå af. I den sidste del af forløbet vil der i samarbejde med den deltagende organisation blive udarbejdet en rapport baseret på de erfaringer, sandkasseforløbet har resulteret i, så andre kan drage nytte af dem.

Datatilsynet og Digitaliseringsstyrelsen udvalgte – efter fristen for den første ansøgningsrunde var udløbet i slutningen af maj 2024 – de to første forløb i den regulatoriske sandkasse. Ved udvælgelsen blev der særligt lagt vægt på at vælge projekter, hvor den viden, som oparbejdes gennem projektforløbet i samarbejde med den deltagende virksomhed eller myndighed, har størst mulig nytteværdi for andre aktører og for samfundet. Rapporterne om de to første sandkasseforløb forventes offentliggjort i begyndelsen af 2025, hvor der også vil blive igangsat en ny ansøgningsrunde med henblik på at finde frem til de næste projekter, der skal indgå i den regulatoriske sandkasse.



# 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 2024.

## Datasæt til udvikling af sprogteknologi

På baggrund af to konkrete henvendelser fra henholdsvis Sønderborg Kommune og Alexandra Instituttet vurderede Datatilsynet i begyndelsen af 2024 – efter at sagen havde været behandlet på et møde i Datarådet – i hvilket omfang etablering og deling af datasæt til brug for udvikling af sprogteknologi kan ske inden for rammerne af databeskyttelsesreglerne.

Sønderborg Kommune havde anmodet om Datatilsynets vurdering af, om kommunen inden for rammerne af databeskyttelsesreglerne kan offentliggøre et datasæt, som kommunen har etableret og benyttet til udvikling af en AI-model, samt om kommunen kan offentliggøre den udviklede model.

Datatilsynet vurderede i den forbindelse, at databeskyttelsesreglerne ikke er til hinder for, at grundmodellen offentliggøres. Med hensyn til offentliggørelse af datasættet er forudsætningen for, at datasættet lovligt kan offentliggøres, at de personoplysninger, der indgår i datasættet, er lovligt indsamlet og behandlet.

Det var endvidere Datatilsynets vurdering, at Sønderborg Kommune lovligt kunne indsamle og behandle de pågældende oplysninger, og at kommunen lovligt kan offentliggøre datasættet. Kommunen skal dog som led i sin eventuelle offentliggørelse være opmærksom på særligt kravene om dataminimering, rigtighed og lovlighed.

Af henvendelsen fra Alexandra Instituttet fremgik det, at instituttet ønskede Datatilsynets vurdering af muligheden for at etablere og dele et datasæt, der skal bruges til udvikling af dansk sprogteknologi.

Datatilsynet tog i den forbindelse bl.a. stilling til spørgsmål om behandlingsgrundlag i relation til etablering og deling af sådanne datasæt, om anonymisering samt om, hvorvidt der er tale om behandling af særlige kategorier af personoplysninger, når der sker behandling af personoplysninger i form af en persons stemme.

Datatilsynet vurderede i det konkrete tilfælde, at indsamling og behandling af personoplysninger som led i etableringen og offentliggørelsen af datasættet kunne ske under henvisning til opfyldelsen af en kontrakt. Datasættet kunne derimod efter Datatilsynets vurdering ikke anses for at være anonymiseret i databeskyttelsesretlig forstand. Det skyldes, at der findes hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse med henblik på at identificere de personer, der fremgår af datasættet.

Herudover vurderede Datatilsynet, at behandlingen – uanset at der kan være tale om biometriske data – ikke er omfattet af forbuddet mod behandling af særlige kategorier af personoplysninger i GDPR. Det skyldtes, at Alexandra Instituttets behandling af oplysningerne ikke skete med det formål entydigt at identificere en fysisk person.

## Børn og sociale medier

Børns Vilkår rettede i foråret 2024 henvendelse til Datatilsynet om en række forskellige sociale mediers (Meta, TikTok, Google, X og Snap Inc.) behandling af oplysninger om børn. Børns Vilkår oplyste i henvendelsen, at de sociale medier ikke overholder de nationalt fastsatte aldersgrænser, herunder aldersgrænsen i den danske databeskyttelseslov, som gælder for samtykke i forbindelse med udbud af såkaldte informationssamfundstjenester direkte til børn. Børns Vilkår påpegede også, at børn ikke kan indgå en kontrakt med de sociale medier, fordi de er umyndige.

I et brev til Børns Vilkår erklærede Datatilsynet – efter at sagen havde været behandlet på et møde i Datarådet – sig indledningsvis enig med Børns Vilkår i, at det er vigtigt, at oplysninger om børn behandles i overensstemmelse med databeskyttelsesreglerne, herunder at der passes ordentligt på oplysningerne. Børn skal efter databeskyttelsesreglerne have en særlig beskyttelse, fordi de ofte er mindre bevidste om de risici og konsekvenser, der kan være forbundet med behandling af personoplysninger.

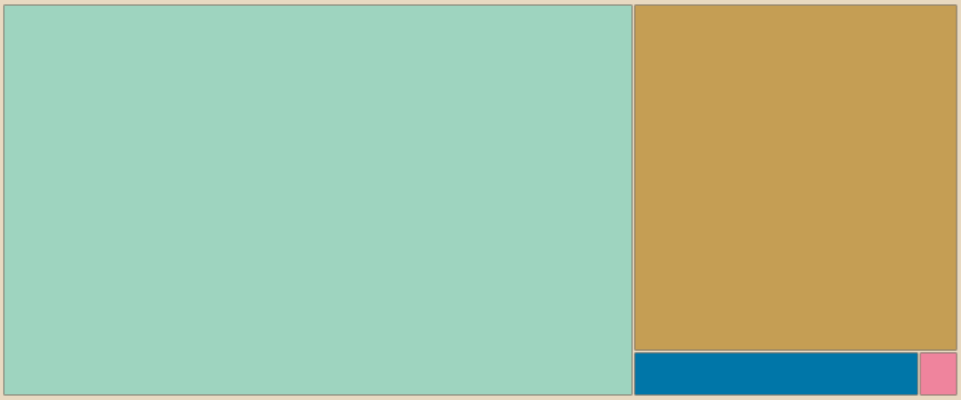
Samtidig oplyste Datatilsynet, at de nævnte sociale medier – som led i den behandlingsaktivitet, som består i oprettelse af en profil – normalt ikke behandler personoplysninger på baggrund af børnenes samtykke. Disse sociale medier henviser i stedet til, at oplysningerne behandles af hensyn til opfyldelsen af en kontrakt (de nævnte sociale mediers servicevilkår) med børnene. Aldersgrænsen for børns samtykke har derfor ikke nødvendigvis betydning for børns generelle adgang til de nævnte sociale medier.

Endvidere oplyste Datatilsynet, at spørgsmålet om, hvorvidt et barn kan indgå en gyldig kontrakt ikke reguleres af databeskyttelsesreglerne, men af aftaleretlige regler, og selv om tilsynet har en vis begrænset mulighed for at påse, at der eksisterer en kontrakt, falder det uden for Datatilsynets kompetence at foretage en mere dybdegående fortolkning og vurdering af eventuelt indgåede aftaler. Datatilsynet ville dog i forlængelse af Børns Vilkårs henvendelse indgå i en dialog med Justitsministeriet, som er ressortmyndighed for bl.a. værgemålsloven, omkring børns adgang til at indgå aftaler, herunder acceptere sociale mediers servicevilkår.

Datatilsynet bemærkede endelig, at uanset hvilken aldersgrænse et socialt medie (lovligt) måtte have valgt, skal mediet – også som følge af databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger – indføre passende foranstaltninger for at sikre, at den valgte grænse overholdes, f.eks. relevante aldersverifikationsmekanismer. Datatilsynet oplyste i forlængelse heraf, at der i forhold til spørgsmålet om aldersverifikation pågår en række aktiviteter herom både nationalt og i EU, herunder i regi af Det Europæiske Databeskyttelsesråd (EDPB).

# Høring over lovforslag mv.

**634** sager i alt



| | | |
|---|---|---|
| **418** | | Høringer over bekendtgørelser, cirkulærer, vejledninger, anordninger mv. |
| **191** | | Høringer over betænkninger, lovforslag, EU-retsakter, konventioner mv. |
| **22** | | Folketingsspørgsmål, private lovforslag, folketingsbeslutninger, høringer mv. |
| **3** | | 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 **624** sager i 2024 vedrørende høringer over lovforslag m.v.*

Datatilsynet forholder sig i sine udtalelser til de eventuelle databeskyttelsesretlige problemstillinger i lovudkastene 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 udkast til lovforslag, som har været sendt i høring hos Datatilsynet i 2024.

## Ændring af tv-overvågningsloven mv. (gennemførelse af Bandepakke IV)

I februar 2024 afgav Datatilsynet en udtalelse over Justitsministeriets udkast til forslag til lov om ændring af straffeloven, retsplejeloven, tv-overvågningsloven og en række forskellige andre love, der havde til formål at gennemføre dele af den politiske aftale om Bandepakke IV.

Datatilsynet udtalte sig særligt om ændringen af tv-overvågningsloven, som indebar en udvidelsen af det såkaldte afstandskrav. Konkret blev det foreslået at øge det areal, som en dataansvarlig må tv-overvåge, fra op til 30 m. til op til 100 m. for visse erhvervsdrivende og offentlige myndigheder. Dette blev foreslået med henblik på bl.a. at styrke politiets indsats mod bandekriminalitet. Ved at udvide afstandskravet ville politiet efter Justitsministeriets opfattelse få yderligere redskaber i kampen mod kriminalitet.

Datatilsynet udtalte, at selvom tilsynet anerkendte de saglige formål bag den foreslåede udvidelse af afstandskravet, rejste den foreslåede ændring væsentlige spørgsmål i relation til databeskyttelse.

Datatilsynet fandt det bl.a. yderst betænkeligt at indføre mulighed for at øge den afstand, som dataansvarlige kan foretage tv-overvågning på, da en sådan udvidelse ville medføre en markant øget overvågning af almindelige borgere, når de færdedes i det offentlige rum. Datatilsynet bemærkede i den forbindelse, at der allerede med afstandskravet på op til 30 m. skete indsamling og behandling af meget store mængder personoplysninger.

Endvidere fandt tilsynet det yderst betænkeligt, at private erhvervsdrivende og offentlige myndigheder mv. som konsekvens af lovforslaget ville skulle foretage tv-overvågning, som rækker ud over behandling af personoplysninger til deres egne formål, idet lovforslaget lagde op til, at de pågældende ville skulle foretage tv-overvågning til varetagelse af politiets opgave med at håndtere bl.a. bandekriminalitet. Datatilsynet udtalte hertil, at tv-overvågning med henblik på generel kriminalitetsbekæmpelse efter tilsynets opfattelse er en politimæssig opgave og ikke en opgave for de enkelte dataansvarlige.

Datatilsynet udtalte også, at den konsekvensanalyse vedrørende databeskyttelse, som Justitsministeriet havde foretaget i forbindelse med lovforslaget, efter tilsynets opfattelse ikke levede op til kravene i databeskyttelsesforordningens artikel 35, stk. 7.

## Lovforslag om uafhængige erklæringsudbydere vedrørende bæredygtighedsrapportering

Erhvervsstyrelsen sendte i september 2024 en høring over et udkast til et lovforslag, som regulerer uafhængige erklæringsudbydere og såkaldte verifikatorer.

Datatilsynet udtalte i sit høringssvar bl.a., at der efter tilsynets forståelse var uklarhed om, hvem som kunne agere som verifikator, herunder om der kunne være tale om en fysisk person. Herudover var der også andre spørgsmål i forbindelse med lovforslaget, som kunne give anledning til uklarhed om anvendelsen af databeskyttelsesreglerne. Datatilsynet udtalte derfor bl.a., at det var væsentligt, at dataansvarlige ved administration af loven er bevidste om, hvorvidt der behandles oplysninger, som er omfattet af databeskyttelsesreglerne eller ej.

Lovudkastet indeholdt også andre bestemmelser og bemærkninger, som efter Datatilsynets opfattelse kunne give anledning til uklarhed. Det gjaldt f.eks. en tvetydig formulering i lovudkastets bemærkninger om, at en bestemt udveksling af personoplysninger skulle leve op til reglerne i databeskyttelsesforordningen. Uanset at dette var korrekt, kunne det efter tilsynets opfattelse frygtes, at bemærkningen kunne læses sådan, at anden udveksling af (person)oplysninger ikke behøvede at leve op til databeskyttelsesreglerne.

I lovudkastet var der – i forbindelse med bestemmelser om kontrol og tilsyn –lagt op til at gøre nationale undtagelser fra databeskyttelsesforordningen. Det var imidlertid ikke klart for Datatilsynet, om det rent faktisk var tilsigtet at udnytte det nationale råderum. Datatilsynet lagde således generelt op til, at Erhvervsstyrelsen overvejede at præcisere en række forhold vedr. lovforslaget.

## Lov om Nemkontosystemet

I efteråret 2024 behandlede Datatilsynet en høring fra Digitaliseringsstyrelsen vedrørende et udkast til et lovforslag om et nyt Nemkontosystem, som Digitaliseringsstyrelsen skal udvikle, idriftsætte og eje.

Det fremgik bl.a. af lovudkastet, at Digitaliseringsstyrelsen skulle kunne "indhente de personoplysninger og oplysninger, som er nødvendige til brug for udvikling, drift, vedligeholdelse og forvaltning af Nemkontosystemet". Ikke bare fra told- og skatteforvaltningen, Det Centrale Personregister og fra Det Centrale Virksomhedsregister, men også fra "øvrige myndigheder".

Dette fandt Datatilsynet umiddelbart vidtgående, særligt fordi der i lovudkastets bemærkninger ikke var givet yderligere vejledning om, hvilke myndigheder, der kunne være tale om, eller hvornår en sådan indhentningsadgang skulle anses for nødvendig. Datatilsynet henstillede derfor til, at der enten i bestemmelsen eller i lovbemærkningerne blevet taget nærmere stilling til disse spørgsmål, herunder til hvordan bestemmelsen tænkes administreret, og hvordan oplysningspligten efter databeskyttelses-forordningens artikel 14 overholdes ved Digitaliseringsstyrelsens indhentning af oplysninger fra andre registre og myndigheder.

Det fremgik også af lovudkastet, at Digitaliseringsstyrelsen skulle kunne behandle personoplysninger og oplysninger om privatpersoner og juridiske enheder i Nemkontosystemet, når det "er nødvendigt af hensyn til anvendere af Nemkontosystemets kontrol- og tilsynsopgaver". Datatilsynet anbefalede, at hensigten om den sammenstilling og evt. videregivelse af personoplysninger, som forslaget indebar, blev nærmere præciseret i lovudkastets bemærkninger.

Endvidere fremgik det af lovudkastet, at der skulle kunne fastsættes nærmere regler om, at Digitaliserings-styrelsen – når det var nødvendigt – måtte behandle personoplysninger til andre formål end de formål, hvortil oplysningerne oprindeligt var indsamlet.

Datatilsynet pegede i sit høringssvar på princippet om formålsbegrænsning, og selvom fravigelsen måtte antages at hvile på samfundsmæssige hensyn til kontrol og misbrugsbekæmpelse, opfordrede Datatilsynet til, at Digitaliseringsstyrelsen i lovforslagets bemærkninger som minimum tog stilling til, hvordan man påtænkte at overholde de kvalificerede krav, som fremgår af databeskyttelsesforordningens artikel 23, stk. 2. Denne bestemmelse skal sikre sammenhæng mellem den ønskede begrænsning og klarheden i den hjemmel, der danner grundlag for begrænsningen.

# Tilsyn

**2295** sager i alt

**1777** Klager

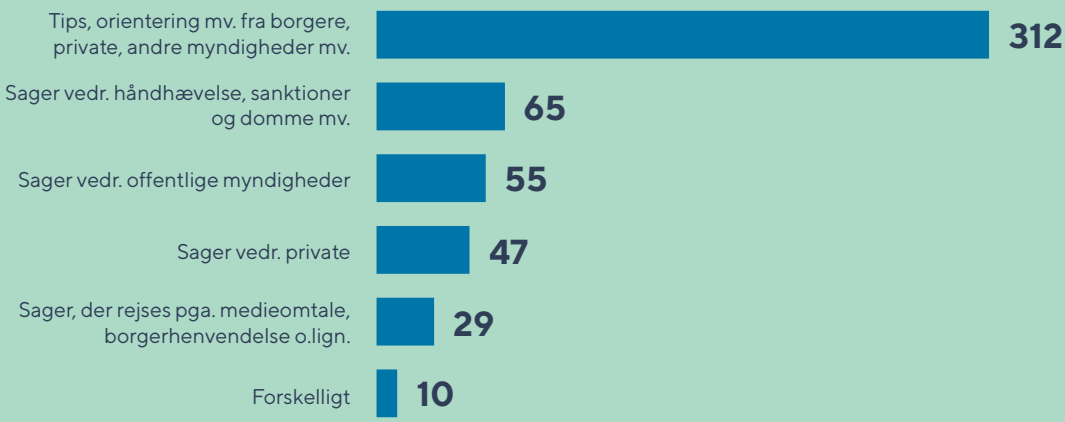
*En vigtig opgave for Datatilsynet er at føre tilsyn med, at myndigheder, virksomheder og andre dataansvarlige og databehandlere overholder reglerne for databeskyttelse.*

*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 2024 indgivet **5** politianmeldelser med indstilling om bøde for overtrædelse af databeskyttelsesreglerne.*

## 518 Sager på Datatilsynets eget initiativ



## Særlige fokusområder for Datatilsynets tilsynsaktiviteter i 2024

Datatilsynets aktiviteter i 2024 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:

### Brug af kunstig intelligens

Udviklingen og udbredelsen af kunstig intelligens ("AI") er vokset eksponentielt gennem de seneste par år. Denne udvikling er bl.a. særligt drevet af udvikling inden for såkaldt generativ AI, som bliver spået til at få en grundlæggende betydning for måden, vi alle arbejder på. Teknologien indebærer dog særlige risici for de borgere, hvis oplysninger bliver behandlet som led i udvikling eller brug af disse løsninger. Et andet område, hvor AI også i stigende omfang bliver udbredt er inden for sundhedssektoren, hvor løsninger bl.a. bruges som beslutningsstøtte i patientbehandlingen. Brug af sådanne løsninger indebærer særligt i sundhedssektoren store risici for borgerne.

Datatilsynet vil derfor i 2024 fastholde sit fokus på kunstig intelligens og føre tilsyn med offentlige og private organisationers brug af kunstig intelligens, herunder særligt generativ AI løsninger og AI-løsninger inden for sundhedssektoren.

### Overvågning af ansatte

Datatilsynet vil i 2024 have fokus på overvågning af ansatte og vil i den forbindelse foretage et tilsyn i form af en kortlægning af omfanget og karakteren af den overvågning, der finder sted med henblik på kontrol af ansatte. Kortlægningen skal omfatte både private og offentlige arbejdsgivere.

### Online og fysisk indkøb

I onlinehandel har det i sagens natur altid været nødvendigt at behandle personoplysninger om kunderne, f.eks. for at levere den bestilte vare eller at sende kunderne relevante tilbud, hvis de har bedt om det. I stigende omfang er det dog også blevet muligt at gemme sine betalingskortoplysninger for at gøre det lettere at handle igen næste gang.

Tilsvarende sker der i dag også behandling af personoplysninger, når kunderne handler i fysiske butikker. Det sker bl.a. ved brug af de såkaldte scan-og-betal apps, hvor en række detailhandel gør det muligt for kunderne at scanne deres varer undervejs og betale via appen og på den måde undgå den almindelige kassebetjening.

Datatilsynet vil i 2024 bl.a. have fokus på, at behandling af personoplysninger som led i disse aktiviteter sker inden for rammerne af databeskyttelsesreglerne.

### Kommunale webarkiver

På baggrund af flere klagesager offentliggjorde Datatilsynet i 2021 retningslinjer for kommuners offentliggørelse af oplysninger i webarkiver. Datatilsynet vil i 2024 føre tilsyn med, hvordan kommunerne har implementeret disse retningslinjer.

## Den registreredes ret til indsigt

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. I 2023 deltog Datatilsynet i den koordinerede indsats om udpegning af databeskyttelsesrådgivere og deres rolle. Også i 2024 deltager Datatilsynet, hvor indsatsen kommer til at omhandle de dataansvarliges behandling af anmodninger om indsigt fra den registrerede.

