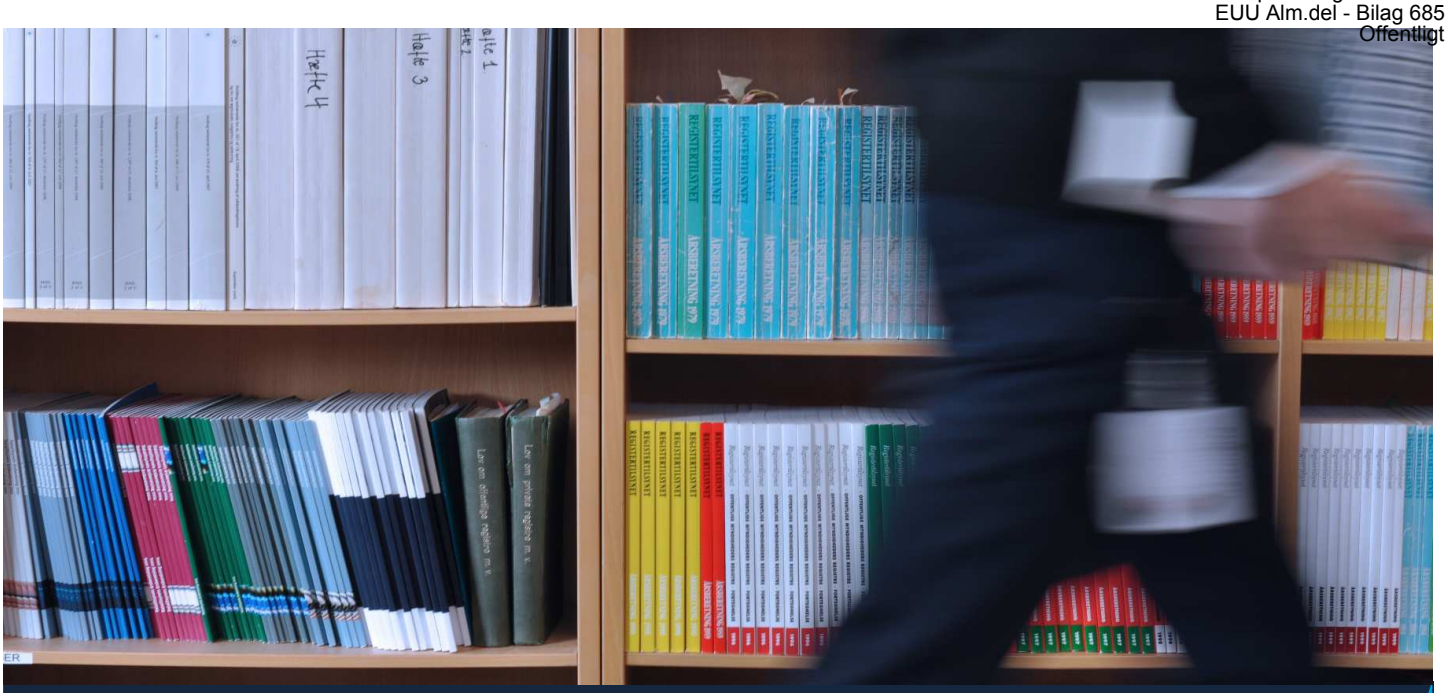

Bidrag fra Datatilsynet

Erfaringsindsamling i forbindelse med Justitsministeriets nationale evaluering af databeskyttelsesreglerne

April 2021

DATATILSYNET

Indhold

1. Hørte myndigheder, organisationer mv.

Justitsministeren har i februar 2020 iværksat en national evaluering af databeskyttelsesreglerne. Evalueringen indebærer bl.a. en erfaringsindsamling, i hvilken forbindelse der har været gennemført en høring af relevante interessenter og en offentlig høring, således at enhver har haft mulighed for at bidrage til erfaringsindsamlingen, herunder belyse konkrete situationer, hvor der opleves uklarhed, når databeskyttelsesreglerne skal efterleves i praksis, og formidle mulige løsninger og eventuel vejledning om konkrete problemstillinger.