## Boligforeninger

Mange registrerede bor i boliger, der administreres af professionelle administratorer. I denne forbindelse behandler boligadministrationsselskaberne og boligselskabernes egen administration en lang række oplysninger om de registrerede og vil ofte også håndtere eksempelvis retten til indsigt eller sletning på vegne af den dataansvarlige andels-, ejerforening eller boligselskab. Datatilsynet vil i 2024 derfor fokusere på håndteringen og overholdelse af de registreredes rettigheder hos disse professionelle aktører. Herudover vil Datatilsynet sætte fokus på boligforeningers brug af tv-overvågning.

## Privatskoler

Datatilsynet vil i 2024 føre tilsyn med privatskolers behandling af personoplysninger, hvor temaerne vil være hjemmel samt håndtering af indsigts- og sletningsanmodninger.

## Grundlæggende behandlingssikkerhed hos kommuner og regioner

Datatilsynet har siden 2020 gennemført en række modenhedstilsyn med fokus på grundlæggende behandlingssikkerhed hos mange af landets kommuner og landets regioner. Dette har givet anledning til fysiske tilsynsbesøg, kritik- og påbudsafgørelser og straffesager samt en lang række vejledningsinitiativer, der alle er målrettet relevante områder, som er identificeret gennem tilsynsindsatsen.

Datatilsynet vil i 2024 fortsat følge op på flere enkeltområder, hvor tilsynsindsatsen har afdækket problemer med behandlingssikkerhed, herunder områder som i flere tilfælde har givet anledning til politianmeldelse. Det gælder emner som kryptering af bærbare datamedier, scanningsværktøjer og udarbejdelse af konsekvensanalyser. I 2024 gennemføres derudover den sidste del af modenhedstilsynet med særlig fokus på de kommuner, som endnu ikke har været omfattet af indsatsen.

## 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-samarbejdet (SIS), Visuminformationssystemet (VIS) og Toldinformationssystemet (CIS). Datatilsynet vil i 2024 føre tilsyn med en række myndigheders behandling af personoplysninger i forbindelse med anvendelsen af flere af disse fælleseuropæiske informationssystemer.

## Rettighedsstyring og forebyggelse af misbrug af adgang til personoplysninger

Offentlige og private organisationer har – som dataansvarlige og/eller som databehandlere – et ansvar for at etablere et passende sikkerhedsniveau, når de behandler personoplysninger. Det indebærer, at der bl.a. skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab fx som led i misbrug af adgangsrettigheder.

Datatilsynet har de senere år set mange eksempler på persondatabrud, hvor mangelfuld rettighedsstyring har forøget risikoen for misbrug af personoplysninger, fx fordi en hacker har fået bedre mulighed for at tilgå oplysninger inde i systemet eller hvor medarbejdere uberettiget tilgår personoplysninger af nysgerrighed eller for at opnå en form for personlig vinding uden risiko for opdagelse. Øget anvendelse af automatisering gennem RPA teknologi kan ligeledes øge risikoen for misbrug, hvis ikke der er styr på rettighedsstyringen. Systematisk rettighedsstyring, gode kontrolprocedurer og effektiv håndhævelse fra den dataansvarliges side er tiltag der er centrale i forebyggelsen af denne type misbrug. I 2024 har Datatilsynet derfor besluttet at sætte fokus på dette hos et antal offentlige og private dataansvarlige.

## 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 retshåndhævelsesloven – dog med undtagelse af domstolene. Datatilsynet behandler endvidere klagesager og tager sager op af egen drift på området. Datatilsynet vil i 2024 udføre et antal tilsynsaktiviteter i forhold til de retshåndhævende myndigheders overholdelse af en række af lovens bestemmelser.

## PNR-lov

PNR-loven udgør den retlige ramme for politiets indsamling og behandling af de passagerlisteoplysninger (PNR-oplysninger), som luftfartsselskaberne er i besiddelse af om deres passagerer. Oplysningerne må ifølge loven alene behandles til nogle særligt opregnede formål. Der er i medfør af loven etableret en PNR-enhed hos politiet, som er ansvarlig for bl.a. at indsamle, opbevare, og videregive oplysningerne. Datatilsynet er udpeget til at føre tilsyn med PNR-enheden. Datatilsynet vil i 2024 føre tilsyn med politiets overholdelse af lovens bestemmelser.

I næste afsnit følger en række eksempler på klage- og andre tilsynssager, som Datatilsynet i 2024 traf afgørelser i. For eksempler på sager om anmeldelser af brud på persondatasikkerheden, som tilsynet i 2024 traf afgørelse i, henvises til afsnittet herom.

## Tilsyn med kommuners behandlingssikkerhed

I 2024 igangsatte og afsluttede Datatilsynet tilsyn med 48 kommuners behandlingssikkerhed. Målet var at få indblik i og understøtte arbejdet med grundlæggende behandlingssikkerhed hos kommunerne. Indsatsen lå i forlængelse af lignende tilsyn de seneste tre år.

Tilsynene blev gennemført skriftligt og omfattede 77 spørgsmål fordelt på 15 forskellige emner inden for behandlingssikkerhedsområdet. Kommunerne havde seks uger til at besvare spørgsmålene. På baggrund af svarene kunne Datatilsynet bede om at få udleveret dokumentation, stille yderligere spørgsmål, iværksætte stikprøvekontrol og varsle opfølgende tilsynsbesøg.

På baggrund af tilsynene blev der udarbejdet individuelle rapporter med anbefalinger til de enkelte kommuner, som kan bruges i kommunernes videre arbejde med grundlæggende behandlingssikkerhed. Tilsynene blev gennemført som led i Datatilsynets strategi om en mere data- og risikobaseret tilgang til vejledning og kontrol.

Datatilsynet afsluttede i 2024 også to fysiske tilsynsbesøg hos henholdsvis Kerteminde Kommune og Brøndby Kommune.

Tilsynet hos Kerteminde Kommune fokuserede på logning og logauditering, interne procedurer for håndtering, anmeldelse og registrering af brud på persondatasikkerheden, herunder brug af auto-complete, test af backup, test af beredskaber m.v., procedurer for sletning samt konsekvensanalyser.

Datatilsynet konkluderede, at Kerteminde Kommune ikke havde implementeret faste procedurer for løbende logkontrol (f.eks. stikprøvekontrol) for at sikre, at kommunens brugere kun tilgik oplysninger, de havde et arbejdsbetinget behov for. Kommunen foretog kun kontrol af loggen ved konkret mistanke om misbrug.

Som følge heraf udtalte Datatilsynet kritik af, at Kerteminde Kommune ikke havde truffet passende sikkerhedsforanstaltninger.

I forhold til de øvrige områder bemærkede Datatilsynet, at Kerteminde Kommune bør fortsætte med at udarbejde politikker og procedurer for sletning i løst tilknyttede systemer og i fagsystemer. Derudover påpegede Datatilsynet, at kommunen fortsat skal afdække, hvilke behandlingsaktiviteter der kræver konsekvensanalyser, og at der i den forbindelse udarbejdes en plan for gennemførslen af disse analyser.

Tilsynet hos Brøndby Kommune omhandlede den periodiske kontrol med adgangsrettigheder og brugen af flerfaktorautentifikation/Multi-Factor Authentication (MFA) ved adgang direkte fra internettet til kommunens it-systemer.

Datatilsynet konkluderede, at Brøndby Kommune ikke havde foretaget løbende dokumenteret kontrol af almindelige brugeres adgange til KMD Nexus (dvs. brugere der ikke har udvidede rettigheder/administratorrettigheder), da kommunens seneste kontroller forud for tilsynsbesøget var foretaget i januar 2020 og marts 2021.

Endvidere havde Brøndby Kommune ikke implementeret MFA ved adgang til KMD Nexus, SAPA eller Momentum direkte fra internettet frem til medio november 2023. MFA blev først implementeret efter, at Datatilsynet havde varslet tilsynet over for Brøndby Kommune, og fem år efter at kommunen i en risikovurdering af KMD Nexus havde vurderet, at manglende MFA ved login direkte fra internettet udgjorde en sårbarhed.

På den baggrund udtalte Datatilsynet alvorlig kritik af, at Brøndby Kommune ikke havde truffet passende sikkerhedsforanstaltninger.

## Tilsyn med sikkerheden i AULA

Datatilsynet traf i 2023 afgørelse i fem ud af de seks tilsynssager, som tilsynet havde igangsat i efteråret 2021 vedrørende udvalgte kommuners behandling af personoplysninger i it-systemet AULA.

I juni 2024 traf Datatilsynet afgørelse i den sjette og sidste tilsynssag, som omhandlede Københavns Kommune. Tilsynssagen med Københavns Kommune indeholdt flere elementer end de øvrige fem tilsynssager. Datatilsynet var således på baggrund af en presseomtale i foråret 2023 blevet opmærksom på en intern tilsynsrapport fra Københavns Kommunes databeskyttelsesrådgiver, som bl.a. vedrørte kommunens brug af AULAs modul "Sikker fildeling". Datatilsynet undersøgte derfor som led i tilsynssagen også dette modul og anmodede Københavns Kommune om at besvare nogle spørgsmål herom.

I Datatilsynets afgørelse fik Københavns Kommune kritik for mangler i kommunens konsekvensanalyse. Datatilsynet vurderede, at den ikke opfyldte alle mindstekravene til en konsekvensanalyse. Afgørelsen indeholdt derudover en række anbefalinger til kommunens videre arbejde med den planlagte opdatering af konsekvensanalysen. Datatilsynet anbefalede bl.a., at Københavns Kommune – eventuelt i dialog med de øvrige kommuner, KOMBIT og KL – fik præciseret formålet med behandlingen af personoplysninger i AULA i kommunens konsekvensanalyse. Datatilsynet bemærkede endvidere, at det var relevant at præcisere, hvilke dokumenttyper "Sikker fildeling" i AULA anvendes til, og hvilke typer personoplysninger disse dokumenttyper typisk indeholder.

Som opfølgning på AULA-tilsynene tog Datatilsynet i øvrigt initiativ til på et møde i maj 2024 i det kontaktudvalg for kommunerne og regionerne, som tilsynet etablerede i efteråret 2020, at drøfte myndighedernes praktiske erfaringer med risikovurderinger og konsekvensanalyser. Esbjerg Kommune og KOMBIT deltog i mødet efter anmodning fra Datatilsynet for at dele deres praktiske erfaringer med risikovurderinger og konsekvensanalyser om behandlingen af personoplysninger i AULA.

Esbjerg Kommune fremhævede under mødet bl.a. vigtigheden af at skabe overblik gennem gode fortegnelser, der danner grundlag for det videre arbejde med databeskyttelse. Kommunen understregede også betydningen af, at man som dataansvarlig integrerer teknologi (løsningerne/systemerne), proces (standarder/arbejdsgange for anvendelse) og personale (den daglige brug) for at identificere og reducere risici, når et nyt system tages i brug. Endvidere påpegede Esbjerg Kommune, at det er en forudsætning for arbejdet at have indsigt i medarbejderes arbejdsgange og deres praktiske brug af it-redskaber. Dette kendskab gør det nemmere at foretage risikovurderinger ved fremtidige beslutninger om indkøb og implementering af nye systemer og it-løsninger generelt. KOMBIT præsenterede deres overvejelser om en eventuel fælles konsekvensanalyse, og flere kommuner kom med bemærkninger og forslag på mødet.

## Tilsyn med parkeringsselskabers brug af tv-overvågning

Datatilsynet afsluttede i marts 2024 tilsyn med tre parkeringsselskabers brug af tv-overvågning (kamerateknologi) i forbindelse med udstedelse af parkeringsafgifter.

Baggrunden var, at flere borgere havde klaget til tilsynet over forskellige parkeringsselskabers behandling af deres personoplysninger. Datatilsynet har overordnet forstået klagerne således, at de pågældende forud for modtagelse af en parkeringsafgift ikke var bekendt med, at parkeringsområdet var tv-overvåget, eller var af den opfattelse, at tv-overvågningen var opsat til brug for kriminalitetsbekæmpelse. Derudover fremgik det af klagerne, at de registrerede ikke havde fået tilstrækkelige oplysninger om behandlingen af deres personoplysninger ved modtagelse af en parkeringsafgift.

Datatilsynet besluttede på den baggrund at indlede et generelt tilsyn over for en række parkeringsselskaber med etablering i Danmark med det overordnede formål at undersøge, dels om de pågældende parkeringsselskaber eventuelt anvendte tv-overvågning opsat i kriminalitetsforebyggende øjemed til udstedelse af parkeringsafgifter, dels om selskaberne iagttog oplysningspligten efter databeskyttelses-forordningen i forbindelse med udstedelse af parkeringsafgifter ved brug af tv-overvågning (kamera-teknologi). De udvalgte selskaber var Avantpark, Oparko (tidligere Parkeringskompagniet) og Parkzone.

I forhold til Avantpark og Oparko udtalte Datatilsynet kritik, da disse selskaber ikke oplyste de registrerede (parkanterne) om behandlingen af deres personoplysninger ved opkrævningen af parkeringsafgifter. Tilsynet slog i den forbindelse fast, at denne information skal gives senest ved udstedelsen af parkeringsafgiften, og den dataansvarlige skal tage aktive skridt for at opfylde oplysningspligten. Det er dermed ikke nok at have oplysningerne liggende på en hjemmeside.

Datatilsynet konkluderede i forhold til Parkzone, at dette selskab opfyldte sin oplysningspligt ved at linke til selskabets persondatapolitik i deres betalingspåkrav. Derved var parkanten rettidigt informeret om behandlingen af dennes personoplysninger.

## Tilsyn med sikrede døgninstitutioners brug af tv-overvågning

Datatilsynet afsluttede i marts 2024 en række tilsyn med sikrede døgninstitutioners behandling af personoplysninger i forbindelse med tv-overvågning. Baggrunden for tilsynene var bl.a., at børn og unge nyder en særlig beskyttelse efter databeskyttelsesreglerne.

Tilsynene tog udgangspunkt i fysiske tilsynsbesøg på døgninstitutionerne, hvor Datatilsynets medarbejdere bl.a. fik forevist de arealer, som bliver tv-overvåget. Tilsynene fokuserede bl.a. på omfanget af tv-overvågning på institutionerne, reglerne for videregivelse af optagelser, iagttagelse af de registreredes rettigheder og sikkerhed i forbindelse med opbevaring af optagelser.

På baggrund af tilsynene kunne Datatilsynet konstatere, at institutionernes behandling af personoplysninger i forbindelse med tv-overvågning generelt skete inden for rammerne af databeskyttelsesreglerne.

Det er Datatilsynets opfattelse, at døgninstitutioner skal være opmærksomme på ikke at foretage tv-overvågning i større omfang end nødvendigt i forhold til formålene med tv-overvågningen, og at tv-overvågningen sker med respekt for privatlivets fred. Derfor skal døgninstitutioner være opmærksomme på at få vinklet kameraerne, så de f.eks. ikke filmer ind på de unges værelser, når de åbner døren el.lign.

Døgninstitutioner skal derudover være opmærksomme på, at oplysningspligten skal iagttages, både i forhold til anbragte børn og unge, men også i forhold til ansatte på institutionerne. Informationerne bør gives skriftligt og skal bl.a. være i et klart og enkelt sprog, som tager højde for, om de er rettet mod børn. Døgninstitutioner skal også være opmærksomme på, at ansatte bør oplyses om det, hvis optagelser fra tv-overvågning bruges til at vurdere ansættelsesmæssige forhold, f.eks. i forbindelse med klager over personalet.

Herudover skal døgninstitutioner sørge for at træffe passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau for de personer, som bliver tv-overvåget. Dette indebærer bl.a., at man skal foretage logning af ansattes adgang til lagrede optagelser fra tv-overvågning for derved at være i stand til at kontrollere, om medarbejderne kun tilgår optagelser, som de har et arbejdsbetinget behov for at tilgå. I den forbindelse skal man etablere foranstaltninger – f.eks. personlige logins for de medarbejdere, som kan tilgå lagrede optagelser – så man i loggen kan se, hvilken medarbejder der har tilgået en konkret optagelse.

## Manglende indsigt i og sletning af tv-overvågningsoptagelser

I juni 2024 traf Datatilsynet afgørelse i en sag, hvor en borger klagede over, at Clemens Bar ApS havde afvist at give ham indsigt i tv-overvågningsoptagelser fra natklubben, hvor han fremgik. Tv-overvågningen på natklubben var iværksat for at understøtte politiets efterforskning og behandling af straffesager og for at skabe tryghed hos Clemens Bars gæster generelt.

Clemens Bar havde afvist at imødekomme indsigtsanmodningen med den begrundelse, at indsigt i tv-overvågningsoptagelserne kunne kompromittere sikkerheden på natklubben og formindske den kriminalitetsbekæmpende effekt, som var formålet med tv-overvågningen, idet kameraernes placering og blinde vinkler kunne blive afsløret. Clemens Bar udleverede derfor alene overvågningsmateriale efter anmodning fra politiet i forbindelse med politiets efterforskning af eventuelle straffesager. Clemens Bar henviste endvidere til, at det ikke ville være muligt at sløre de øvrige personer på optagelserne uden samtidig at sløre klager på grund af det store antal personer, der optrådte på optagelserne.

Clemens Bar havde gemt de omhandlede tv-overvågningsoptagelser som følge af klagen til Datatilsynet, men på grund af en menneskelig fejl slettede natklubben optagelserne, inden tilsynet havde (færdig)behandlet sagen.

Datatilsynet fandt, at Clemens Bar ikke kunne afvise at give klager indsigt med henvisning til hensynet til offentlige interesser. Datatilsynet lagde bl.a. vægt på, at det alene var Clemens Bar, som af egen drift havde foretaget denne vurdering, og at denne vurdering ikke var understøttet af en erklæring fra politiet eller lignende.

Der var imidlertid efter Datatilsynets opfattelse samtidig ikke tilstrækkeligt grundlag for at tilsidesætte Clemens Bars vurdering af, at klagers anmodning om indsigt i de pågældende tv-overvågningsoptagelser kunne afvises, da udlevering af optagelserne kunne krænke andres rettigheder og frihedsrettigheder.

Datatilsynet lagde i den forbindelse vægt på, at der er tale om et natklubmiljø, og at der efter det oplyste fremgik ca. 150 personer af optagelserne.

Datatilsynet konstaterede endvidere, at de pågældende optagelser var blevet slettet, hvilket betød at dette spørgsmål ikke længere kunne efterprøves. Datatilsynet fandt derfor, at der var grundlag for at udtale alvorlig kritik af, at Clemens Bar – ved at have slettet de omhandlede tv-overvågningsoptagelser – ikke havde håndteret klagers anmodning i overensstemmelse med det grundlæggende princip om lovlighed, rimelighed og gennemsigtighed.

## Tilsyn med universitets behandling af personoplysninger på forskningsområdet

I september 2024 afsluttede Datatilsynet to tilsyn med fokus på Aarhus Universitets behandling af personoplysninger på forskningsområdet.

Datatilsynet havde i det ene tilsyn udvalgt tre forskningsprojekter som genstand for et skriftligt tilsyn inden for emnerne "behandlingsgrundlag" og "ansvar og roller".

Datatilsynet fandt, at der var uklarhed om hjemmelsgrundlaget i to af projekterne. I et andet projekt var der tvivl om, hvorvidt der var indgået en fyldestgørende databehandleraftale. Endelig fandt tilsynet, at der i to projekter ikke var ført tilstrækkeligt tilsyn med universitetets databehandlere.

Tilsynet udtalte derfor kritik af, at Aarhus Universitets behandling af personoplysninger i de tre projekter ikke var sket i overensstemmelse med de databeskyttelsesretlige regler.

Under det andet tilsyn havde Datatilsynet været på fysisk tilsynsbesøg hos Aarhus Universitet, hvor genstanden for tilsynet var en tilladelse til at videregive biologisk materiale fra et forskningsprojekt. Datatilsynet besluttede efterfølgende at udvide tilsynet til at omfatte alle forskningsprojekter baseret på databeskyttelseslovens § 10, hvor der inden for de seneste to år var sket videregivelse omfattet af tilladelseskravet i § 10, stk. 3.

Datatilsynet fandt grundlag for at udtale kritik af Aarhus Universitet, fordi universitetet ikke havde sikret sig et overførselsgrundlag i forbindelse med videregivelse af personoplysninger fra et forskningsprojekt.

Endelig udtalte tilsynet alvorlig kritik af, at universitetet i flere tilfælde ikke havde indhentet Datatilsynets tilladelse til videregivelse af personoplysninger.

## Samtykke til ansigtsgenkendelse i fitnesscenter

Datatilsynet traf i juli 2024 afgørelse i en sag, hvor en borger klagede over, at Sporting Health Club havde indført ansigtsgenkendelse i forbindelse med sine fitnesscentre.