Justitsministeriet har modtaget høringssvar fra:

3F, Akademikerne, Danmarks DPO-forening, Danmarks Idrætsforbund, Dansk Arbejdsgiverforening, Dansk Erhverv og IT-Branchen (fælles), Dansk Industri, Dansk Ungdoms Fællesråd (DUF), Danske Advokater, Danske Arkiver, Danske Handicaporganisationer, Danske Medier, Danske Regioner, Danske Universiteter, DGI, EjendomDanmark, Erhvervslivets EU- og Regelforum, Fagbevægelsens Hovedorganisation, Finans Danmark, Finans og Leasing, FOA, Folkeoplysningens Brancheorganisation, Forbrugerrådet Tænk, Danske Revisorer, HK, KL, Kræftens Bekæmpelse, MyData Denmark, Henrik Stougaard, PriWay, PROSA, Rigsarkivet, Rigspolitiet, Rådet for Digital Sikkerhed, Sikkerhedsbranchen, SMVdanmark.

Nedenfor er gengivet de mest centrale spørgsmål og udfordringer, som er kommet frem i forbindelse med erfaringsindsamlingen. Datatilsynets bemærkninger hertil er anført med *kursiv*.

2. Behov for mere (konkret) vejledning

Akademikerne, Dansk Arbejdsgiverforening, Dansk Erhverv og IT-branchen, Dansk Industri, DUF, Danske Handicaporganisationer, Danske Medier, Danske Regioner, EjendomDanmark, Erhvervslivets EU- og Regelforum, Finans Danmark, Forbrugerrådet Tænk, KL, Kræftens Bekæmpelse, Rådet for Digital Sikkerhed, Sikkerhedsbranchen og **SMVdanmark** anfører, at der er behov for mere konkret og branchespecifik vejledning med praksisnære eksempler om databeskyttelsesreglerne. Der peges i den forbindelse også på, at relevante parter i højere grad bør inddrages, ligesom Datatilsynet bør offentliggøre flere og mere operationelle afgørelser samt udarbejde flere konkrete værktøjer, herunder tjeklister, skabeloner, flowcharts, FAQ'er, videoer mv.

Der har siden 1970'erne været regler for behandling af personoplysninger i Danmark. I 1979 blev adgangen til at registrere og videregive oplysninger om personer, virksomheder, foreninger mv. således fastlagt i lov om offentlige myndigheders registre og lov om private registre.

Formålet med disse regler, som var nogle af de første af sin slags på verdensplan, var at sikre, at behandling af personoplysninger skete på en sådan måde, at den enkelte borgers retsbeskyttelse og integritet ikke blev krænket, idet den stigende anvendelse af elektronisk databehandling i Danmark skabte en frygt i befolkningen for registreringsaktiviteterne og for, at de indsamlede oplysninger blev udnyttet på en måde, der krænkede den personlige fred og frihed.

I 1990 fremsatte EF-Kommissionen et forslag til Rådets direktiv om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, som blev endeligt vedtaget den 24. juli 1995. Formålet var at harmonisere beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandlingsaktiviteter og at sikre den frie udveksling af personoplysninger mellem medlemsstaterne. Direktivet blev gennemført i dansk ret ved lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven), som trådte i kraft den 1. juli 2000.

Den hastige teknologiske udvikling og globaliseringen har imidlertid skabt nye udfordringer, hvad angår beskyttelsen af personoplysninger. Omfanget af indsamlingen og delingen af personoplysninger er steget betydeligt. Teknologien har givet både private virksomheder og offentlige myndigheder mv. mulighed for at udnytte personoplysninger i et hidtil uset omfang, når de udøver deres aktiviteter. Endvidere deler fysiske personer i stigende grad deres personoplysninger offentligt og globalt.

Denne udvikling fandt EU's medlemslande krævede en stærk og mere sammenhængende databeskyttelsesramme, som understøttes af effektiv håndhævelse, fordi det er vigtigt at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked. Dette var baggrunden for, at databeskyttelsesforordningen den 27. april 2016 blev vedtaget, og siden 25. maj 2018 erstattede reglerne i persondataloven (med senere ændringer), der som nævnt havde været gældende siden år 2000.