Borgeren påpegede bl.a., at der ikke var tilstrækkelige og tilsvarende alternativer til ansigtsgenkendelse. Det fremgik imidlertid af sagen, at brugere af fitnesscentrene, som ikke ønskede at samtykke til ansigtsgenkendelse, kunne blive lukket ind af receptionen i den bemandede åbningstid. Udenfor bemandet åbningstid kunne brugerne kontakte døgnsupporten, der enten kunne fjernåbne døren eller generere en kode til døren.

Datatilsynet har i en tidligere sag om en anden virksomhed inden for samme branche (FysioDanmark) (indirekte) vurderet, at brugen af ansigtsgenkendelse som adgangskontrol til virksomhedens fitnesscentre ikke i sig selv strider mod de grundlæggende principper i databeskyttelsesforordningens artikel 5, herunder kravene til proportionalitet.

Sporting Health Club kunne derfor ifølge Datatilsynet – forudsat at betingelserne for lovlig behandling i øvrigt var opfyldt – tilsvarende anvende ansigtsgenkendelse som adgangskontrol til sine fitnesscentre. Sagen rejste i den forbindelse en række generelle spørgsmål om kravene til et samtykke, herunder om de mulige alternativer i den konkrete sag kunne anses for at udgøre et reelt alternativ. Endvidere rejste sagen spørgsmål om samtykke i forhold til klager.

Efter at sagen havde været behandlet i Datarådet, fandt Datatilsynet, at Sporting Health Club kunne indhente et gyldigt samtykke, der kan udgøre en undtagelse til forbuddet mod behandling af særlige kategorier af oplysninger, hvis virksomheden sikrede sig, at samtykket var informeret og korrekt indhentet.

Datatilsynet fandt imidlertid grundlag for at udtale kritik af det samtykke, som Sporting Health Club konkret havde forsøgt at indhente fra klager, da klager var blevet oplyst om, at der ikke var alternativer til ansigtsgenkendelse.

## Tilsyn med gymnasiers brug af eksamensovervågningssoftware

Datatilsynet blev gennem medieomtale bekendt med, at en række gymnasier påtænkte at benytte software til at overvåge elevernes eksamensaflæggelse med henblik på at forebygge og kontrollere snyd.

På den baggrund besluttede Datatilsynet at føre tilsyn med en række gymnasiers behandling af personoplysninger i forbindelse med deres brug af software til eksamensovervågning. Sagens fokus var gymnasiernes iagttagelse af reglerne om behandlingsgrundlag, proportionalitetsprincippet, opbevarings-begrænsning, oplysningspligt samt databeskyttelse gennem design og gennem standardindstillinger.

På baggrund af de modtagne svar udvalgte Datatilsynet enkelte gymnasier til en nærmere undersøgelse, herunder Roskilde Katedralskole.

I forhold til Roskilde Katedralskole fandt Datatilsynet overordnet, at gymnasiet havde iagttaget databeskyttelsesforordningens regler om behandlingsgrundlag, proportionalitetsprincippet, opbevaringsbegrænsning og oplysningspligt. Tilsynet opfordrede imidlertid Roskilde Katedralskole til at overveje om – og i givet fald i hvilket omfang – det var muligt at gøre den oplysningspligtmeddelelse, der gives til eleverne, endnu mere letforståelig og bruge klarere og enklere sprog.

Endvidere fandt Datatilsynet grundlag for at udtale kritik af, at Roskilde Katedralskole ikke havde foretaget en tilstrækkelig risikovurdering og som følge heraf ikke havde gennemført passende tekniske eller organisatoriske foranstaltninger, som var designet med henblik på at sikre, at der ikke blev indhentet yderligere oplysninger end de tilsigtede. Roskilde Katedralskoles behandling af personoplysninger var dermed ikke sket i overensstemmelse med reglerne om databeskyttelse gennem design i databeskyttelsesforordningens artikel 25, stk. 1.

På baggrund heraf henstillede Datatilsynet, at Roskilde Katedralskole som led i sin eventuelle fremtidige brug af eksamensovervågning gennemførte en fornyet risikovurdering efter forordningens artikel 25, som bl.a. adresserede de i afgørelsen nævnte risici, samt i øvrigt i langt højere grad tog højde for, at eksamensaflæggelse – og overvågning – sker ved brug af elevens egen computer. Gymnasiet skulle samtidig i et større omfang gøre eleverne opmærksomme på de identificerede risici, opfordre eleverne til og give konkrete eksempler på, hvilke tiltag eleverne selv kan gøre for at undgå utilsigtet at eksponere (private) oplysninger i eksamenssituationen. Det kunne f.eks. omfatte vejledende information om, at eleverne under eksamen kan gøre brug af en anden browser, som ikke indeholder deres private oplysninger.

Datatilsynet afsluttede efterfølgende tilsyn med tre andre gymnasiers brug af eksamensovervågningssoftware med henvisning til denne afgørelse og henstillede, at de pågældende gymnasier orienterede sig i afgørelsen og på baggrund heraf vurderede, om – og i givet fald i hvilket omfang – de skulle foretage justeringer af deres eventuelle brug af eksamensovervågningssoftware for at sikre, at den sker i overensstemmelse med databeskyttelsesreglerne.

## Tilsyn med de frie grundskolers behandling af personoplysninger

Datatilsynet afsluttet i efteråret 2024 en række tilsyn med udvalgte frie grundskoler, hvor det overordnede formål med tilsynene var at undersøge skolernes behandling af personoplysninger, særligt med fokus på videregivelse af personoplysninger, indsigt og sletning. Tilsynene med skolerne gav således Datatilsynet et indblik i skolernes "modenhedsniveau" i forhold til efterlevelse af reglerne om hjemmel til videregivelse og håndtering af rettighedsanmodninger.

Datatilsynet blev i forbindelse med tilsynene bl.a. opmærksom på, at en større antal af skolernes privatlivspolitikker, indeholdte følgende afsnit:

*"Du har ret til at få indsigt i de oplysninger, som vi behandler om dig og en række andre oplysninger. Skolen kan tage et gebyr for dette arbejde. Dette skal være et rimeligt gebyr under hensyn til de administrative omkostninger ved at give de pågældende oplysninger. Datatilsynet skriver på deres hjemmeside, at den private dataansvarlige kan kræve 10 kr. for hver påbegyndt side, men at betalingen ikke kan overstige 200 kr."*

Datatilsynet understregede, at det pågældende afsnit ikke længere var i overensstemmelse med de gældende databeskyttelsesregler og opfordrede derfor de pågældende skoler til, at det blev fjernet fra privatlivspolitikken.

På baggrund af besvarelserne fra skolerne kunne Datatilsynet derudover konstatere, at der var behov for nærmere vejledning angående hjemmel til videregivelse og håndtering af rettighedsanmodninger.

## Brug af cookie walls på avishjemmeside

Datatilsynet traf i 2023 to principielle afgørelser vedrørende brug af cookie walls på hjemmesider, og tilsynet udgav i samme forbindelse et sæt generelle retningslinjer for brugen af sådanne samtykkeløsninger.

I marts 2024 traf Datatilsynet endnu en principiel afgørelse på området. Sagen omhandlede Berlingskes specifikke fremgangsmåde, hvor brugerne på berlingske.dk blev mødt af en cookie wall, når de forsøgte at tilgå indlejret indhold, f.eks. videoafspillere eller blogindlæg. Det betød, at indholdet var utilgængeligt, medmindre brugeren accepterede behandling af sine personoplysninger til statistiske og markedsføringsmæssige formål ved brug af cookies.

Datatilsynet fandt – efter at sagen var blevet behandlet i Datarådet – overordnet, at en fremgangsmåde, hvor brugeren alene kan få adgang til delindhold, der er indlejret på berlingske.dk, herunder videoafspillere og blogindlæg, ved at give samtykke til behandling af personoplysninger til statistiske og markedsføringsmæssige formål, ikke opfylder databeskyttelsesforordningens krav til et gyldigt samtykke. Virksomheden blev derfor meddelt et påbud om at sikre, at samtykket fra brugerne på berlingske.dk opfyldte databeskyttelsesforordningens krav til et gyldigt samtykke.

## Brug af kunstig intelligens til analyse af optagne telefonsamtaler

Datatilsynet afsluttede i juni 2024 en undersøgelse af egen drift af IDA Forsikrings brug af kunstig intelligens til at analysere selskabets telefonsamtaler med personer, som ringede til IDA Forsikrings kundeservice.

Ifølge IDA Forsikring blev de indgående telefonopkald optaget, hvorefter lydfilerne fra optagelserne blev sendt til analyse ved en databehandler, der ved hjælp af egenudviklet talegenkendelse omdannede filerne til tekst. Analysen af samtalerne havde til formål at forbedre IDA Forsikrings medlemsservice, sikre kvaliteten og give medarbejderne indsigt i deres samtaler for at styrke servicen overfor medlemmerne.

Datatilsynet fandt – efter at sagen havde været behandlet i Datarådet – at IDA Forsikring, inden for rammerne af databeskyttelsesreglerne, kunne optage og analysere indkomne telefonsamtaler.

Efter tilsynets opfattelse levede IDA Forsikrings proces for indhentelse af samtykke fra den person, der ringer ind, imidlertid ikke op til databeskyttelsesreglerne.

IDA Forsikring havde – efter at have gennemgået sine behandlingsaktiviteter – vurderet, at optagelse og opbevaring af telefonsamtaler til brug for henholdsvis dokumentations- og kvalitetssikringsformål (uddannelse) burde ske på grundlag af et samtykke i henhold til databeskyttelsesforordningens artikel 6, stk. 1, litra a, og 9, stk. 2, litra a, fra den person, der ringer ind.

Betingelserne for et gyldigt samtykke fremgår af databeskyttelsesforordningens artikel 4, nr. 11, og artikel 7, og et gyldigt samtykke forudsætter derfor bl.a., at det er frivilligt, specifikt, informeret og udtryk for en utvetydig viljestilkendegivelse.

Ifølge Datatilsynet indebærer kravet om frivillighed, at den dataansvarlige skal give den registrerede et frit valg og kontrol over personoplysninger om den pågældende selv. Et samtykke vil ikke være afgivet frivilligt, hvis den registrerede ikke har et reelt frit valg. Dette betyder bl.a., at et samtykke ikke kan anses for frivilligt, hvis proceduren til opnåelse af samtykke ikke giver den registrerede mulighed for at give særskilt samtykke til forskellige behandlingsformål vedrørende personoplysninger, og den registrerede dermed tvinges til at samtykke til samtlige formål. Et samtykke skal derfor granuleres (opdeles).

Datatilsynet kunne i den konkrete sag konstatere, at der i forbindelse med, at en person ringede til IDA forsikring, alene blev indhentet ét samlet samtykke til både dokumentations- og kvalitetssikringsformål (uddannelse). Vedkommende, som ringede, fik således ikke mulighed for at vælge kun at samtykke til et af formålene.

Den omstændighed, at indsamling af personoplysninger skete telefonisk, ændrede ifølge tilsynet ikke ved kravene til et gyldigt samtykke. Det var på den baggrund Datatilsynets vurdering, at det samtykke, som IDA Forsikring indhentede, ikke var tilstrækkelig granuleret og derfor ikke kunne anses for frivilligt. Samtykket var som følge heraf ikke gyldigt, og det kunne ikke udgøre et behandlingsgrundlag.

Da Datatilsynet ikke tidligere havde forholdt sig til, hvordan samtykke indhentes telefonisk, når man som dataansvarlig har flere formål, fandt tilsynet konkret ikke anledning til at udtale kritik. IDA Forsikring blev i stedet bedt om (fremover) at sikre sig, at IDA Forsikrings proces i forbindelse med optagelse af telefonsamtaler sker i overensstemmelse med databeskyttelsesreglerne. IDA Forsikring kan i den forbindelse – under inddragelse af Datatilsynets vejledning om telefonsamtaler – overveje, om der kan ske optagelse og opbevaring af telefonsamtaler til et eller begge af de nævnte formål på andet grundlag end samtykke. Hvis dette ikke er tilfældet, må IDA Forsikring indrette sin indhentelse af samtykke på anden vis, f.eks. ved at anmode om ”to tryk”.


DATATILSYNET

## Behandling af ulovligt tilvejebragte oplysninger

Datatilsynet traf i september 2024 afgørelse i en sag, hvor en borger klagede over, at Helsingør Kommune i forbindelse med behandlingen af en modtaget underretning havde besluttet at inddrage oplysninger, som var ulovligt tilvejebragt af tredjemand.

Det fremgik af sagen, at faren til klagers barn havde foretaget aflytninger i form af skjulte mikrofoner. Det fremgik ligeledes af sagen, at de pågældende aflytninger havde resulteret i en dom for ulovlig aflytning.

Helsingør Kommune havde tidligere, på baggrund af en indsigelse fra klageren, besluttet at udelukke de omhandlede aflytninger og transskriberinger fra kommunens sagsbehandling, da kommunen formodede, at de var tilvejebragt gennem en strafbar handling. Helsingør Kommune ændrede senere denne beslutning og valgte at anvende oplysningerne.

Det følger af Datatilsynets praksis, at offentlige myndigheders behandling af oplysninger, som er tilvejebragt i strid med andre regler, under visse omstændigheder kan anses som urimelig, selvom oplysningerne har relevans for en konkret sag.

I den konkrete sag fandt Datatilsynet imidlertid – efter at sagen havde været behandlet i Datarådet – at Helsingør Kommunes behandling af personoplysninger var i overensstemmelse med reglerne i databeskyttelsesforordningen.

## Ret til indsigt i navn på utilsigtet modtager

I september 2024 traf Datatilsynet afgørelse i to sager, hvor to borgere klagede over, at Udviklings- og Forenklingsstyrelsen havde afvist at give klagerne indsigt i bl.a., hvilken revisor der ved en fejl havde modtaget personoplysninger om dem.

Baggrunden for sagerne var, at oplysninger om klagerne i forbindelse med besvarelsen af en aktindsigtsanmodning ved en fejl var blevet videregivet af Skattestyrelsen til en revisor, som havde delt oplysningerne med en klient. Klagerne ønskede herefter at få oplyst, hvem deres oplysninger var blevet videregivet til. Udviklings- og Forenklingsstyrelsen afviste imidlertid at give indsigt i identitetsoplysningerne på de utilsigtede modtagere under henvisning til, at oplysningerne var fortrolige og omfattet af en særlig tavshedspligt i skatteforvaltningsloven.

Klagerne gav Datatilsynet anledning til at tage stilling til, om utilsigtede modtagere af personoplysninger er omfattet af modtagerbegrebet og dermed omfattet af retten til indsigt.

Efter behandling af sagen i Datarådet fandt Datatilsynet, at utilsigtede modtagere er omfattet af den brede definition af en "modtager" og dermed omfattet af retten til indsigt i modtagere af personoplysninger.

Endvidere fandt Datatilsynet, at der i de konkrete sager var et tilstrækkeligt sikkert grundlag for at tilsidesætte Udviklings- og Forenklingsstyrelsens vurdering af, at oplysningen om revisorens navn var en fortrolig oplysning omfattet af tavshedspligten i skatteforvaltningslovens § 17.

## Videregivelse af personoplysninger fra en dansk virksomhed til Meta

Datatilsynet traf i april 2024 afgørelse i en sag, hvor en borger klagede over Telmore A/S' videregivelse af vedkommendes e-mailadresse til Meta Irland.

Videregivelsen skete ifølge Telmore med henblik på at undtage klager fra virksomhedens målrettede markedsføring på Facebook. Dette skete ved brug af Facebooks Custom Audience-værktøj, hvilket tillader virksomheder at skræddersy deres annoncer til specifikke brugergrupper. I sagen havde Telmore vurderet, at Meta Irland handlede som databehandler for virksomheden.

I Datatilsynets afgørelse konkluderede tilsynet – efter at sagen havde været behandlet i Datarådet – at Telmores behandling af klagers personoplysninger ikke kunne ske med hjemmel i interesseafvejningsreglen. Datatilsynet udtalte på den baggrund kritik over for Telmore. Derudover blev Telmores vurdering af rollefordelingen mellem virksomheden og Meta Irland tilsidesat af tilsynet, der fastslog, at der i sagen forelå fælles dataansvar. Datatilsynet valgte dog ikke at udtale kritik heraf, idet den manglende fastlæggelse af ansvar skyldtes, at tilsynet undtagelsesvist tilsidesatte Telmores vurdering af rollefordelingen.

Datatilsynet konkluderede ydermere, at det ikke var hensigtsmæssigt at fortsætte undersøgelsen af sagens øvrige klagepunkter. Dette skyldtes, at det er en afgørende forudsætning for at kunne iagttage databeskyttelsesreglerne, at man korrekt identificerer sin egen rolle ved behandling af personoplysninger, herunder rollefordelingen med eventuelle samarbejdspartnere. Idet Datatilsynet tilsidesatte Telmores vurdering af denne grundlæggende forudsætning, ville en fortsat undersøgelse ikke give klager korrekte informationer om, hvordan oplysningerne blev behandlet. Datatilsynet lagde endvidere vægt på, at Telmore ikke længere delte klagers e-mailadresse med Meta Irland.

Datatilsynet indskærpede endelig over for Telmore, at hvis virksomheden fortsat forventer at benytte Meta Irlands Custom Audience-værktøj, skal virksomheden sikre sig, at der foreligger en såkaldt ordning om fælles dataansvar, der fastlægger parternes respektive ansvar for overholdelsen af forpligtelserne i databeskyttelsesforordningen.

## Behandling af personoplysninger ved rekruttering

I oktober 2023 indledte Datatilsynet en undersøgelse af Parken Services A/S' behandling af personoplysninger i forbindelse med rekruttering. Datatilsynet var efter en konkret henvendelse blevet bekendt med, at Parken Services A/S indhentede kopi af pas og straffeattester på ansøgere som led i rekruttering til stillinger i virksomheden.

Datatilsynet fandt efter en konkret vurdering, at indhentelsen af pasoplysninger og straffeattester skete inden for rammerne af databeskyttelsesreglerne. Tilsynet lagde i den forbindelse vægt på de særlige forhold, der gør sig gældende for Parken Services A/S som arbejdsgiver, herunder det meget store antal personer, virksomheden beskæftiger, og den helt særlige risikoprofil der knytter sig til Parken Stadion som arena for store sports- og underholdningsarrangementer, hvad angår risikoen for terror og anden kriminalitet.
Datatilsynet lagde endvidere vægt på, at Parken Services A/S konkret havde vurderet nødvendigheden af at indhente de pågældende oplysninger for de enkelte stillingskategorier i virksomheden, og at indhentelsen af oplysningerne skete på det senest mulige tidspunkt i forhold til Parken Services A/S' rekrutteringsprocedure.

## Ansvar for eksterne komponenter i forbindelse med design og valg af it-løsninger

I juli 2022 indledte Datatilsynet en sag af egen drift mod Dansk Retursystem A/S, der havde udviklet en applikation (app), som kunne bruges i forbindelse med pantning, fordi appen angiveligt behandlede oplysninger om bl.a. brugernes konti, saldi og lån i banken.

Undersøgelsen viste, at pant-appen havde en indbygget komponent, der indhentede brugerens kontooplysninger for at kunne udbetale penge til den rigtige konto. Men komponenten, som blev stillet til rådighed af en tredjepart, kunne også indsamle oplysninger om bl.a. brugerens saldi, identitetsoplysninger og transaktionshistorik. Disse oplysninger blev dog ikke givet videre til Dansk Retursystem.

Datatilsynet besluttede under sagens behandling at afgrænse tilsynets undersøgelse af sagen til at vedrøre overholdelsen af principperne i databeskyttelsesforordningen om bl.a. lovlighed, rimelighed og gennemsigtighed, princippet om dataminimering samt bestemmelsen om databeskyttelse gennem design.

I september 2024 traf Datatilsynet afgørelse i sagen og udtalte alvorlig kritik af, at Dansk Retursystems behandling af personoplysninger i pant-appen ikke skete i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra a og c, samt artikel 25, stk. 1.

Det fremgår bl.a. af afgørelsen, at ifølge Datatilsynet skal man som dataansvarlig designe og vælge en løsning, der kun behandler de personoplysninger som er strengt nødvendige for at opfylde formålet. Endvidere skal den dataansvarlige ved benyttelse af tredjepartssoftware foretage en risikovurdering og sørge for, at funktioner, som ikke er forenelige med bl.a. de grundlæggende principper i databeskyttelsesforordningen, ikke inkluderes eller deaktiveres. Hvis tredjepartsløsningen ikke tilbyder en sådan mulighed for at tilpasse og begrænse behandlingen af personoplysninger til, hvad der er nødvendigt for opfyldelse af formålet, vil løsningen ikke lovligt kunne anvendes. En lovlig anvendelse vil i det tilfælde kræve et re-design af løsningen.

Dansk Retursystem fik som følge heraf samtidig et påbud om at bringe pant-appen i overensstemmelse med databeskyttelsesforordningen ved at gennemgå de behandlinger af personoplysninger, der blev foretaget i appen, og sikre, at der ikke blev behandlet flere oplysninger end formålet tilsagde, og at de behandlinger, der blev foretaget, sker lovligt, rimeligt og gennemsigtigt.

Endvidere udstedte Datatilsynet en advarsel om, at det til formålet "at kunne udbetale pant via direkte pengeoverførsel til den bankkonto, som brugeren af appen har angivet og kommunikere med brugeren", sandsynligvis ville være i strid med databeskyttelsesforordningen at benytte en tredjepartsløsning til kontooplysninger, der behandler personoplysninger ud over de nødvendige kontooplysninger for at kunne udbetale pantbeløbet ved en pengeoverførsel direkte til kontoen. Dette uanset om der gives brugeren andre muligheder i appen end at bruge den pågældende integration.

## Behandling af oplysninger om boligejere på hjemmeside

I marts 2024 indledte Datatilsynet en sag af egen drift mod Boliglag ApS vedrørende behandlingen af personoplysninger på hjemmesiden www.boliglag.dk. Undersøgelsen blev igangsat på baggrund af en række klager og henvendelser, som Datatilsynet havde modtaget.

Datatilsynet konstaterede i den forbindelse, at det på hjemmesiden var muligt at fremsøge oplysninger om ejendomme ved at søge enten på en bestemt adresse eller ved at søge direkte på en fysisk persons navn. Søgeresultaterne viste boligens profil, hvor der fremgik oplysninger om bl.a. navn, køn og alder på nuværende og tidligere ejere af boligen samt boligens salgshistorik og salgsværdi.

Datatilsynet traf i oktober 2024 afgørelse i sagen og udtalte indledningsvist, at det ofte vil være lovligt for en dataansvarlig at behandle – herunder offentliggøre – personoplysninger, der er indhentet fra et eller flere offentligt tilgængelige registre, og som således allerede er offentliggjort.

Når det gjaldt den behandling af personoplysninger, der skete på hjemmesiden www.boliglag.dk, var det imidlertid tilsynets vurdering, at den ikke kunne ske inden for rammerne af "interesseafvejningsreglen" i databeskyttelsesforordningens artikel 6, stk. 1, litra f. På den baggrund udtalte Datatilsynet kritik af Boliglag ApS.

Datatilsynet lagde i den forbindelse bl.a. vægt på, at de registrerede ikke med rimelighed kunne forvente en så omfattende samkøring og offentliggørelse af deres personoplysninger, som løsningen på www.boliglag.dk medførte. Offentliggørelsen havde en særlig indgribende karakter som følge af, at oplysningerne kunne fremsøges ved en søgning på den enkelte persons navn.

## Brug af Chromebooks i folkeskolen

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

Sagen rummer indtil flere databeskyttelsesretlige problemstillinger, hvor de mest centrale vedrører kommunernes retlige grundlag for, at leverandøren (Google) behandler elevernes oplysninger til egne formål, da dette ikke er hjemlet i folkeskoleloven – og at kommunerne ikke havde formået at tilpasse kontrakter og softwarens virkemåde, så elevernes oplysninger ikke blev videregivet. I den forbindelse havde Helsingør Kommune ikke foretaget risikovurdering og konsekvensanalyse, hvilket allerede i 2021 fik tilsynet til at udstede påbud, meddele en advarsel og en midlertidig begrænsning samt udtale alvorlig kritik af kommunen.

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

Herefter blev der indledt et samarbejde mellem KL, Helsingør Kommune og de 52 andre kommuner, der benyttede denne software, om at indgå dialog med leverandøren om at få lovliggjort brugen af Google Workspace. Datatilsynet suspenderede på den baggrund i september 2022 behandlingsforbuddet og meddelte Helsingør Kommune og de øvrige involverede kommuner et påbud om lovliggørelse.

Efterfølgende fremsendte KL på vegne af de 53 kommuner løbende og helt frem til udgangen af juni måned 2023 materiale til Datatilsynet. Materialet gav en uddybende beskrivelse af de centrale forhold i skolernes brug af tjenesten og leverandørens anvendelse af data.

Dette var en oprindelig forudsætning for, at kommunerne kunne begynde at behandle oplysningerne i Google Workspace, og de pågældende analyser skulle derfor have været på plads, inden værktøjerne blev taget i brug. Denne manglende afklaring og de ufuldstændige analyser er bedømt og sanktioneret i Datatilsynets tidligere afgørelser mod de 53 kommuner.

Kommunerne konstaterede i det fremsendte materiale, at der skete en videregivelse af personoplysninger, som Google bruger til egne formål. Datatilsynet vurderede derfor lovligheden af disse videregivelser og traf i januar 2024 afgørelse i denne del af sagen, da afklaringen af dette var en forudsætning for at kunne behandle oplysningerne i det hele taget. Samtidig satte denne afklaring rammerne for en løsning, hvor der fremover vil kunne behandles personoplysninger om skolebørnene.

Konklusionen i Datatilsynets afgørelse var, at der var hjemmel til at videregive elevernes oplysninger med henblik på levering af tjenesterne, forbedring af sikkerheden og pålideligheden af tjenesterne, kommunikation med bl.a. kommunerne og overholdelse af retlige forpligtelser.

Det var dog samtidig vurderingen, at folkeskoleloven ikke tilstrækkeligt klart hjemler, at kommunerne videregiver elevernes oplysninger til vedligeholdelse og forbedring af Google Workspace for Education-tjenesten, ChromeOS og Chrome-browseren, eller til måling af ydeevnen og udvikling af nye funktioner og tjenester i ChromeOS og Chrome-browseren. Derfor gav Datatilsynet et påbud til kommunerne om at bringe behandlingen i overensstemmelse med reglerne ved at sikre, at der er hjemmel til alle de behandlinger, der sker.

Af Datatilsynets afgørelse fremgik, at det eksempelvis kunne ske ved:

a. At kommunerne ikke længere videregiver personoplysninger til Google til disse formål. Det vil sandsynligvis kræve, at Google udvikler en teknisk mulighed for, at de pågældende datastrømme afskæres.
b. At Google selv afstår fra at behandle oplysningerne til disse formål.
c. At Folketinget tilvejebringer et tilstrækkeligt klart retsgrundlag for videregivelse til disse formål.

Kommunerne skulle efterleve påbuddet fra 1. august 2024, men de blev bedt om senest 1. marts 2024 at tilkendegive, hvordan de havde til hensigt at efterleve det.

Den 24. juni 2024 oplyste KL på vegne af 53 kommuner, at kommunerne fra 1. august 2024 ikke længere vil videregive personoplysninger til de af Googles egne formål, som Datatilsynet i sin delafgørelse fra januar 2024 fandt uhjemlede.

Datatilsynet konstaterede ved brev af 10. juli 2024 til KL, at det udkast til kontrakt, som KL havde fremsendt afspejlede dette. Samtidig noterede tilsynet sig, at kommunerne på denne måde ville opfylde påbuddet fra 30. januar 2024. Datatilsynet indskærpede dog, at kommunerne dels får indgået aftalerne inden påbudsfristen, dels får indført alle kontrolforanstaltninger, der vurderes nødvendige for at påvise overholdelsen af databeskyttelsesforordningen.

Endvidere noterede Datatilsynet sig, at der var sket tilpasninger af kontrakten, der sikrer, at personoplysninger udelukkende vil blive behandlet efter den dataansvarlige kommunes instruks, bortset fra tilfælde, hvor det måtte være krævet af gældende ret i henhold til EU-regler eller en EU-medlemsstats ret.

Afslutningsvist oplyste Datatilsynet, at tilsynet havde anmodet Det Europæiske Databeskyttelsesråd om en udtalelse om bl.a. rækkevidden af den dataansvarliges dokumentationsforpligtelse for databehandlerens brug af underdatabehandlere. Når denne udtalelse forelå, ville Datatilsynet foretage en endelig vurdering af underdatabehandlerkæden ved kommunernes brug af Googles produkter.

Sagerne forventes afklaret i løbet af 2025.

## Chromebook-sagens relevans for andre organisationer og cloudservices

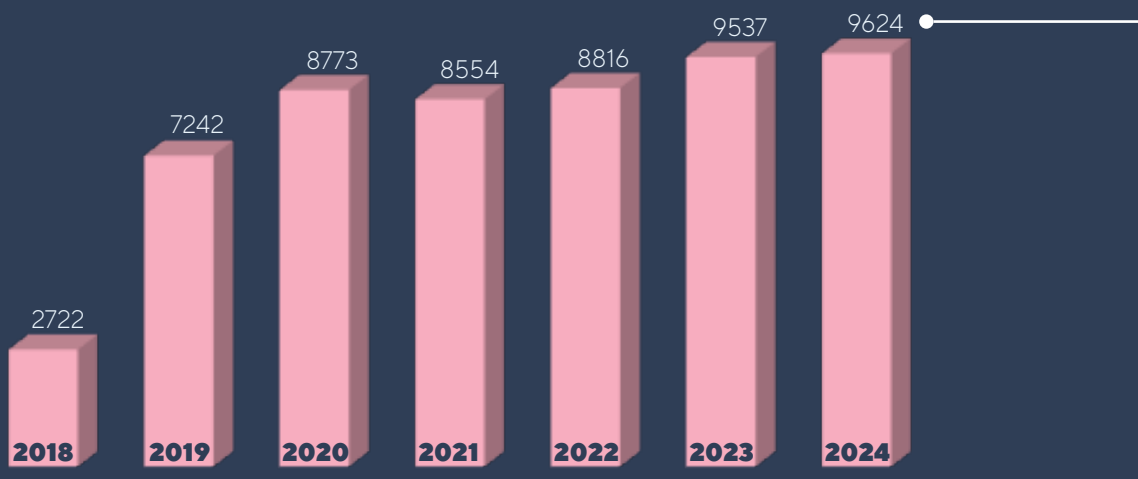
Kort efter offentliggørelsen af Datatilsynets afgørelse fra januar 2024 i den såkaldte Chromebook-sag henvendte Region Syddanmark sig til Datatilsynet med to spørgsmål vedrørende regionens egen påtænkte migrering til Microsoft 365.

Det var Datatilsynets umiddelbare opfattelse – på baggrund af det materiale, som regionen havde fremsendt til tilsynet – at der med hensyn til regionens påtænkte brug af Microsoft 365 var en tilsvarende problemstilling om videregivelse af personoplysninger til cloudserviceleverandøren – i dette tilfælde Microsoft – til brug for dennes egne formål, som regionen skulle adressere. Datatilsynet anviste i den forbindelse en række konkrete forhold, som Region Syddanmark skulle kortlægge, afklare og vurdere.

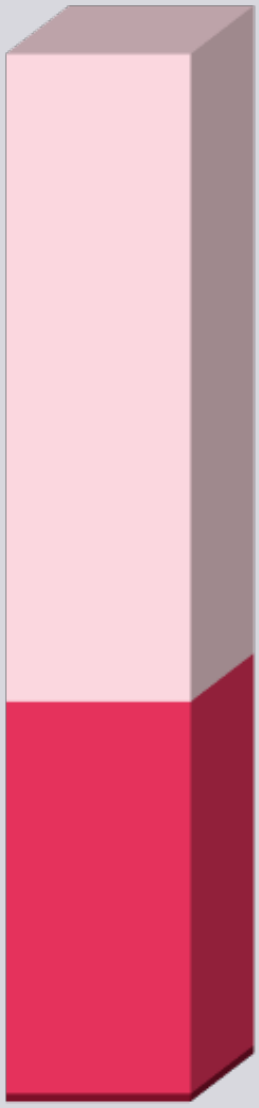
Svaret til Region Syddanmark skete som led i en verserende sag, men belyste efter tilsynets opfattelse en række helt principielle spørgsmål, som er blevet rejst generelt som følge af Chromebook-sagen. Derfor valgte Datatilsynet undtagelsesvis i februar 2024 at offentliggøre tilsynets svar til regionen.

# Anmeldelser af brud på persondatasikkerheden

*Datatilsynet modtager hvert år en stor mængde anmeldelser af brud på persondatasikkerheden. I 2024 blev der anmeldt **9.624** brud på persondatasikkerheden, hvilket er 87 fere anmeldelser end i 2023 og samtidig det hidtidig højeste antal, siden anmeldelsespligten blev indført i maj 2018.*



**9624** brud i alt*



**5950**
Anmeldelser fra offentlige myndigheder

**3601**
Anmeldelser fra private

**73**
Forskelligt

## Manglende sikkerhedsforanstaltninger

Datatilsynet udtalte i maj 2024 ligeledes alvorlig kritik af Københavns Kommune for ikke at have truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der var ved myndighedens behandling af personoplysninger.

I Københavns Kommune var der – som følge af en menneskelig fejl i forbindelse med flytning af filer med en større mængde data (diskswap) – blevet givet for brede brugeradgange til det drev, hvor data blev opbevaret. Det resulterede i, at ca. 37.500 medarbejdere i kommunen uberettiget fik adgang til oplysninger om op mod 3,7 millioner personer. Dataene relaterede sig til en såkaldt SAS-installation (format til ledelsesinformation mv.), og det var alene fire SAS datavarehus-udviklere, der skulle have haft adgang til dataene. For størstedelen af de berørte var der bl.a. tale om navne- og adresseoplysninger, men derudover indeholdt filerne også oplysninger om trivsel, sprogvurdering og oplysninger om tandlæge og sundhedspleje vedrørende børn. Den brede adgang eksisterede i knap to måneder, indtil Københavns Kommune konstaterede fejlen ved en sikkerhedsmæssig rutinescanning af kommunens åbne drev. Adgangen blev herefter lukket, og hændelsen blev anmeldt til Datatilsynet som et brud på persondatasikkerheden.

Kommunen oplyste, at der var en meget lille sandsynlighed for, at en almindelig it-bruger havde kunnet støde på drevet, da det krævede særlige forudsætninger at finde det. Netværksregistrering var således slået fra på de enkelte pc'er, og det betød, at medarbejderne ikke ved almindelige søgninger på pc'en kunne finde drevet. Det betød også at URL'en skulle kendes, eller at der skulle scannes aktivt efter drevet. Kommunens undersøgelser viste, at der ikke havde været anvendt et scanningsværktøj, der havde ledt efter åbne drev i perioden for bruddet. Undersøgelse af den administrative log viste endvidere kun adgange for personer med et arbejdsbetinget behov. Kommunens logs over alle administrative it-brugeres potentielle adgang til drevet gik dog ikke så langt tilbage i tiden, at kommunen endegyldigt kunne konkludere, at ingen andre medarbejdere end dem, der havde et arbejdsbetinget behov, havde tilgået oplysningerne i perioden. Kommunen anførte også, at hovedparten af SAS-filer ikke umiddelbart var læselige for dem, der uberettiget havde fået adgang hertil, og at det krævede, at data først blev bearbejdet i et SAS-program.

Datatilsynet lagde i sin afgørelse vægt på, at kommunen ikke havde sikret, at kun medarbejdere med et arbejdsbetinget behov havde adgang til drevet, at der var et set-up, hvor en enkelt medarbejders fejl kunne resultere i et brud, der omfattede 3,7 mio. personer, og at det ikke umiddelbart efter flytningen af oplysningerne var blevet testet, om rettighederne til drevet var korrekte, hvilket straks ville have afsløret fejlen, da alle administrative medarbejdere havde fået adgang hertil.

Datatilsynet har generelt den opfattelse, at der ved nyudvikling af applikationer eller flytning af fildrev, indledningsvist skal vurderes, om det fremover er nødvendigt at flytte og opbevare oplysningerne i personhenførbar form. Hvis det er nødvendigt for formålet ved behandlingen, kan en mulig sikkerhedsforanstaltning være, at den dataansvarlige sikrer, at oplysningerne er krypteret sådan, at kun en adgangsberettiget person kan læse og låse op for oplysningerne. Et proprietært dataformat (som f.eks. et SAS-format) kan ikke sidestilles med kryptering, da der ofte findes viewere eller plugins, der gør det relativt let at kunne læse de pågældende fil-formater.

Ved alle udviklings- og vedligeholdelsesopgaver er det endvidere væsentligt, at der som et led i changeprocessen stilles krav om, at dem, der er bemyndiget hertil af den dataansvarlige, kontrollerer, at den tilsigtede adgangsstyring, kontrol og logning virker, inden ændringen frigives til drift.

## Manglende vedvarende robusthed af NemID-løsningen

Datatilsynet traf i maj 2024 afgørelse i en sag, som tilsynet havde indledt af egen drift over for Nets DanID A/S efter et nedbrud af NemID i juni 2022, hvor op mod 1,5 mio. af NemID-brugerne oplevede problemer med at anvende NemID.

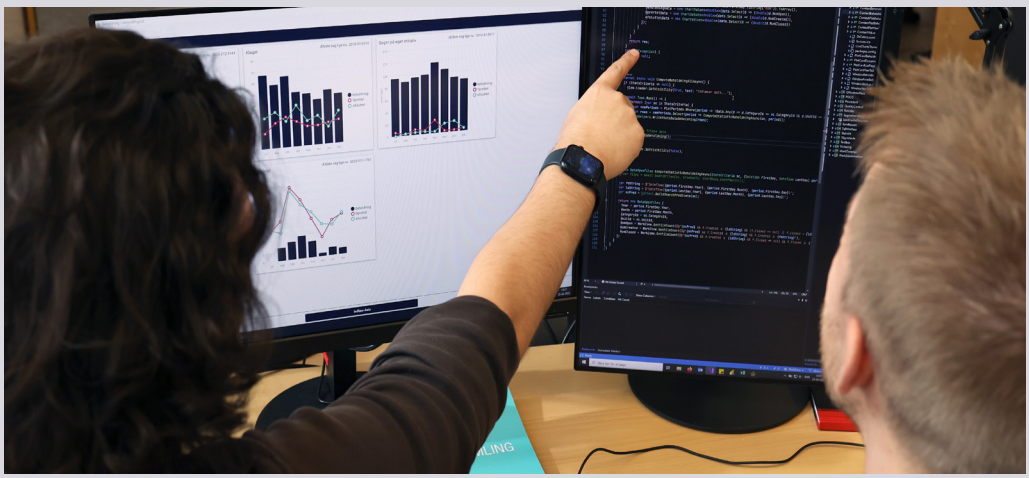
I fire dage kunne de pågældende brugere ikke tilgå større offentlige danske tjenester som borger.dk, e-Boks, sundhed.dk og minretssag.dk ved login med NemID. Nets DanID, som var dataansvarlig på tidspunktet for hændelsen, fulgte selskabets nødprocedure i forsøget på at genoprette normal drift ved at gendanne en server med en backup-løsning. Det var dog ikke muligt for Nets DanID at genoprette normaldriften før fire dage efter nedbruddet, da backup-løsningen var utilgængelig. Den test af nødproceduren, der kunne have konstateret årsagen til, at backup-løsningen var utilgængelig, blev senest foretaget ca. to år inden nedbruddet.

Datatilsynet konkluderede, at Nets DanID's procedurer vedrørende afprøvning, vurdering og evaluering af effektiviteten af backup-løsningen ikke var tilstrækkelige. Derudover vurderede Datatilsynet, at Nets DanID ikke havde truffet tilstrækkelige foranstaltninger for at sikre vedvarende robusthed af NemID-løsningen.

På den baggrund udtalte Datatilsynet alvorlig kritik af Nets DanID for ikke at have tilstrækkelige foranstaltninger for at opnå et sikkerhedsniveau, der passede til de risici, der var for borgerne.

Datatilsynet lagde i sin afgørelse særligt vægt på, at der var tale om kritisk, national infrastruktur, og at nedbruddet derfor potentielt kunne medføre betydelige konsekvenser for de berørte borgere - ikke mindst taget den lange periode i betragtning, som nedbruddet varede.

Det er generelt Datatilsynets opfattelse, at databeskyttelsesforordningens krav om passende sikkerhed normalt vil indebære, at der bør foretages test af backup. Det betyder, at det testes jævnligt, om backup udføres med de forventede intervaller (hyppighed), og om backup-kopien er tilgængelig, indeholder alle relevante data (omfang) og er retvisende (integritet). Derudover bør der foretages test af genetablering, hvor det testes om data reelt kan genindlæses og anvendes i et it-system. Dette er en test af, 1) om genetablering kan udføres med eksisterende vejledninger/procedurer, 2) at alt det, som der er kopier af (hardware, software, data) kan fungere sammen, og 3) at genetablering kan ske hurtigt nok i forhold til, at konsekvensen normalt stiger med tiden (Recovery Time Objective).