Samme tanker er i øvrigt også kommet til udtryk i den fællesoffentlige digitaliseringsstrategi 2016-2020, som er blevet til i et samarbejde mellem den tidligere regering, KL og Danske Regioner. Det fremgår således bl.a. af strategien, at: "Velfærdssamfundet bygger på en høj grad af tillid til den offentlige sektor. Den tillid skal vi værne om, også når den offentlige kommuni-

kation og service bliver mere og mere digital. Det er derfor helt afgørende, at der skabes trygge rammer for, at borgere og virksomheder kan agere digitalt i samspillet med den offentlige sektor. Borgernes og virksomhedernes digitale tryghed er en central forudsætning for, at vi i fællesskab kan udnytte de muligheder, digitalisering giver os for at udvikle og forbedre vores velfærdssamfund. For digitalisering rummer store muligheder såvel for den enkelte som for samfundet som helhed."

Endvidere har Børsen den 24. maj 2018 bragt et debatindlæg skrevet af Dansk Industris tidligere administrerede direktør, Karsten Dybvad, under overskriften: "Tillid til virksomhedernes datahåndtering er hård valuta". Af debatindlægget fremgår det bl.a., at stort set alle virksomheder arbejder i dag med data – og med rette. Men det kan ifølge debatindlægget kun lade sig gøre, hvis kunderne har tillid til, at deres data bliver brugt forsvarligt og ikke bliver misbrugt. Her har Danmark og danske virksomheder et fantastisk udgangspunkt for at gøre digitalisering og datasikkerhed til en styrkeposition, på samme vis som eksempelvis høj fødevaresikkerhed er det i dag. Dermed kan persondataforordningen ifølge debatindlægget faktisk også blive den håndsrækning til danske virksomheder, der gør os mere konkurrencedygtige. Debatindlægget slutter af med at slå fast, at i en tid, hvor data ofte bliver beskrevet som det nye olie, kan den tillid blive en uvurderlig konkurrenceparameter for danske virksomheder.

****

Selv om det ikke nævnes direkte i de indkomne erfaringer fra de hørte myndigheder, organisationer mv., synes det efter Datatilsynets opfattelse i øvrigt i et vist omfang at være et gennemgående tema i mange af disse erfaringer, at det er en svaghed ved databeskyttelsesreglerne, at reglerne i vidt omfang består af retlige standarder, som forudsætter, at den dataansvarlige foretager en konkret vurdering, hvilket skaber bekymring for, om man som dataansvarlig gør det rigtigt.

Formålet med at udforme reglerne som retlige standarder, som forudsætter den dataansvarliges konkrete stillingtagen, er ikke at skabe usikkerhed eller bekymring, men at sikre, at reglerne har den fornødne fleksibilitet. Det er således hensigten med databeskyttelsesreglerne, at de skal kunne tilpasses den enkelte behandlingssituation og den enkelte dataansvarlige.

Det er derimod ikke hensigten med reglerne, ligesom det formentlig heller ikke er i de dataansvarliges interesse, at Datatilsynet udtømmende gør op med, om og hvordan personoplysninger skal behandles. Dette skyldes, at tilsynet i sagens natur ikke har de samme forudsætninger som de dataansvarlige, der til daglig har behov for at behandle personoplysninger, for at vurdere, hvad der i det enkelte tilfælde "er det rigtige at gøre". Datatilsynet har f.eks. ikke indgående kendskab til, hvilke og hvor mange personoplysninger der skal behandles for at drive en virksomhed eller en daginstitution.

Når man som dataansvarlig i henhold til reglerne selv forventes at foretage de nødvendige vurderinger i forhold til, hvordan man tilrettelægger sin behandling af personoplysninger, betyder dette naturligvis også, at i det omfang disse vurderinger bygger på relevante og saglige overvejelser, vil behandlingen som regel være inden for rammerne af databeskyttelsesreglerne. Samtidig er det vigtigt at være opmærksom på, at tiden efter 25. maj 2018 har vist, at man som dataansvarlig ikke skal være nervøs for, at det første, Datatilsynet altid tyr til, er en bøde, hvis tilsynet – på trods af den dataansvarliges relevante og saglige overvejelser – undtagelsesvis måtte komme frem til en anden vurdering i et konkret tilfælde.