## Uberettiget videregivelse af oplysninger om navne- og adressebeskyttelse

Siden den 25. maj 2018, hvor pligten til at anmelde brud på persondatasikkerheden til Datatilsynet blev indført, har tilsynet løbende modtaget mange anmeldelser fra Familieretshuset, hvor bruddet består i, at myndigheden uberettiget har videregivet oplysninger om beskyttede navne og adresser eller andre oplysninger, som potentielt kan afsløre en persons opholdssted, herunder ophold på krisecenter. Oplysningerne er i de fleste tilfælde videregivet til den anden part i sagen, som typisk kunne være årsagen til valget om navne- og adressebeskyttelse eller ophold på krisecenter. De utilsigtede videregivelser skyldes menneskelige fejl som følge af uopmærksomhed hos Familieretshusets medarbejdere.

Datatilsynet har tidligere behandlet to lignende sager om Familieretshusets utilsigtede videregivelse af de samme typer af oplysninger. Datatilsynet traf afgørelse i disse sager i henholdsvis marts 2021 og september 2022. I begge sager blev der udtalt alvorlig kritik, og i sagen fra 2022 fik Familieretshuset tillige et påbud om at foretage en fornyet risikovurdering og på baggrund heraf at etablere fornødne organisatoriske eller tekniske sikkerhedsforanstaltninger for at mindske risikoen for nye lignende brud.

I juli 2024 udtalte Datatilsynet igen alvorlig kritik af Familieretshuset for manglende behandlingssikkerhed, der har ført til flere tilfælde af utilsigtet videregivelse af beskyttede oplysninger og oplysninger om ophold på krisecentre. Dette skete bl.a. som opfølgning på, at Familieretshuset i perioden fra den 6. januar 2023 til den 30. juni 2024 havde anmeldt 28 af ovennævnte type brud på persondatasikkerheden til Datatilsynet.

Det skete, selv om Datatilsynet kunne konstatere, at Familieretshuset igennem en årrække har taget initiativ til at gennemføre en række sikkerhedsforanstaltninger for at mindske risikoen for denne type af brud. I lyset af det fortsat forholdsvist høje antal brud og de meget alvorlige konsekvenser, denne type brud kan have for de berørte personer, var det i den forbindelse Datatilsynets opfattelse, at Familieretshuset fortsat og løbende skal udfolde endog meget store bestræbelser for at undgå utilsigtet

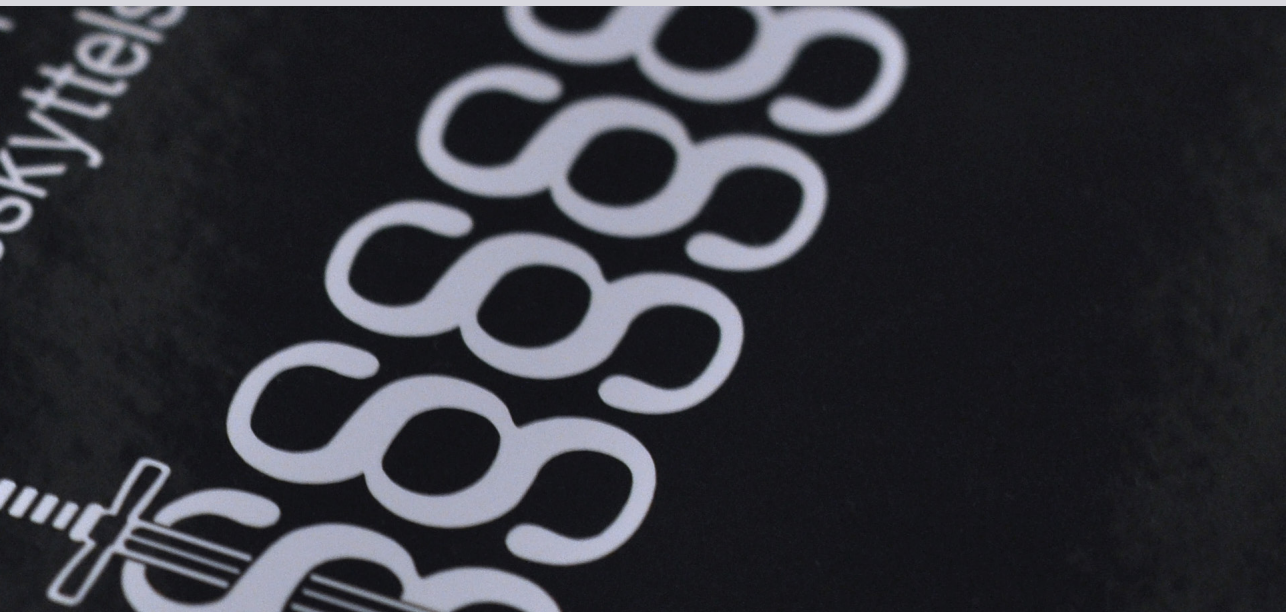
videregivelse af særligt oplysninger om beskyttede navne og adresser og ophold på krisecenter mv.

Endvidere var det Datatilsynets opfattelse, at Familieretshuset endnu ikke har implementeret tilstrækkelige sikkerhedsforanstaltninger – eller sikret, at de identificerede foranstaltninger endnu har haft den fornødne effekt – for at nedbringe risikoen for, at medarbejderne på grund af fejl, misforståelser eller uopmærksomhed utilsigtet videregiver oplysninger om registrerede til uvedkommende modtagere, herunder særligt sagens modpart, som ofte er årsagen til beskyttelsesbehovet.

Familieretshuset har således ikke i tilstrækkelig grad sikret, at medarbejderne har haft den fornødne omhu ved behandlingen af borgernes personoplysninger, herunder i forbindelse med den ekstra kontrol, der i visse tilfælde bliver udført af en anden sagsbehandler, ligesom der endnu ikke i tilstrækkeligt omfang er implementeret organisatoriske eller tekniske sikkerhedsforanstaltninger, som på anden vis kan afhjælpe de utilsigtede videregivelser af personoplysninger, der løbende er sket som følge af misforståelser, fejl eller uopmærksomhed hos medarbejderne.

Af afgørelsen fremgik herudover, at Datatilsynet fortsat vil følge udviklingen i antallet af Familieretshusets anmeldelser af brud på dette område tæt. Datatilsynet bad i den forbindelse Familieretshuset om i det kommende år at fremsende uddybende oplysninger – i forhold til de oplysninger, der allerede angives i forbindelse med anmeldelsen af bruddet – ved eventuelle fremtidige brud af samme type. Det omfatter bl.a. en uddybende beskrivelse af, hvad vurderingen af bruddet har ført til i forhold til at mindske risikoen for lignende brud.

Gentagne brud på persondatasikkerheden bør ifølge Datatilsynet generelt få dataansvarlige til at reflektere over allerede foretagne risikovurderinger. Brudtyper, der henføres til personlige fejl eller enkeltstående episoder, bør ved gentagelse give anledning til indførelse af yderligere effektive kontrolforanstaltninger, nye retningslinjer og eller teknisk understøttelse, der minimerer de nu kendte og aktualiserede risici.



# Tilladelser mv.

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

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

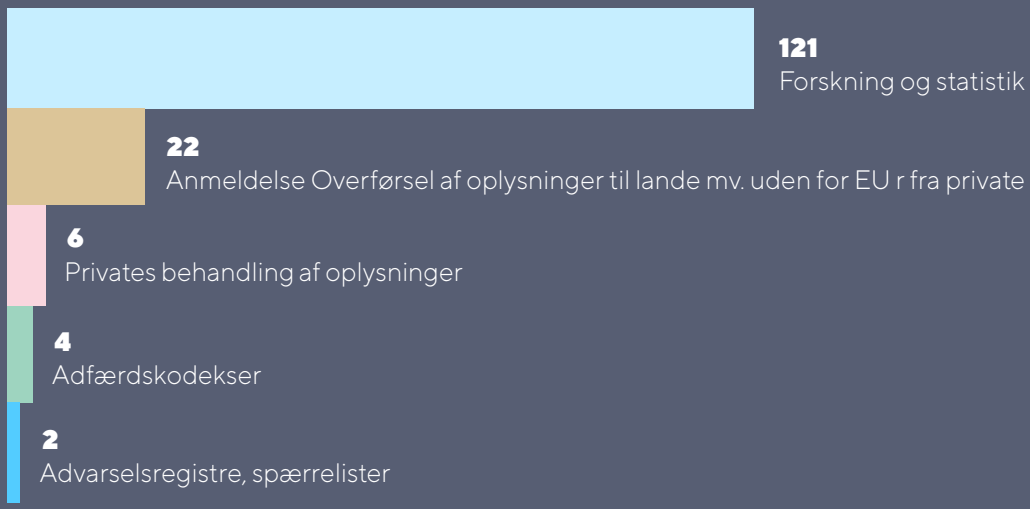
- Med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret (advarselsregister).
- Med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed (kreditoplysningsbureau).
- Udelukkende med henblik på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

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

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

På Datatilsynets hjemmeside findes flere oplysninger om de områder, hvor Datatilsynets tilladelse skal indhentes, ligesom blanketter til indgivelse af ansøgninger om visse tilladelser er tilgængelige på hjemmesiden. Endvidere offentliggøres der på hjemmesiden løbende et udvalg af konkrete tilladelser og afslag på tilladelse. I det følgende omtales et eksempel på en tilladelsessag, som Datatilsynet har behandlet i 2024.

**155** sager i alt




## Videregivelse af personoplysninger fra Danmarks Statistik til Hagstova Føroya

Datatilsynet gav i januar 2024 – i henhold til databeskyttelseslovens § 10, stk. 3, nr. 1 – Danmarks Statistik tilladelse til at videregive oplysninger om personer bosiddende på Færøerne og personer med færøsk oprindelse, der er bosiddende i Danmark, til Hagstova Føroya. Det drejede sig om cirka 105.000 personer, og oplysningerne omfattede bl.a. navn, køn fødselsdato, CPR-nummer eller det færøske P-tal og en række helbredsoplysninger.

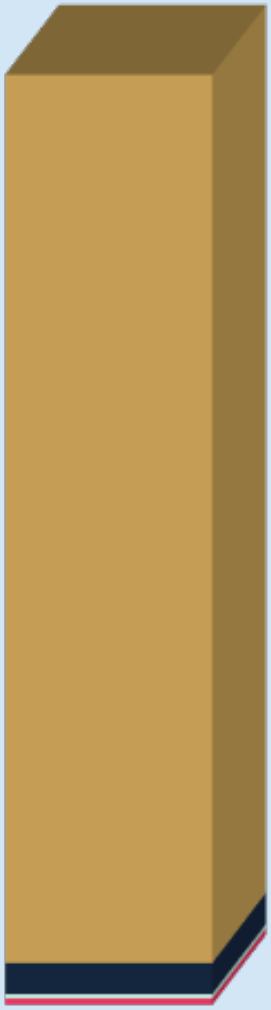
Hagstova Føroya er den centrale færøske institution for indsamling, bearbejdning og formidling af officiel statistik på Færøerne. Formålet med videregivelsen var, at oplysningerne skulle indgå i Hagstova Føroyas registre og bruges til at foretage statistisk belysning af væsentlige samfundsforhold og understøtte videnskabelige formål.

Anmodningen bestod i en løbende videregivelse af personoplysninger til statistisk brug hos en myndighed i et land uden for databeskyttelsesforordningens territoriale anvendelsesområde (men inden for rigsfællesskabet). For at opfylde formålet med videregivelsen, var det nødvendigt at få tilladelse til at videregive oplysningerne i ikke-pseudonymiseret form.

Efter at spørgsmålet havde været behandlet på et møde i Datarådet, fik Danmarks Statistik tilladelse til at videregive oplysningerne til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde.

# Internationalt arbejde

**1146** sager i alt



**1092** EU-sager

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

**6** Nordisk tilsynssamarbejde

**8** 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 tilsynsmyndigheder. Dette afspejler sig i Datatilsynets daglige arbejde i forhold til både udarbejdelse af generel vejledning og behandling af konkrete sager og tilsyn. Det er derfor af afgørende betydning, at 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.

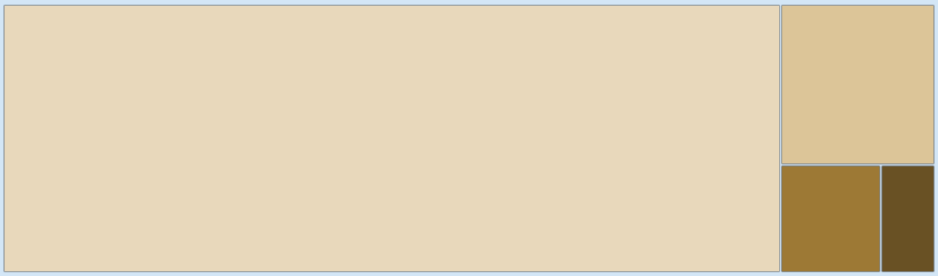
## Fordeling af EU-sager

**911** One-stop-shop-mekanismen

**108** Fælleseuropæiske systemer mv.

**25** Databeskyttelsesrådet

**48** 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 EU-medlemslandenes 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 de 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 de nationale tilsynsmyndigheder, og som har grænseoverskridende virkninger.
- Træffe bindende afgørelser om fortolkningen af databeskyttelsesreglerne, f.eks. hvor de nationale tilsynsmyndigheder har forskellige opfattelser af, hvordan en konkret sag skal afgøres, eller hvis en national tilsynsmyndighed ikke følger rådets udtalelse om et udkast til afgørelse.
- Rådgive Europa-Kommissionen om et hvert 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 on line eller fysisk.

Arbejdet med forberedelsen af vejledninger, udtalelser, afgørelser mv., som EDPB skal godkende, forestås primært af 13 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.

## Ny strategi for EDPB blev vedtaget

I april 2024 vedtog EDPB en strategi for årene 2024-2027. Ligesom den tidligere strategi, der gjaldt for 2021-2023, er der tale om en strategi, der ikke går i detaljen, men derimod har som mål at sætte en overordnet retning.

Medarbejdere fra Datatilsynet har været blandt penneførerne på det udkast, som blev vedtaget. Strategien består af fire hovedsøjler, der fremhæver de vigtigste mål. Hver af søjlerne indeholder tre nøgleaktiviteter, som skal gennemføres for at nå målene.

De fire hovedsøjler er:

- Enhancing harmonisation and promoting
- Reinforcing a common enforcement and culture and effective cooperation
- Safeguarding data protection in the developing digital and cross-regulatory landscape
- Contributing to the global dialogue on data protection

EDPB følger løbende op på indfrielsen af strategiens mål i årsberetningerne.

## EDPB-rapport om ChatGPT

I 2023 besluttede EDPB at nedsætte en taskforce til håndtering af udveksling af oplysninger og fremme af samarbejdet vedrørende eventuelle foranstaltninger, der træffes af de europæiske tilsynsmyndigheder over for ChatGPT. Datatilsynet har deltaget i taskforcen siden oprettelsen.

I maj 2024 vedtog og offentliggjorde EDPB en rapport, som taskforcen havde udarbejdet. Rapporten indeholder de indledende konklusioner fra de undersøgelser, som er foretaget af flere europæiske tilsyn. Idet sagerne mod ChatGPT endnu ikke er afsluttet, er konklusionerne i rapporten kun foreløbige.

Rapporten skelner mellem ChatGPT's indsamling af træningsdata, "forbehandling" af data (herunder filtrering), træning, "prompts" og output og træning af ChatGPT med "prompts". Herefter gennemgår rapporten de principper, som skal overholdes ved hvert af ovennævnte stadier af ChatGPT's behandling af data, herunder lovlighed, rimelighed, gennemsigtighed, rigtighed samt de registreredes rettigheder.

Siden taskforcens oprettelse har virksomheden etableret sig i Irland, hvorfor Irland på nuværende tidspunkt er ledende tilsynsmyndighed for ChatGPT.

## Vejledning om interesseafvejningsreglen

På plenarmødet i oktober 2024 vedtog EDPB en vejledning om den såkaldte interesseafvejningsregel i databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Den første del af vejledningen er en introduktion til interesseafvejningsreglen som behandlingsgrundlag. I vejledningens anden del foretages en analyse af de elementer, den dataansvarlige skal tage højde for, og en gennemgang af de tre trin, man som dataansvarlig skal følge ved brug af interesseafvejningsreglen. Vejledningens tredje del belyser forholdet mellem interesseafvejningsreglen og de registreredes rettigheder. Fjerde del af vejledningen beskriver brugen af interesseafvejningsreglen i konkrete situationer, herunder behandling med henblik på direkte markedsføring og offentlige myndigheders brug af reglen.

Vejledningen har bl.a. til formål at opdatere og bygge videre på den såkaldte Artikel 29-gruppes udtalelse fra 2014 om de tilsvarende regler i det på daværende tidspunkt gældende persondatadirektiv.

## Vejledning om databeskyttelsesforordningens artikel 48

I december 2024 vedtog EDPB en vejledning om databeskyttelsesforordningens artikel 48, som vedrører den situation, hvor en myndighed i et tredjeland (et land uden for EU) på grundlag af en dom eller afgørelse kræver, at en dataansvarlig eller databehandler i EU udleverer personoplysninger.

Hovedbudskabet i vejledningen er, at artikel 48 først og fremmest er en præcisering af, hvad der allerede gælder efter international ret og databeskyttelsesreglerne. Bestemmelsen minder med andre ord om, at domme og afgørelser fra myndigheder i tredjelande kun kan anerkendes eller håndhæves i en EU-medlemsstat, hvis dette er fastsat i en international aftale mellem tredjelandet og den pågældende medlemsstat (eller EU). Hvis en dataansvarlig eller databehandler i EU udleverer personoplysninger til en myndighed i et tredjeland, vil dette være en overførsel til et tredjeland i databeskyttelsesforordningens forstand, hvilket både kræver et behandlingsgrundlag i artikel 6 og et overførselsgrundlag i kapitel V.

Hvis der er indgået en international aftale mellem tredjelandet og den pågældende medlemsstat (eller EU), vil denne efter omstændighederne kunne udgøre både det fornødne behandlingsgrundlag og overførselsgrundlag. Hvis dette ikke er tilfældet, skal det undersøges, om andre behandlingsgrundlag og overførselsgrundlag i databeskyttelsesforordningen kan anvendes. Hvis dette heller ikke er muligt, kan personoplysningerne ikke udleveres til tredjelandet.

## 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 databeskyttelsesforordningen.

I januar 2024 vedtog EDPB en rapport om den fælles undersøgelse fra 2023, som omhandlede rollen som databeskyttelsesrådgiver. Datatilsynet deltog i undersøgelsen sammen med 25 andre lande.

Både offentlige myndigheder og private virksomheder blev kontaktet i forbindelse med undersøgelsen, og der er modtaget mere end 17.000 svar tilsammen. Datatilsynet tog i sin del af undersøgelsen udgangspunkt i rollen som DPO i de danske kommuner, og resultaterne heraf indgår i den samlede rapport.

Resultaterne af undersøgelsen er ifølge rapporten overvejende positive. Størstedelen af DPO'erne har anført:

- at de har de nødvendige færdigheder og viden til at kunne udføre deres arbejde, og at de modtager regelmæssig uddannelse,
- at de har klart definerede opgaver i overensstemmelse med GDPR, og at de ikke modtager instrukser om, hvordan de skal udføre deres opgaver,
- at de i de fleste tilfælde høres, og at de får tilstrækkelige oplysninger til, at de kan udføre deres opgaver og,
- at de har midlerne til at udføre deres opgaver.

På trods af dette er der ifølge rapporten stadig en række udfordringer forbundet med DPO'ens rolle, og der er for mange DPO'er, der ikke har de mest nødvendige forudsætninger for at udføre deres arbejde i overensstemmelse med GDPR.

Rapporten opstiller derfor en række punkter som tilsynsmyndigheder, dataansvarlige og DPO'er skal være opmærksomme på. Til hvert punkt er der knyttet en række anbefalinger, der kan hjælpe med at sætte fokus på punkterne.


THE
FUTURE
IS
EUROPE

## Udtalelser fra EDPB som en del af sammenhængsmekanismen

Med henblik på at sikre en ensartet anvendelse af databeskyttelsesreglerne i hele EU/EØS er der i databeskyttelsesforordningens artikel 63 etableret en såkaldt sammenhængsmekanisme. Som en del af denne sammenhængsmekanisme har bl.a. de enkelte medlemsstaters tilsynsmyndigheder i medfør af databeskyttelsesforordningens artikel 64, stk. 2, mulighed for at anmode Det Europæiske Databeskyttelsesråd (EDPB) om en udtalelse med henblik på at få afklaret et generelt spørgsmål om fortolkningen af databeskyttelsesreglerne eller et spørgsmål, som har betydning for flere medlemsstater.