Datatilsynet har ifølge databeskyttelsesforordningen en række reaktionsmuligheder, når tilsynet konstaterer, at reglerne ikke overholdes. Overtrædelse af databeskyttelsesreglerne kan ef-

ter omstændighederne således sanktioneres ved bl.a. at udtale kritik og/eller meddele den dataansvarlige påbud eller forbud i forhold til en given handling eller undladelse. Efter omstændighederne kan det også komme på tale at sanktionere overtrædelsen med en bøde. De forskellige sanktioner kan enten anvendes alene eller kombineres afhængigt af de konkrete omstændigheder. Datatilsynet foretager altid en konkret vurdering baseret på den enkelte sags omstændigheder, når tilsynet beslutter, hvilken sanktion eller reaktion den enkelte sag skal ende med. Datatilsynet lægger i den forbindelse bl.a. vægt på karakteren, herunder omfanget, af overtrædelsen, om overtrædelsen må anses som udtryk for manglende vilje til at overholde reglerne, lemfældig omgang med personoplysninger eller der fx er tale om gentagelsestilfælde. Det er langt fra alle sager, som Datatilsynet behandler, som resulterer i en politianmeldelse med indstilling om bøde. Således afgør Datatilsynet i dag en meget stor andel af tilsynets sager ved anvendelse af andre sanktioner end bøde.

****

Datatilsynet har i de senere år brugt og bruger fortsat betydelige ressourcer på at rådgive og vejlede om de nye databeskyttelsesregler. Alligevel har de aktører, som har en interesse i Datatilsynets arbejde, oplevet, at tilsynets vejledning ikke har været tilstrækkelig konkret eller tilstrækkelig anvendelig i praksis.

Datatilsynet har derfor foretaget en række organisatoriske tiltag for at styrke tilsynets vejledningsindsats yderligere, idet fokus på mere konkret og anvendelig vejledning nu er en del af tilsynets strategiske grundlag, hvilket gerne skulle bidrage til at sikre, at tilsynets vejledning også opleves sådan i praksis. Et af disse initiativer er, at Datatilsynet har oprettet en ny enhed – Vejledning og Informationssikkerhed – som bl.a. skal have et særligt fokus på at give mere konkret vejledning til virksomheder, myndigheder og borgere, herunder ved udarbejdelse af vejledninger, skabeloner, tjeklister mv.

I forlængelse heraf har Datatilsynet nedsat to forskellige kontaktudvalg, som har til formål at skabe et tættere samspil mellem tilsynet og centrale interessenter i såvel den private som den offentlige sektor, for at tilsynet kan være tæt på de problemer, som virksomheder og myndighederne står med, således at tilsynet bedre kan hjælpe dem til at overholde reglerne, hvilket i sidste ende også er til gavn for alle de borgere, hvis oplysninger det hele drejer sig om.

Datatilsynet arbejder endvidere på at få offentliggjort så mange afgørelser som muligt på tilsynets hjemmeside. Afgørelserne vil blive offentliggjort med et lille resume, hvor tilsynet dels "oversætter" afgørelsen for offentligheden og dels angiver, hvad den dataansvarlige burde have gjort eller har gjort godt. Datatilsynet er således også opmærksom på at få fremhævet de dataansvarlige, som gør det godt og har udviklet nogle gode løsninger mv.

Herudover arbejder Datatilsynet målrettet på at stille de samme budskaber til rådighed i flere forskellige formater, f.eks. vejledninger, korte tekster, små animerede videoer og podcasts, ligesom tilsynet i disse år har stor opmærksomhed på, hvordan tilsynet formulerer sig, og hvor øvelsen som på så mange andre områder består i at finde den rette balance, så formidlingen ikke kun er korrekt, men også til at forstå. Dette har bl.a. betydet, at Datatilsynet har valgt at ansætte flere kommunikationsmedarbejdere.

Er Datatilsynet så i mål? Langt fra. Men Datatilsynet arbejder målrettet videre på at gøre det bedre med de ressourcer, som tilsynet har til rådighed.

3. Begreberne dataansvarlig og databehandler

3.1 Afklaring af roller

3F, Dansk Erhverv og IT-branchen, Dansk Industri, Danske Medier, Danske Regioner, EjendomDanmark, KL og **Sikkerhedsbranchen** anfører, at det i praksis er vanskeligt at placere og afgrænse dataansvaret, herunder i forhold til leverandører, samarbejdspartnere, tillidsrepræsentanter mv.

Når der behandles personoplysninger, er det vigtigt at være opmærksom på rollefordelingen. Det gælder i særdeleshed, hvis der er flere parter involverede i behandlingen. Hvis de parter, der deltager i en behandling af personoplysninger, er usikre på, hvem der har ansvaret for at leve op til de forskellige regler om databeskyttelse, er der en risiko for, at ingen af parterne påtager sig ansvaret, eller at en part påtager sig et ansvar, som den pågældende reelt ikke har.