Der er ikke fastsat nogen begrænsninger for, hvilke emner tilsynsmyndighederne kan spørge EDPB om, men ofte vil der være tale om spørgsmål om, hvordan databeskyttelsesreglerne skal fortolkes i forhold til nye teknologiske løsninger eller nye forretningsmodeller.

Hvis anmodningen overholder de formkrav, der er fastsat, er EDPB ifølge databeskyttelsesforordningens artikel 64, stk. 3, forpligtet til at afgive en udtalelse om det spørgsmål, som er stillet af tilsynsmyndigheden. Udtalelsen skal vedtages inden for otte uger med simpelt flertal blandt medlemmerne af EDPB. Fristen kan dog forlænges med seks uger, hvis der er tale om et komplekst spørgsmål.

I løbet af 2024 afgav EDPB fem udtalelser af denne type.

### *Udtalelse om begrebet en dataansvarligs hovedvirksomhed i Unionen*

Den første udtalelse i 2024 efter proceduren i databeskyttelsesforordningens artikel 64, stk. 2 og 3, blev vedtaget af EDPB i februar efter anmodning fra datatilsynet i Frankrig. Udtalelsen omhandler begrebet en dataansvarligs hovedvirksomhed i Unionen i henhold til databeskyttelsesforordningens artikel 4, stk. 16, litra a. Udtalelsen blev udarbejdet på anmodning af det franske datatilsyn

EDPB konkluderer i sin udtalelse, at "stedet for [den dataansvarliges] centrale administration i Unionen" kun kan betragtes som hovedvirksomhed i henhold til forordningens artikel 4, stk. 16, litra a, hvis det træffer beslutninger vedrørende formål og hjælpemidler i forbindelse med behandling af personoplysninger, og hvis det har beføjelse til at få disse beslutninger gennemført.

I udtalelsen præciserer EDPB bl.a. også, hvordan tilsynsmyndighederne i praksis bør anvende forordningens artikel 4, stk. 16, litra a, for at sikre en ensartet anvendelse heraf. EDPB gentager navnlig, at bevisbyrden i forhold til det sted, hvor de relevante beslutninger om behandling træffes, og hvor der er beføjelse til at gennemføre sådanne beslutninger i Unionen, i sidste ende påhviler de dataansvarlige, og at de har pligt til at samarbejde med tilsynsmyndighederne.

### *Udtalelse om "giv samtykke eller betal"-modeller*

I april 2024 vedtog EDPB sin anden udtalelse efter proceduren i databeskyttelsesforordningens artikel 64, stk. 2 og 3. Udtalelsen omhandler store onlineplatformes brug af såkaldte "giv samtykke eller betal"-modeller, hvor den registrerede tilbydes et valg med hensyn til at få adgang til den dataansvarliges online service. Ofte består valget i, at den registrerede enten kan give samtykke til behandling af personoplysninger til brug for adfærdsbaseret markedsføring eller betale et pengebeløb for adgang til den pågældende service.

Anmodningen om udtalelsen blev fremsat af datatilsynene i Norge, Holland og Tyskland (Hamborg). Det skete i lyset af EU-Domstolens dom i sagen C-252/21, Meta Platforms Inc. m.fl. og på baggrund af, at flere tilsyn i EU/EØS-lande havde vedtaget nationale retningslinjer for mindre virksomheders brug af disse løsninger. Datatilsynet fulgte udtalelsens tilblivelse tæt og gjorde sin indflydelse gældende undervejs.

I udtalelsen adresserer EDPB, hvordan de såkaldte "giv samtykke eller betal"-modeller kan implementeres af "store onlineplatforme" på en måde, der overholder kravene til et gyldigt, og navnlig frivilligt, samtykke, og i sin konklusion understreger EDPB vigtigheden af, at platformen – i overensstemmelse med princippet om ansvarlighed – skal kunne dokumentere, at alle kravene til et gyldigt samtykke er opfyldt.
I umiddelbar forlængelse af udtalelsen besluttede EDPB i maj 2024 at igangsætte et arbejde med at udarbejde egentlige retningslinjer om brugen af "giv samtykke eller betal"-modeller. Til forskel fra udtalelsen skal retningslinjerne adressere spørgsmålet om indhentning af gyldigt samtykke mere generelt og er således ikke begrænset til store onlineplatformes brug af sådanne modeller.

Grundlæggende skal retningslinjerne bygge videre på udtalelsen fra april 2024 og udfolde analyserne i udtalelsen i en generel kontekst. Retningslinjerne skal derudover adressere flere emner, som f.eks. brugen af "giv samtykke eller betal"-modeller i relation til mindreårige, samspillet med ePrivacy-direktivet og sammenhængen med udøvelsen af de registreredes rettigheder.

Datatilsynet deltager aktivt i dette arbejde, da tilsynet allerede har afgjort flere sager på området.

### *Udtalelse om ansigtsgenkendelse i lufthavne*

Den tredje udtalelse i 2024 efter proceduren i databeskyttelsesforordningens artikel 64, stk. 2 og 3, blev vedtaget af EDPB i maj. Udtalelsen omhandler brugen af ansigtsgenkendelse i lufthavne med henblik på at strømline passagerflowet og give en bedre brugeroplevelse. EDPB var blevet anmodet om i udtalelsen at vurdere, hvorvidt denne brug var forenelig med databeskyttelsesforordningens artikel 5, stk. 1, litra e og f, artikel 25 og artikel 32.

EDPB fastslår i udtalelsen, at det ikke vil være i overensstemmelse med bl.a. databeskyttelsesforordningens artikel 25, hvis de biometriske data (billede og template) opbevares uden for den registreredes (dvs. passagerens) egen kontrol.

Udtalelsen blev udarbejdet på anmodning af det franske datatilsyn, idet den pågældende form for ansigtsgenkendelse allerede var påbegyndt i test i flere lufthavne i Frankrig og andre EU-lande.

Datatilsynet orienterede de danske lufthavne om udtalelsen.

### *Udtalelse om den dataansvarliges forpligtelser ved brug af databehandlere*

På plenarmødet i oktober 2024 vedtog EDPB sin fjerde udtalelse i medfør af databeskyttelsesforordningens artikel 64, stk. 2 og 3, om dataansvarliges forpligtelser ved brugen af databehandlere.

Anmodningen om udtalelsen blev fremsat af Datatilsynet i lyset af, at mange dataansvarlige – både i Danmark og i resten af Europa – i vidt omfang gør brug af databehandlere, herunder navnlig i forbindelse med brugen af cloudservices, hvor cloudleverandøren ofte benytter sig af en række underleverandører til brug for levering af sine services. Et af de områder, som mange dataansvarlige løbende oplever udfordringer med, er spørgsmålet om den dokumentation, som de dataansvarlige skal tilvejebringe for i sidste led at sikre overholdelsen af GDPR.

I udtalelsen adresserer EDPB bl.a. spørgsmålet om, i hvilket omfang man som dataansvarlig skal kunne identificere alle sine databehandlere, og i hvilket omfang den dataansvarlige skal verificere og dokumentere, at underdatabehandlere faktisk bliver pålagt de samme databeskyttelsesforpligtelser som den første databehandler.

Udtalelsen adresserer også spørgsmålet om den dataansvarliges dokumentationsforpligtelse i den situation, hvor en databehandler inden for EU/EØS overfører personoplysninger til en (under)databehandler i et tredjeland.

### *Udtalelse om udvikling og anvendelse af AI-modeller*

I december 2024 vedtog EDPB sin femte udtalelse i medfør af databeskyttelsesforordningens artikel 64, stk. 2 og 3, om en række databeskyttelsesretlige aspekter i forbindelse med udvikling og drift af AI-modeller.

Anmodningen om udtalelsen blev fremsat af datatilsynet i Irland bl.a. med henblik på bedre at kunne vejlede om en række af de problemstillinger, der opstår hos de dataansvarlige, når de udvikler eller anvender AI-modeller.

I udtalelsen bekræfter EDPB, at AI-modeller, som er trænet ved behandling af personoplysninger, efter omstændighederne vil kunne anonymiseres i databeskyttelsesretlig forstand. EDPB opstiller en række elementer, der kan indgå i denne vurdering.
EDPB tager også stilling til behandlingsgrundlaget i forbindelse med udvikling og anvendelse af AI-modeller.

Endelig behandler udtalelsen spørgsmålet om, hvorvidt en ulovlig behandling af personoplysninger i udviklingsfasen påvirker lovligheden i forbindelse med den efterfølgende anvendelse af AI-modellen. EDPB understreger bl.a., at en forudgående overtrædelse af reglerne på et tidligere stadie efter omstændighederne kan have en indvirkning på vurderingen af lovligheden af en efterfølgende behandling.

## Europa-Kommissionen opretholder 11 tilstrækkelighedsafgørelser

I januar 2024 udgav EU-Kommissionen sin evalueringsrapport om 11 såkaldte tilstrækkelighedsafgørelser vedtaget under det tidligere gældende databeskyttelsesdirektiv.

I rapporten konkluderede EU-Kommissionen, at personoplysninger, som overføres fra EU/EØS til Andorra, Argentina, Canada, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz og Uruguay, fortsat er sikret et tilstrækkeligt beskyttelsesniveau. Dermed opretholdes de 11 tilstrækkelighedsafgørelser, og personoplysninger kan derfor frit overføres til de pågældende lande og territorier.

EU-Kommissionens evaluering af tilstrækkelighedsafgørelserne viste også, at niveauet for databeskyttelse i alle 11 lande og territorier er højnet og kommet tættere på standarden i EU/EØS, siden afgørelserne blev vedtaget. Databeskyttelsesforordningen har således haft en positiv indflydelse på udviklingen, herunder er der kommet flere rettigheder for de registrerede, tilsynsmyndighedernes uafhængighed og beføjelser er styrket, og reglerne for internationale overførsler af personoplysninger er opdateret. Endvidere er offentlige myndigheder i de 11 lande og territorier ifølge EU-Kommissionen underlagt passende garantier med hensyn til deres adgang til personoplysninger, navnlig med henblik på retshåndhævelse eller national sikkerhed. Dette omfatter effektive tilsyns- og klagemekanismer for de registrerede.

## Nye klageformularer vedrørende overførsler af personoplysninger til USA

I sommeren 2023 afgjorde EU-Kommissionen, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger overført fra EU/EØS til virksomheder omfattet af EU-U.S. Data Privacy Framework. Tilstrækkelighedsafgørelsen har stor betydning for samarbejdet mellem europæiske og amerikanske virksomheder.

En helt grundlæggende forudsætning for EU-Kommissionens afgørelse var, at personer i EU/EØS skulle have adgang til at klage over behandlingen af deres personoplysninger, som var overført på baggrund af tilstrækkelighedsafgørelsen. I april 2024 vedtog EDPB i den forbindelse to klageformularer til formålet:

- Den ene klageformular kan benyttes til at klage til et datatilsyn i EU/EØS over en amerikansk virksomheds manglende overholdelse af EU-U.S. Data Privacy Framework.
- Den anden klageformular kan benyttes til klager over amerikanske efterretningstjenesters behandling af personoplysninger overført til USA. Sådanne klager skal også indgives til det nationale datatilsyn i EU/EØS, som herefter videreformidler klagen til klageinstansen i USA.

## Første evaluering af EU-U.S. Data Privacy Framework

Den første evaluering af tilstrækkelighedsafgørelsen for EU-U.S. Data Privacy Framework (DPF) fandt sted i juli 2024 i Washington, D.C. En delegation bestående af repræsentanter for EU-Kommissionen og Det Europæiske Databeskyttelsesråd (EDPB) – herunder en medarbejder fra Datatilsynet – deltog i to dages møder med de involverede amerikanske myndigheder samt repræsentanter for private klageorganer og DPF-certificerede virksomheder.

Forud for de fysiske møder havde delegationen udsendt spørgeskemaer til amerikanske erhvervsorganisationer og NGO'er og holdt et onlinemøde med en række amerikanske NGO'er inden for digitale rettigheder og privatlivsbeskyttelse. Målet var at indsamle tilstrækkeligt med information til at kunne vurdere, om DPF-ordningen og den relevante amerikanske lovgivning fungerede efter hensigten, og om tilstrækkelighedsafgørelsen dermed kunne opretholdes.

På baggrund af evalueringen offentliggjorde EU-Kommissionen i oktober 2024 en rapport til Europa-Parlamentet og Rådet, hvori man konkluderede, at de fornødne procedurer var på plads for at sikre, at DPF-ordningen fungerer efter hensigten. Dermed kan personoplysninger fortsat overføres til DPF-certificerede virksomheder i USA uden yderligere foranstaltninger.

I forlængelse af EU-Kommissionens rapport fulgte EDPB i november 2024 op med sin egen rapport og anbefalinger. Rapporten var overordnet positiv over for de amerikanske myndigheders implementering af DPF-ordningen og relevant ny lovgivning, særligt vedrørende efterretningstjenesternes adgang til overførte oplysninger og klageadgang for registrerede på dette område. Rapporten indeholdt dog også en række anbefalinger og opmærksomhedspunkter, som vil blive fulgt op på i forbindelse med næste evaluering.

## 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. Endvidere deltager Datatilsynet på EU-niveau i en koordinationsgruppe for tilsynet med SIS (SIS CSC). Der har i 2024 været afholdt 6 møder i denne gruppe.

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

Datatilsynet har efterfølgende samarbejdet med evalueringsholdet om opfølgningen på evalueringen. Den endelige evalueringsrapport blev vedtaget i 2024. Datatilsynet skal herefter følge op på rapportens anbefalinger og bemærkninger.

### VIS (Visuminformationssystemet)

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

I 2024 traf Datatilsynet afgørelse i en sag med Udlændinge- og Integrationsministeriet, hvor tilsynet bl.a. konstaterede, at ministeriet har etableret en sletteprаksis i det nationale visuminformationssystem, hvor visumsager automatisk bliver slettet som udgangspunkt 5 år fra f.eks. udløbet af et visum, datoen for meddelelse af et afslag mv. Der blev imidlertid ikke ført kontrol med, at den automatiske sletteprаksis fungerer efter hensigten.

Det er Datatilsynets vurdering, at løbende kontrol med overholdelse af den dataansvarliges slettefrister er en forudsætning for, at den dataansvarlige i henhold til princippet om ansvarlighed efter databeskyttelses-forordningens artikel 5, stk. 2, kan påvise at overholde princippet om opbevaringsbegrænsning i artikel 5, stk. 1, litra e.

Herudover følger det af VIS-forordningens artikel 25, stk. 1, at oplysningerne i en visumansøgningssag straks skal slettes fra

visuminformationssystemet, hvis ansøgeren inden slettefristens udløb opnår statsborgerskab i en medlemsstat.

Udlændinge- og Integrationsministeriet havde imidlertid en praksis, hvor den registrerede blev vejledt til selv at kontakte Udlændingestyrelsen med henblik på at få oplysninger slettet i systemet, i stedet for at ministeriet slettede oplysningerne af egen drift. Det er Datatilsynets vurdering, at en sådan fremgangsmåde ikke lever op til VIS-forordningens krav om sletning før tid.

Datatilsynet udtalte på den baggrund kritik af Udlændinge- og Integrationsministeriet.
Som led i tilsynet med behandling af personoplysninger i VIS deltager Datatilsynet også på EU-niveau i en koordinationsgruppe for tilsynet med visuminformationssystemet (VIS CSC). Der har i 2024 været afholdt to møder.

## 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 2024 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.

## 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 toldadministration.

Toldstyrelsen er dataansvarlig for CIS i Danmark, og Datatilsynet fører 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 2024 været afholdt to møder.

## 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 2024 været afholdt 6 møder, hvor man bl.a. arbejder på et sæt anbefalinger til nationale myndigheder om iagttagelse af oplysningspligten, når personoplysninger behandles i IMI.

## Europarådet

Europarådet danner rammen om et samarbejde mellem 47 lande, herunder de 27 EU-lande. Danmark var blandt de 10 stiftende medlemmer af Europarådet i 1949. Medlemskab af Europarådet kræver, at staterne underskriver Den Europæiske Menneskerettighedskonvention (EMRK).

I databeskyttelsessammenhæng har Danmark ratificeret Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) og tillægsprotokollen om tilsynsmyndigheder og grænseoverskridende dataudveksling (konvention 181). Datatilsynet er udpeget som tilsynsmyndighed i forhold til konvention 108.

Af ressourcemæssige årsager har Datatilsynet ikke deltaget i møder i Europarådet i 2024.

## 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 2024 afholdt to møder (Oslo og Bruxelles).

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

I 2024 har gruppens fokus på privatliv og sikkerhed vedrørt følgende Working Papers:

- AI, store sprogmodeller: Omhandler brugen af personoplysninger i store sprogmodeller, lovlighed ved træning og dataindsamling samt gennemsigtighed og de registreredes rettigheder.
- Datadeling: Omhandler udbredelsen og brugen af data på tværs af platforme, regler og jurisdiktioner, særligt i forhold til formålsbegrænsning og de registreredes rettigheder. Der arbejdes herudover på et papir om udfordringerne ved globale standarder for teknologier til samtykkestyring.
- Digitale centralbankpenge: Forholder sig til indsamling og behandling af oplysninger ved brug af applikationer, software og hardware i tilknytning til digitale valutaer. Der er i dokumentet fokus på den afkobling, der skal ske mellem individet og transaktionerne for alle andre end dem, der er involveret i den konkrete transaktion. Særligt er der fokus på at eliminere reidentifikation. Gruppens mål har været at få lavet beskrivelser og oplæg til at adressere de pågældende problemstillinger.

I årets løb har Berlin-gruppen i øvrigt arbejdet med aktuelle emner, som indeholder problemstillinger med hensyn til databeskyttelse og beskyttelse af privatliv. Det gælder eksempelvis quantum computing, neuroteknologi, genomics, immersive virtuel worlds (extended reality), biometri i elektronisk online autentifikation, ISO-standardisering, privatlivsbeskyttelse ved ICANN's RDS (Registration Directory Services) for internettet og forhold omkring fake news, informationsmonopolisering, 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.

Hvert år afholdes der et officielt nordisk møde, hvor alle de nordiske datatilsyn samles for at drøfte aktuelle spørgsmål på databeskyttelsesområdet. I 2024 fandt mødet sted i maj i Oslo. Som det har været en tradition, siden det danske datatilsyn som afslutning på det nordiske møde i 2018 i København introducerede det, vedtog de nordiske lande også i 2024 en "Oslo-erklæring".

Af "Oslo-erklæringen, der er offentliggjort og stadig tilgængelig på Datatilsynets hjemmeside, fremgår det, at de nordiske lande har fokus på bl.a. kunstig intelligens, de mange andre retsakter, der er en del af EU's digitale pakke og fastsættelse af bøder for overtrædelse af databeskyttelsesreglerne. De nordiske tilsynsmyndigheder vedtog endvidere et sæt fælles principper, som skal styrke databeskyttelsen af børn i forbindelse med online gaming.

## Den europæiske konference

Den europæiske konference for databeskyttelsesmyndigheder, også kaldet Forårskonferencen, afholdes en gang årligt. Datatilsynet var repræsenteret på konferencen i 2024, som blev afholdt i Riga.

På konferencen drøftede deltagerne bl.a. databeskyttelsesmyndighedernes rolle i forhold til kunstig intelligens og andre nye teknologier, helbredsoplysninger og digitalisering samt mulighederne for et øget samarbejde på tværs af landegrænserne. Endvidere blev der set nærmere på samspillet mellem AML-reguleringen og databeskyttelsesreglerne.

## 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 den såkaldte Berlin-gruppe, der har skiftet navn til Den internationale arbejdsgruppe om databeskyttelse i teknologi (International Working Group on Data Protection in Technology), jf. ovenfor.

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 2024 i Jersey, som Datatilsynet deltog i, vedtog GPA en række resolutioner. Der blev bl.a. vedtaget en resolution, som opfordrer til brugen af certificeringsordninger på databeskyttelsesområdet, en resolution om behandling af personoplysninger inden for neurovidenskab og neuroteknologi samt en resolution om standarder for overførsel af personoplysninger på tværs af landegrænser.

# Grønland og Færøerne

**25** 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 2024 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.

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 an- klagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk data behandling, 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, af sløre 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 Domstols-styrelsen og retterne i overensstemmelse med retshåndhævelseslovens regler.

I 2024 har Datatilsynet på retshåndhævelsesområdet bl.a. behandlet klagesager, forespørgsler og anmeldelser om brud på persondatasikkerheden.


POLITI

## Politikredse fik kritik for manglende behandlingssikkerhed

I 2024 afsluttede Datatilsynet tre skriftlige tilsyn med henholdsvis Nordjyllands Politi, Fyns Politi og Bornholms Politis brugerstyring og logkontrol af politiets sagsstyringssystem POLSAS. De tre politikredse blev udpeget til et tilsyn ud fra, at de varierer i størrelsen, ligesom Datatilsynet ønskede en geografisk spredning.

Politikredsenes oplysninger om brugerstyring i POLSAS – dvs. administration af adgangsrettigheder, herunder hvordan adgangsrettigheder tildeles og afmeldes – gav ikke Datatilsynet anledning til bemærkninger.

Datatilsynet fandt imidlertid anledning til at udtale kritik af, at politikredsenes logkontrol ikke var i overensstemmelse med reglerne om behandlingssikkerhed, idet de ikke havde implementeret faste procedurer for løbende logkontrol (f.eks. ved stikprøvekontrol) for at sikre, at brugerne kun tilgår oplysninger, de har et arbejdsbetinget behov for at behandle. Politikredsene kontrollerede kun loggen ved konkret mistanke om misbrug.

Det er Datatilsynets opfattelse, at kravet om passende sikkerhed normalt vil indebære, at den dataansvarlige løbende foretager stikprøver af loggen for at kontrollere, at brugerne kun tilgår oplysninger, de har et arbejdsbetinget behov for. En konkret risikovurdering kan danne grundlag for, hvordan og hvor ofte denne kontrol skal udføres. Det er dog tilsynets opfattelse, at stikprøvekontrol hvert halve år ofte vil være et absolut minimum, hvis der er tale om en bred adgang, hvor medarbejdere har adgang til mange fortrolige eller følsomme oplysninger og/eller adgang til oplysninger om mange personer. Dataansvarlige kan endvidere overveje at etablere alarmer (f.eks. baseret på logdata), som automatisk aktiveres ved mistænkelig aktivitet – og dette kan supplere eller erstatte mere tilfældigt udvalgte stikprøver.

Logkontrol har umiddelbart en korrigerende funktion, men et andet væsentligt formål med implementering af logkontrol er, at det kan have en forebyggende effekt. Orientering til medarbejdere om, at der løbende gennemføres logkontrol, kan derfor være et effektivt middel til at reducere risikoen for misbrug af ellers legitime adgangsrettigheder.

Forebyggelse af misbrug af adgangsrettigheder bør efter Datatilsynets opfattelse ske ved en kombination af awareness bl.a. om, hvad der er berettiget/uberettiget opslag, systematisk rettighedsstyring samt logning og løbende kontrol af brugernes opslag i systemer, hvori der behandles personoplysninger. Derudover skal den dataansvarlige sikre en effektiv håndhævelse af reglerne.

Datatilsynet lagde i vurderingen af sagerne vægt på, at der i POLSAS både behandles almindelige, følsomme og andre beskyttelsesværdige personoplysninger, og at reelt alle medarbejdere i politikredsene har adgang til POLSAS – og som udgangspunkt også adgang til alle sager og oplysninger i systemet.

Datatilsynet bemærkede i øvrigt i anledning af tilsynet, at:

- arbejdsgivere skal overholde de databeskyttelsesretlige regler om oplysningspligt ved iværksættelse af kontrolforanstaltninger som f.eks. logkontrol. Det indebærer, at medarbejderne klart og utvetydigt skal informeres om, at registreringen og kontrollen foretages.
- når der er tale om fælles dataansvar mellem to eller flere parter, er det vigtigt at udarbejde en aftale, der tydeligt fastlægger deres respektive ansvar for overholdelse af de forskellige pligter, der pålægges en dataansvarlig efter databeskyttelsesforordningen. To af politikredsene gav udtryk for, at den manglende gennemførelse af stikprøvekontrol skyldtes en misforståelse af, at en sådan kontrol blev udført af Rigspolitiet.

Datatilsynet orienterede Rigspolitiet om tilsynene og bemærkede i den forbindelse, at tilsynet forudsætter, at det sikres, at der også implementeres behørig logkontrol hos de øvrige politikredse, hvis ikke det allerede er sket.

## Spørgsmål til Rigspolitiet om brug af ansigtsgenkendelse

I september 2024 udsendte Justitsministeriet en pressemeddelelse om, at regeringen er blevet enige med flere partier om at give politiet øget mulighed for at benytte ansigtsgenkendelsesteknologi i efterforskningen – i første omgang ved sager om personfarlig kriminalitet som drab, grov vold og voldtægt. Pressemeddelelsen blev udsendt samtidig med, at der i slutningen af august i medierne havde været en artikel om, at politiet allerede forberedte et projekt om netop dette med henblik på hurtigt at kunne tage det i brug efter en politisk beslutning.

På den baggrund sendte Datatilsynet en række spørgsmål om den påtænkte brug af ansigtsgenkendelse til Rigspolitiet. Spørgsmålene omhandlede blandt andet Rigspolitiets overvejelser om udarbejdelse af konsekvensanalyse og forudgående høring af Datatilsynet.

I sit svar til Datatilsynet oplyste Rigspolitiet, at der endnu ikke var udarbejdet en konsekvensanalyse for det pilotprojekt, som omfatter ansigtsgenkendelse, da anskaffelsen af det relevante system stadig var i en tidlig fase. Rigspolitiet understregede dog, at en konsekvensanalyse ville blive igangsat, så snart grundlaget herfor var til stede i projektet, og Datatilsynet vil blive orienteret om resultatet.

I oktober 2024 sendte Datatilsynet et svar retur til Rigspolitiet og oplyste, at tilsynet ser frem til at modtage konsekvensanalysen, når den foreligger. Tilsynet bemærkede i den forbindelse, at enhver behandling af personoplysninger omfattet af retshåndhævelsesloven - herunder behandling til tests og pilotprojekter - skal leve op til reglerne i loven. Dette indebærer bl.a., at hvis behandlingen af personoplysninger kræver en konsekvensanalyse, skal denne analyse gennemføres før behandlingen påbegyndes.

# 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 opgaver

Tilsynet med databeskyttelsesområdet indebærer et stort antal forskelligartede opgaver. Datatilsynet har i 2024 bl.a. haft følgende opgaver:

- Information, rådgivning og vejledning.
- Behandling af klagesager.
- Behandling af anmeldelser af brud på persondatasikkerheden.
- Sager på Datatilsynets eget initiativ, herunder tilsyn med offentlige myndigheder og private dataansvarlige mv.
- Udtalelser om lovudkast 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 Data beskyttelsesråd (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. på Schengen-, visum og toldområdet), hvilket betyder, at tilsynet fører tilsyn med de danske myndigheders behandling af oplysninger i forbindelse med brugen af disse systemer.

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

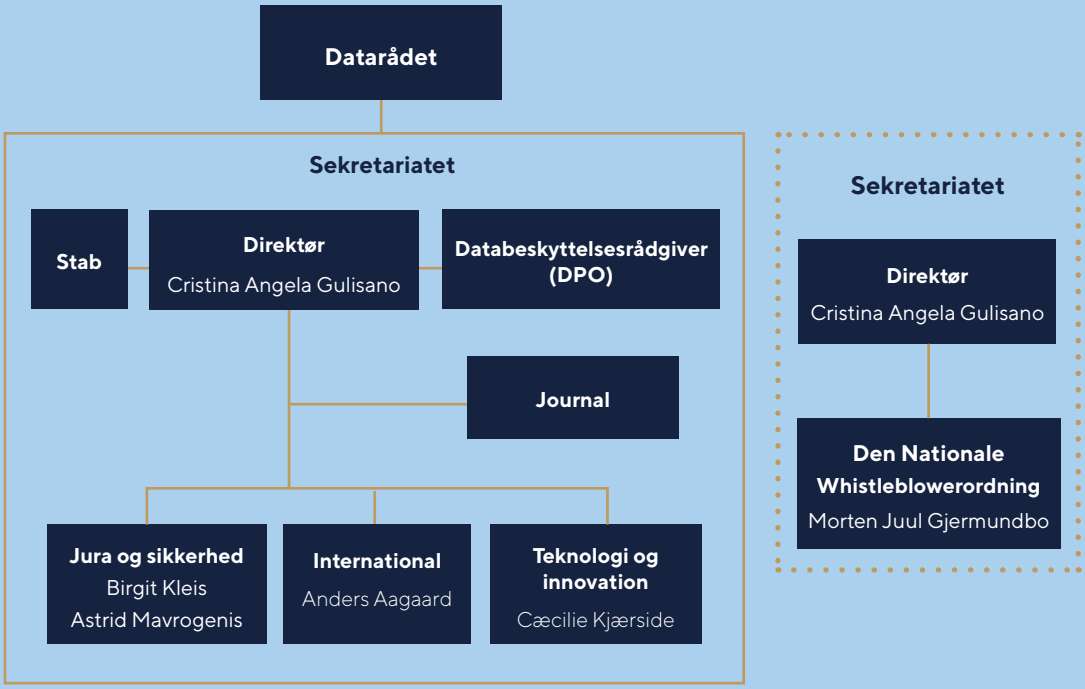
Ordningen har siden skiftet navn til Den Nationale Whistleblowerordning for tydeligere at signalere til omverdenen, at selv om ordningen er etableret i Datatilsynet, så kan den bruges til at indberette om alle forhold omfattet af whistleblowerloven – ikke kun forhold vedrørende databeskyttelse. Den Nationale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

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

## Datatilsynets organisation

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

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




*Datatilsynets organisationsdiagram pr. 31. december 2024*

## 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 2024)

**Formand**
Kristian Korfits Nielsen, højesteretsdommer (udnævnt af justitsministeren)

**Medlemmer**
Henrik Udsen, dr.jur., Københavns Universitet (udnævnt af justitsministeren)
Henning Mortensen, formand for Rådet for Digital Sikkerhed (udnævnt af justitsministeren)
Pia Kirstine Voldmester, advokat og partner, Kromann & Reumert (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)
Stine Mangor Tornmark, CEO & co-founder i Openli (udnævnt af digitaliseringsministeren)

## Sekretariatet

Tilsynets sekretariat består af ca. 74 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 2024, der kan findes på undersiden "Årsberetninger og årsrapporter" på Datatilsynets hjemmeside.

## Sekretariatets medarbejdere (pr. 31. december 2024)*

Direktør, cand.jur. Cristina Angela Gulisano
Kommitteret, cand.jur. Birgit Kleis
Kontorchef, cand.jur. Anders Aagaard
Kontorchef, cand.jur. Astrid Aglaia Mavrogenis
Kontorchef, cand.jur. Morten Juul Gjermundbo
Chefkonsulent, cand.jur. Cæcilie Kjærside
Chefkonsulent, cand.jur. Kenni Elm Olsen
Chefkonsulent, cand.jur. Vibeke Dyssemark Thomsen
Specialkonsulent, cand.jur. Andreas Droob Kristensen
Specialkonsulent, cand.jur. Anna Carolina Jensen
Specialkonsulent, cand.jur. Kasper Folmar
Specialkonsulent, cand.jur. Line Cecilia Koldkjær Sørensen
Specialkonsulent, cand.jur. Lise Fredskov Reinholdt
Specialkonsulent, cand.jur. Mads Nordstrøm Kjær
Specialkonsulent, cand.jur. Marie Louise Buch-Lassen
Specialkonsulent, cand.jur. Pernille Ørum Walther
Specialkonsulent, cand.jur. Sacha Lena Kiming Faltum
Specialkonsulent, cand.jur. Signe Vestergård Spring
Fuldmægtig, cand.jur. Alberte Kylén Pedersen
Fuldmægtig, cand.jur. Ajla Catovic
Fuldmægtig, cand.jur. Anne Elisabeth Tinten
Fuldmægtig, cand.jur. Anne-Sofie Bruunsgaard Secher
Fuldmægtig, cand.jur. Camilla Bormann von Köller
Fuldmægtig, cand.jur. Caroline Magrethe Lindstrøm
Fuldmægtig, cand.jur. Casper Sørensen
Fuldmægtig, cand.jur. Charlotte Svane Guglielmetti
Fuldmægtig, cand.jur. Christine Børrum
Fuldmægtig, cand.jur. Delaram Ostadian-Lam
Fuldmægtig, cand.jur. Frederik Vahlgren
Fuldmægtig, cand.jur. Jane Mindstrup Hagelin
Fuldmægtig, cand.jur. Johan Daugaard Jacobsen

Fuldmægtig, cand.jur. Kamilla Bay Christensen
Fuldmægtig, cand.jur. Kamille Frølund Thomsen
Fuldmægtig, cand.jur. Line Hedmann Jacobsen
Fuldmægtig, cand.jur. Louise Lunddahl Nielsen
Fuldmægtig, cand.jur. Lucas Marott Sundram
Fuldmægtig, cand.jur. Michelle Tronier Didia Balling
Fuldmægtig, cand. merc. jur. Miriem Naima Johansson
Fuldmægtig, cand. merc. jur. Nanna Stig Pedersen
Fuldmægtig, cand. merc. jur. Nicolai Philip van Hauen
Fuldmægtig, cand.jur. Pernille Appel Himmelstrup
Fuldmægtig, cand.jur. Rasha Suhiela Said Eleish (orlov)
Fuldmægtig, cand.jur. Rikke Madsen
Fuldmægtig, cand.jur. Rumaisa Hajaj
Fuldmægtig, cand.jur. Signe Adler-Nissen
Fuldmægtig, cand.jur. Sophie Lynggaard Hansen
Fuldmægtig, cand.jur. Tóra Í Stórustovu
It-sikkerhedsspecialist, cand.jur. Allan Frank
It-sikkerhedskonsulent, cand.merc.dat. Morten Rasmussen
It-sikkerhedskonsulent, politiassistent Poul Erik Høj Weidick
It-sikkerhedskonsulent, diplomingeniør Walther Starup-Jensen
Dataanalytiker, cand.soc. Gry Wad
Dataspecialist, cand.mag. Morten Engberg Helmstedt
Stabskonsulent, cand.soc. Anne Bech
HR-jurist, cand.jur. Mette Odel Spliid
Kommunikationskonsulent, cand.mag. Hisar Sindi
Kommunikationsfuldmægtig, cand.comm. Stine Eimerdal
Vidensformidler, cand.comm. Magnus Frederik Jacobsen
Controller, cand.merc.aud. Yimin Huang Nielsen
Kontorfunktionær Anette Sørensen
Kontorfunktionær Anne-Marie Christina Müller
Kontorfunktionær Camilla Knutsdotter Hallingby
Kontorfunktionær Cathrine Bartels Thing
Kontorfunktionær Mette-Maj Aner Leilund
Kontorfunktionær Pernille Jensen
Informationssikkerhedskoordinator, Nicklas Bøgh Andersen
It-driftskoordinator, Søren Heine Sørensen
It-supporter, Poul Hansen
Stud.inf. Amalie Cia Skau Björnsson
Stud.jur. Anab Abdisalan Isak Ahmed
Stud.jur. Salin Omar
Stud.jur. Simon Odgaard Kanstrup
Stud.scient. Freyr Guðmundsson
Stud.scient.pol. Emily Christine Reiter

** Oversigten viser antallet af medarbejdere og ikke antallet af årsværk. Der kan derfor være visse afvigelser i forhold til den økonomiske årsrapport for 2024.*

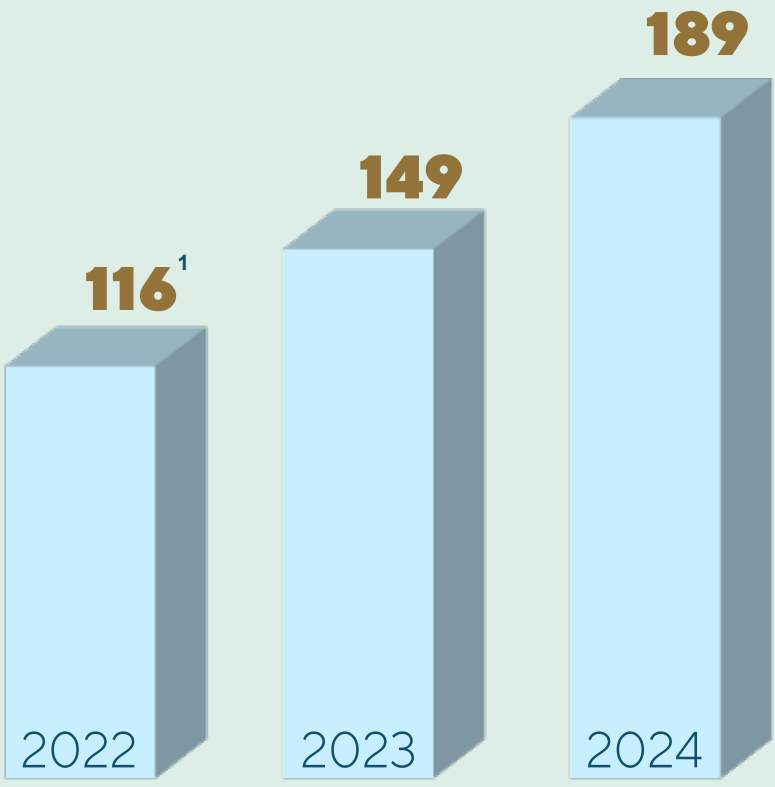
## Den interne whistleblowerordning i Datatilsynet

Den 17. december 2021 blev en intern whistleblowerordning etableret i Datatilsynet. Datatilsynets interne whistleblower ordning 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 ikke modtaget nogle indberetninger.

# Indberetninger til Den Nationale Whistleblowerordning




*Antal modtagne indberetninger*

[1] I forbindelse med rapporteringen fra 2022 besluttede Den Nationale Whistleblowerordning at lave opgørelsen for perioden fra lovens ikrafttræden den 17. december 2021 til og med den 21. december 2022.

Ved udgangen af 2024 var det godt tre år siden, at whistleblowerloven[2] trådte i kraft. Loven indførte en pligt for offentlige myndigheder og en lang række private virksomheder og organisationer til at etablere interne whistleblowerordninger, ligesom der bl.a. blev oprettet en national ekstern whistleblowerordning som supplement til de interne ordninger.

Whistleblowerloven sikrer ikke kun, at der er etableret whistleblowerordninger, som man kan henvende sig til som whistleblower. Loven fastsætter også en række regler for beskyttelse af whistleblowere, bl.a. regler om tavshedspligt om whistleblowernes identitet og regler om beskyttelse af whistleblowere mod uretmæssig afskedigelse eller andre repressalier begrundet i deres indberetning til en whistleblowerordning.

Den Nationale Whistleblowerordning dækker – med få undtagelser – alle typer arbejdspladser i landet, og whistleblowerordningen modtager og behandler indberetninger vedrørende en række overtrædelser af EU-retten, herunder offentligt udbud, produktsikkerhed, miljøbeskyttelse, fødevaresikkerhed m.v. Derudover behandler Den Nationale Whistleblowerordning indberetninger om alvorlige lovovertrædelser eller øvrige alvorlige forhold.

Den Nationale Whistleblowerordning er etableret i Datatilsynet, men fungerer uafhængigt og selvstændigt i forhold til Datatilsynets øvrige virksomhed.

Ved udgangen af 2024 var 6 jurister og et antal journalmedarbejdere tilknyttet whistleblowerordningen. Medarbejderne er alle ansat i Datatilsynet og beskæftiger sig også med databeskyttelsesretlige opgaver, men de pågældende er derudover særligt autoriseret til også at arbejde med indberetninger i Den Nationale Whistleblowerordning, og deres arbejde med indberetningerne foregår adskilt fra Datatilsynets øvrige virksomhed. Medarbejderne er desuden underlagt en særlig tavshedspligt i forhold til deres arbejde med whistleblower-indberetninger.

Selv om Den Nationale Whistleblowerordning er etableret i Datatilsynet, kan ordningen som nævnt anvendes til at indberette om alle forhold omfattet af whistleblowerloven – ikke kun forhold vedrørende databeskyttelse. De indberetninger, som Den Nationale Whistleblowerordning modtog i løbet af 2024, viser da også, at der indberettes om forhold på en række forskellige retsområder. Der henvises til afsnittet ”Om indberetningerne i 2024” nedenfor.

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. På den baggrund gives der på Den Nationale Whistleblowerordnings hjemmeside – og her i Datatilsynets årsberetning – de nævnte oplysninger om Den Nationale Whistleblowerordnings virksomhed for det forgangne år.