De indkomne høringssvar viser, at det i praksis ikke altid er lige let at afklare rollefordelingen, og at der er behov for yderligere – praksisnær – vejledning på området. Datatilsynet vil derfor tage initiativ til, at det vejledende materiale om dataansvarlige og databehandlere, som pt. er tilgængelig på Datatilsynets hjemmeside, løbende opdateres og udbygges med praksisnære eksempler. En opdateret vejledning med spørgsmålet om offentlige myndigheders anvendelse af private leverandører forventes offentliggjort inden længe.

Datatilsynet har også i regi af Det Europæiske Databeskyttelsesråd (EDPB) bidraget til udarbejdelsen af en fælleseuropæisk vejledning om databeskyttelsesforordningens begreber dataansvarlige og databehandlere (vejledning 07/2020). Vejledningen har været sendt i offentlig høring og forventes snart vedtaget med de ændringer, som de indkomne høringssvar måtte give anledning til. Når den endelige vejledning foreligger, vil Datatilsynets nationale vejledning blive opdateret i overensstemmelse hermed.

For så vidt angår bemærkningen fra 3F om, at det i praksis giver udfordringer at afgøre, hvorvidt dataansvaret skal placeres hos enten den faglige organisation eller tillidsrepræsentanten, fremgår det af Datatilsynets reviderede vejledning fra december 2020 om databeskyttelse i forbindelse med ansættelsesforhold, at det beror på en konkret vurdering af rollefordelingen og de aftaler mv., der måtte ligge til grund herfor på det pågældende område. Hvis den faglige organisation har indrettet sig på en sådan måde, at organisationen har instruktionsbeføjelser over for tillidsrepræsentanten i form af mandat, bemyndigelse, vejledning eller lign., vil der som udgangspunkt foreligge dataansvar for de faglige organisationer, hvorimod tillidsrepræsentanten som udgangspunkt vil være at betragte som selvstændigt dataansvarlig, hvis organisationen ikke har en sådan instruktionsbeføjelse over for tillidsrepræsentanten.

Datatilsynets vejledning om databeskyttelse i forbindelse med ansættelsesforhold, der blev udgivet første gang i november 2018, sætter fokus på de regler inden for databeskyttelsesretten, der især kommer i spil i forbindelse med ansættelsesforhold, herunder en række afsnit om dataansvaret i en ansættelsesretlig sammenhæng og de faglige organisationers og tillidsrepræsentanters behandling af personoplysninger. Vejledningen, som senest er revideret i december 2020, er bl.a. blevet til på baggrund af drøftelser med repræsentanter for arbejdsmarkedets parter. Datatilsynet forventer i øvrigt bl.a. på baggrund af nærværende nationale eva-

luering af databeskyttelsesreglerne at påbegynde en yderligere gennemgang og revision af vejledningen inden udgangen af 2021.

3.2 Tilsyn med databehandlere

Akademikerne, Danmarks DPO-Forening, Dansk Erhverv og IT-branchen, Danske Regioner, DUF, Finans Danmark, KL og **Sikkerhedsbranchen** giver udtryk for, at det er en udfordring at føre tilsyn med – og påse behandlingssikkerheden hos – databehandlere, herunder at det er uklart, hvad der reelt er genstanden for tilsynet med databehandlere. Det er ifølge de nævnte organisationer mv. ressourcekrævende, og det vil være forenklende med en tjekliste eller andre værktøjer. Herudover er det svært at føre tilsyn med, hvad de nævnte organisationer betegner som "techgiganter", og ikke alle it-leverandører er forberedt på, hvad den dataansvarliges kontrol indebærer.

For så vidt angår udfordringerne i forhold til at få påset behandlingssikkerheden hos databehandlere udarbejdede Datatilsynet i maj 2018 en vejledende tekst om tilsyn med databehandlere og underdatabehandlere, hvori der redegøres for, hvorfor det er nødvendigt at påse behandlingssikkerheden hos databehandlere, ligesom der redegøres for, hvem der kan påse behandlingssikkerheden, hvordan behandlingssikkerheden kan påses og hvor ofte behandlingssikkerheden bør påses.