På Den Nationale Whistleblowerordnings hjemmeside, www.whistleblower.dk, kan man læse mere om f.eks. ordningens opgaver og om, hvordan man kan komme i kontakt med ordningen.

[2] Lov nr. 1436 af 29. juni 2021 om beskyttelse af whistleblowere. Loven blev vedtaget den 24. juni 2021 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.

## Om indberetningerne i 2024

Den Nationale Whistleblowerordning har i løbet af 2024 håndteret en lang række skriftlige whistleblower-indberetninger, besvaret telefoniske henvendelser om whistleblowerordningen og i enkelte tilfælde afholdt møder med whistleblowere, som ønskede et fysisk møde.

Den Nationale Whistleblowerordning modtog i perioden fra den 1. januar 2024 til den 31. december 2024 i alt 186 indberetninger. Det er 37 flere indberetninger end året før (svarende til en stigning på ca. 25 pct.).

Der er tale om en markant stigning i antallet af indberetninger i forhold til 2023. Stigningen ses primært at udgøres af et højere antal indberetninger om forhold hos offentlige myndigheder. Antallet af indberetninger om offentlige myndigheder steg således fra 46 i 2023 til 73 i 2024.

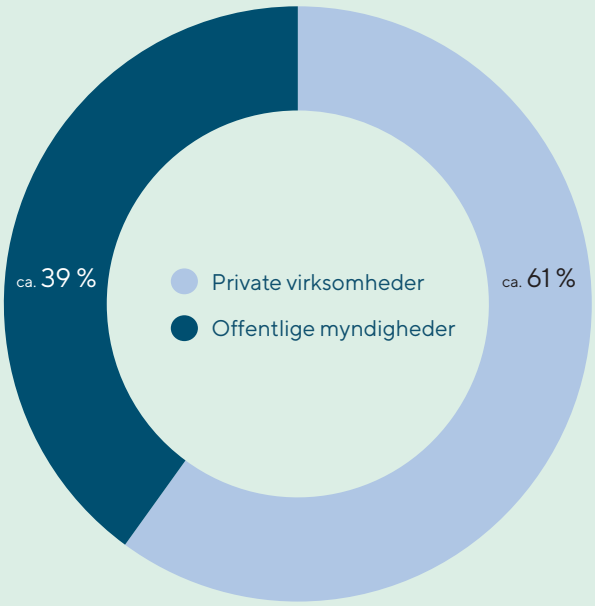
Der er dog stadig flest indberetninger om forhold i private virksomheder. I 2024 blev der således modtaget 113 indberetninger om private virksomheder eller privatpersoner (mod 103 i 2023).

Ca. 61 pct. af indberetningerne, som blev færdigbehandlede i 2024 angik private virksomheder eller privatpersoner. Ca. 39 pct. angik offentlige myndigheder.

Efter at Den Nationale Whistleblowerordning i 2023 havde haft særligt fokus på at gøre opmærksom på ordningens brede anvendelsesområde (idet 66 pct. af de modtagne indberetninger i 2022 vedrørte databeskyttelsesretlige forhold), og efter at ordningen i begyndelsen af 2023 bl.a. skiftede navn til Den Nationale Whistleblowerordning, faldt andelen af indberetninger, som handlede om databeskyttelsesretlige forhold, til 35 pct. i 2023. For 2024 er tallet ca. 23 pct. I absolutte tal er der tale om et fald fra 52 til 43 sager.

Indberetninger, som handlede om databeskyttelse, udgør således stadig en væsentlig del af det samlede antal modtagne indberetninger. Derudover handlede en væsentlig del af indberetninger – som i 2023 – forhold vedrørende arbejdsmiljø eller økonomiske forhold på arbejdspladsen.

Hvad blev der indberettet om?



**Den Nationale Whistleblowerordnings behandling af indberetningerne**

I 2024 færdigbehandlede Den Nationale Whistleblowerordning 186 indberetninger. Ud af disse 186 færdigbehandlede indberetninger var hovedparten (175 indberetninger) modtaget i 2024, og de resterende 11 indberetninger var modtaget i sidste kvartal af 2023.

11 indberetninger, som blev modtaget i 2024, var fortsat under behandling pr. 31. december 2024.

I 2024 fandt Den Nationale Whistleblowerordning i 82 ud af de 186 færdigbehandlede indberetninger grundlag for at videregive oplysninger om et eller fere forhold i indberetningerne til videre foranstaltning hos relevante myndigheder, herunder 3 sager til politiet. Det svarer til 44 pct. af de færdigbehandlede indberetninger i 2024, og det er en stigning i forhold til 2022 og 2023, hvor henholdsvis 26 og 33 pct. af indberetningerne blev videregivet.

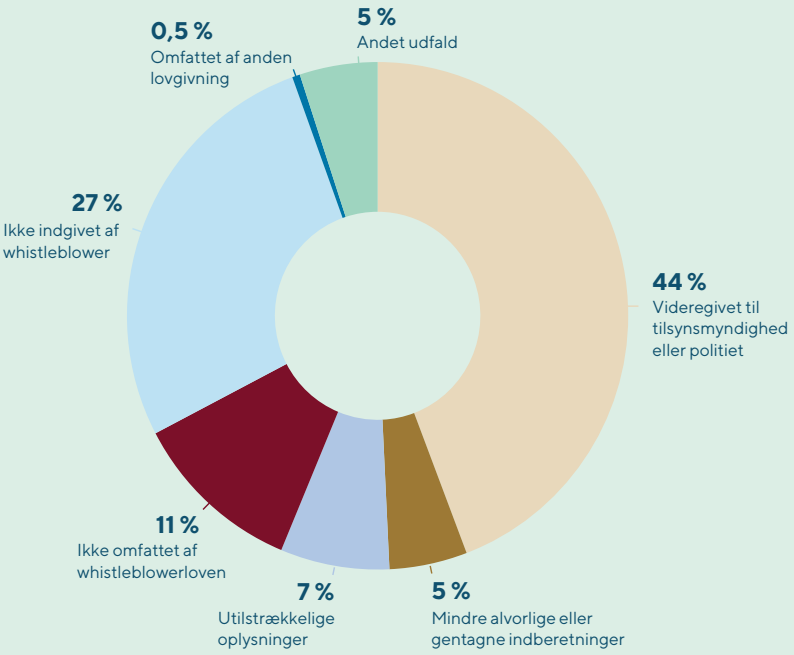
9 indberetninger blev efter endt undersøgelse vurderet til at omhandle forhold, som ikke krævede yderligere opfølgning, jf. whistleblowerlovens § 21.

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

En række sager blev endvidere afvist, fordi indberetningerne faldt uden for whistleblowerlovens anvendelsesområde (21 sager mod 31 i 2023), eller fordi indberetninger var indgivet af personer, som ikke var whistleblowere i lovens forstand (51 tilfælde mod 48 i 2023).

En enkelt indberetning, som blev færdigbehandlet af Den Nationale Whistleblowerordning i 2024, skulle i stedet behandles af en af de særligt oprettede eksterne whistleblowerordninger, jf. whistleblowerlovens § 17. 9 sager blev afsluttet med andet udfald end de ovenfor nævnte kategorier.

Udfald af indberetningerne i procent



### Sagsbehandlingstid

Det fremgår af whistleblowerlovens § 20, stk. 2, nr. 3, at whistleblowerordningens sager skal færdigbehandles inden for en rimelig frist, som ikke overstiger tre måneder fra bekræftelsen af modtagelsen. Tidsrammen på tre måneder kan forlænges til 6 måneder i tilfælde, hvor det er nødvendigt på grund af sagens konkrete omstændigheder, herunder indberetningens art og kompleksitet.

Alle sager, som blev afsluttet i 2024, blev – med undtagelse af én sag – færdigbehandlet inden for fristerne i whistleblowerlovens § 20, stk. 2, nr. 3. I den ene sag blev sagsbehandlingsfristen overskredet med én dag, idet sagen først blev færdigbehandlet tre måneder og én dag efter bekræftelsen.

I en enkelt af de 186 sager, som blev færdigbehandlet i 2024, var der behov for gennemførelse af en længerevarende undersøgelse, og sagsbehandlingstiden nåede i denne sag derfor op på ca. fem måneder. Idet forlængelsen af tre måneders-fristen var nødvendig for sagens behandling, og fordi den blev afsluttet inden 6 måneder, blev denne sag dog også færdigbehandlet i overensstemmelse med whistleblowerlovens frister.

Den gennemsnitlige sagsbehandlingstid for de 186 sager, som blev færdigbehandlet i 2024, var på ca. 30 dage.

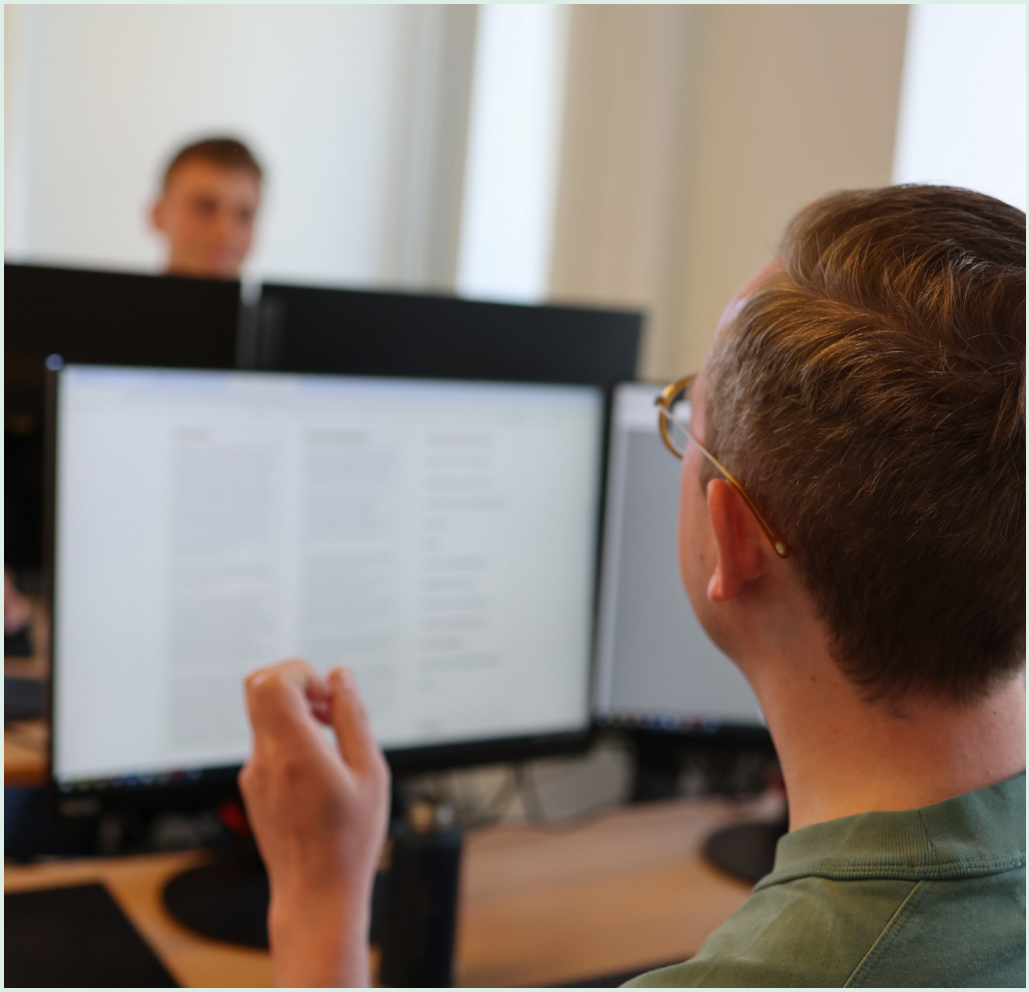
### Evaluering af whistleblowerordningen

Det følger af artikel 14 i whistleblowerdirektivet[3], at en ekstern whistleblowerordning skal gennemgå sine procedurer m.v. regelmæssigt og mindst én gang hvert tredje år.

Bestemmelsen indebærer, at der skal gennemføres en evaluering af den eksterne whistleblowerordning med henblik på at vurdere, om der er behov for tilpasninger, således at det sikres, at ordningen fungerer efter hensigten. Evalueringen skal gennemføres med udgangspunkt i de hidtidige erfaringer med whistleblowerordningen, og proceduren for modtagelse, håndtering og opfølgning af indberetningerne skal i givet fald tilpasses i overensstemmelse hermed.

På den baggrund igangsatte Den Nationale Whistleblowerordning i december måned 2024 – hvor ordningen havde været i kraft i tre år – den nævnte evaluering af ordningens procedurer for modtagelse af indberetninger og opfølgningen herpå.

[3] Europa-Parlamentets og Rådets direktiv 2019/1937/EU af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten



# 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**
- Lovbekendtgørelse nr. 289 af 8. marts 2024 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

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

**Retshåndhævelsesloven**
- Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger med senere ændringer.

**Tv-overvågningsloven**
- Lovbekendtgørelse nr. 182 af 24. februar 2023 om tv-overvågning med senere ændringer.

**Whistleblowerloven**
- Lov nr. 1436 af 29. juni 2021 om beskyttelse af whistleblowere med senere ændringer.

**Relevante bekendtgørelser**
- Bekendtgørelse nr. 1287 af 25. november 2010 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager inden for Den Europæiske Union og Schengensamarbejdet med senere ændringer.
- Bekendtgørelse nr. 1080 af 20. september 2017 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG) med senere ændringer.
- Bekendtgørelse nr. 1078 af 20. september 2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser.
- Bekendtgørelse nr. 1079 af 20. september 2017 om behandling af personoplysninger i Politiets Efterforskningsstøttedatabase (PED).
- Bekendtgørelse nr. 1134 af 13. oktober 2017 om underretning ved udgang og løsladelse mv. samt ved medvirken i tv- eller radioprogrammer eller portrætinterview med senere ændringer.
- 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 om videregivelse af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2, med senere ændringer.
- Bekendtgørelse nr. 1035 af 29. juni 2020 om PNR-enhedens behandling af PNR-oplysninger med senere ændringer.
- Bekendtgørelse nr. 777 af 29. april 2021 om Statens Serum Instituts videregivelse af gensekvenser og isolater fra mikroorganismer og tilknyttede personoplysninger i forbindelse med forebyggelse og bekæmpelse af udbredelsen af smitsomme sygdomme.
- Bekendtgørelse nr. 1860 af 23. september 2021 om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret) med senere ændringer.
- Bekendtgørelse nr. 2449 af 13. december 2021 om krav til eksterne whistleblowerordninger
- Bekendtgørelse nr. 220 af 11. februar 2022 om hel eller delvis opbevaring her i landet af personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning med senere ændringer.
- 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.
- Bekendtgørelse nr. 463 af 4. maj 2023 om logningskrav for retshåndhævende myndigheders automatiske databehandlingssystemer indført før den 6. maj 2016
- Bekendtgørelse nr. 851 af 27. juni 2024 om behandling af personoplysninger i kriminalforsorgens efterretningsdatabase (KrimIntel)

**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).
- Lovforslag nr. 168 af 28. marts 2017 om lov om retshåndhævende myndigheders behandling af personoplysninger (Gennemførelse af direktiv om databeskyttelse på retshåndhævelsesområdet)

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

**Datatilsynets vejledninger mv.**
- Vejledning om dataansvarlige og databehandlere (november 2017)
  - Vejledende principper om dataansvar for vikarer og konsulenter
  - Vejledende tekst om rollefordelingen, når private er leverandører til det offentlige (november 2021)
- Vejledning af om databeskyttelsesrådgivere (december 2017)
- Vejledning om håndtering af brud på persondatasikkerheden (opdateret i juli 2024)
- Vejledning af om konsekvensanalyse (marts 2018)
  - Liste over behandlinger, der altid er underlagt kravet om konsekvensanalyse
- Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger (juni 2018)
- Vejledning om de registreredes rettigheder (juli 2018)
  - 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 om risikovurdering (juni 2019 – under opdatering)
- Vejledning om kreditoplysningsbureauer (oktober 2019)
- Vejledning om videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige (oktober 2019)
- Vejledning om spærrelister (november 2019)
- Vejledning om behandling af personoplysninger om hjemmesidebesøgende (februar 2020)
- Vejledning om fortegnelse (august 2020)
- Vejledning om optagelse af telefonsamtaler (opdateret i april 2024)
- Vejledning om udmåling af bøder til virksomheder (januar 2021 - under opdatering)
- Vejledning om udveksling af personoplysninger med politiet (januar 2021)
- Vejledning om certificeringsordninger (april 2021)
  - Datatilsynets supplerende akkrediteringskrav for certificeringsorganer (marts 2021)
- Vejledning om samtykke (maj 2021)
- Vejledende tekst om kommuners offentliggørelse af personoplysninger i offentligt tilgængelige webarkiver (juli 2021)
- Informationspjece – det skal du vide om databeskyttelse (august 2021)
- Informationspjece om begrebet personoplysninger – få et hurtigt overblik (august 2021)
- Vejledning om tilsyn med databehandlere (oktober 2021)
- Vejledende tjekliste til vuggestuer og børnehaver ved brug af billeder og video (december 2021)
- Vejledning om cloud (marts 2022)
- Vejledning om overførsel af personoplysninger til tredjelande (opdateret i april 2024)

- Vejledning om advarselsregistre (oktober 2022)
- Vejledning om databeskyttelsesreglerne i forbindelse med valgkampagner (oktober 2022)
- Retningslinjer for lokalarkivers behandling af personoplysninger (november 2022)
- Vejledende tjekliste ved skolers brug af billeder og video (januar 2023)
- Vejledning om databeskyttelse i ansættelsesforhold (marts 2023)
- Vejledning om udmåling af bøder til fysiske personer (marts 2023)
- GDPR-univers for små virksomheder, lanceret i maj 2023 af Datatilsynet i samarbejde med Dansk Industri, Dansk Erhverv og SMV Danmark
- Vejledning om direkte markedsføring (juni 2023)
- Vejledning om adfærdskodekser (juni 2023)
  - Akkrediteringskrav for kontrolorganer til adfærdskodekser (november 2020)
- Vejledning om tv-overvågning – private virksomheder (juni 2023)
- Vejledning om rollefordeling i forskningsprojekter (juli 2023)
- Vejledende tekst om auto-complete af e-mailadresser (august 2023)
- Vejledning om offentlige myndigheders brug af kunstig intelligens – Inden I går i gang (oktober 2023)
- Vejledning om tv-overvågning – offentlige myndigheder (november 2023)
- Vejledning om tv-overvågning – boligorganisationer (december 2023)
- Vejledning om adgangsrettigheder (december 2023)
- Vejledende tekster i katalog over sikkerhedsforanstaltninger (november 2023 og frem)
- Vejledende tekst om de 10 typiske brud på persondatasikkerheden (januar 2024)
- De nordiske tilsynsmyndigheders fælles principper om børn og online spil (maj 2024)
- Vejledende tekst om kravene til underretning af registrerede ved brud på persondatasikkerheden (maj 2024)
- GDPR-univers for små foreninger, lanceret i juni 2024 af Datatilsynet i samarbejde med ABF, DGI og Fonden for Socialt Ansvar

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.
- Vejledning nr. 9248 af 16. december 2021 for whistleblowere
- Vejledning nr. 9249 af 16. december 2021 for whistleblowerordninger på offentlige arbejdspladser
- Vejledning nr. 9250 af 16. december 2021 for whistleblowerordninger på private arbejdspladser

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 tjene- ster (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 forordningen (Vejledning 9/2020)
- Restriktioner i henhold til artikel 23 i GDPR (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)
- Gyldigt samtykke i forbindelse med "Consent or Pay"-løsninger implementeret af store onlineplatforme (Udtalelse 08/2024)
- Anvendelse af ansigtsgenkendelse til at strømline passagerstrømmen i lufthavne (forenelighed med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR) (Udtalelse 11/2024)
- Den dataansvarliges forpligtelser ved brug af databehandlere (Udtalelse 22/2024)
- Behandling af personoplysninger baseret på artikel 6, stk. 1, litra f (Vejledning 1/2024)
- Behandling af personoplysninger i forbindelse med udvikling og anvendelse af AI-modeller (Udtalelse 28/2024)

De nævnte vejledninger mv. er offentliggjort på EDPB's hjemmeside og kan tilgås via Datatilsynets hjemmeside, hvor der løbende offentliggøres nye vejledninger mv.

**Årsberetning**
© 2024 Datatilsynet

Eftertryk med kildeangivelse er tilladt

**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 Danmark

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

DATATILSYNET

# Ansvarlig anvendelse af borgernes data i et digitaliseret samfund

**Datatilsynet**
Carl Jacobsens Vej 35
2500 Valby