Endvidere lancerede Datatilsynet og FSR - danske revisorer sammen i februar 2019 en revisorerklæring, som skal hjælpe dataansvarlige med at påse, at deres databehandlere lever op til kravene i GDPR. I november 2020 blev erklæringen fulgt op af en ny udgave med en begrænset grad af sikkerhed, når der f.eks. er mindre kompleksitet i behandlingen af personoplysninger. Formålet med den nye erklæring var at bidrage til at sikre, at brugen af revisorerklæringer står mål med behovet i den konkrete situation. Det er ikke nødvendigt at benytte revisorerklæringer for at efterleve databeskyttelsesforordningen, men kan være en god måde at sikre, at de relevante områder bliver belyst, og at man får foretaget en uvildig kontrol af sikkerhedsniveauet. Begge revisorerklæringer er tilgængelige på FSR – danske revisorers og Datatilsynets hjemmesider.

De indkomne høringssvar viser imidlertid, at der, som det er tilfældet i forhold til afklaringen af rollefordelingen, er behov for yderligere vejledning på området, herunder ved inddragelsen af praksisnære eksempler, tjeklister mv. Datatilsynet forventer derfor i 2. kvartal 2021 at opdatere og supplere tilsynets vejledende materiale om tilsyn med databehandlere og underdatabehandlere.

3.3 Aftaler om fælles dataansvar og databehandleraftaler

DUF, Danske Medier, Finans Danmark og **KL** oplyser, at det er vanskeligt at indgå et retvisende aftalegrundlag (databehandleraftaler eller aftale om fælles dataansvar) med techgiganter, herunder Facebook, Google og Microsoft, da disse opererer med standardvilkår og er afvisende over for dialog eller forhandling.

Finans Danmark finder endvidere, at databeskyttelsesforordningens artikel 28, stk. 4, ikke tager højde for, at de aktiviteter, som underdatabehandleren udfører på vegne af databehandleren, kan divergere væsentligt fra den samlede aktivitet, der er outsourcet til databehandleren – både for så vidt angår selve behandlingsaktiviteterne, kategorierne af personoplysninger og dermed det samlede risikobillede. **Finans Danmark** ønsker derfor oplyst, om en praktisk løsning kan være, at databehandleren foretager en selvstændig risikovurdering af underdatabehandlerens aktiviteter med henblik på fastsættelse af tekniske og organisatoriske sik-

kerhedsforanstaltninger, hvorefter denne risikovurdering og beskrivelse af sikkerhedsforanstaltningerne forelægges den dataansvarlige til godkendelse.

FSR – danske revisorer bemærker, at det er den dataansvarliges forpligtelse at sikre, at der er en databehandleraftale på plads. Dataansvarlige har ofte tolket dette således, at den dataansvarlige også skal udarbejde krav til bl.a. tekniske og organisatoriske foranstaltninger. Dette giver udfordringer for mange – særligt mindre databehandlere – da de bliver mødt med mange forskelligartede databehandleraftaler med forskellige krav til blandt andet tekniske og organisatoriske foranstaltninger.

Det følger af databeskyttelsesforordningens artikel 28, stk. 3, at en databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og som fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. Endvidere følger det af forordningens artikel 26, at fælles dataansvarlige skal fastlægge deres respektive ansvar for overholdelse af forpligtelserne i forordningen.

Der er imidlertid efter Datatilsynets opfattelse ikke noget til hinder for, at det er databehandleren, som tager initiativ til udarbejdelsen af databehandleraftalen, eller i øvrigt fastlægger indholdet heraf. Dette vil særligt være relevant, hvor den ydelse, som databehandleren leverer, kan karakteriseres som en standardydelse, hvor det ikke vil være muligt individuelt at "forhandle" spørgsmålet om f.eks. tekniske og organisatoriske foranstaltninger. Den dataansvarlige må i disse tilfælde vurdere, om den tilbudte aftale, de beskrevne foranstaltninger og forholdene, behandlingerne sker under, indebærer, at forordningen overholdes, jf. forordningens artikel 28, stk. 1. Det samme gælder i forhold til den ordning, som skal fastlægges i henhold til forordningens artikel 26.

De egentlige vilkår må således baseres på markedet, men Datatilsynet forventer, at de ydelser, der tilbydes, også bliver tilbudt på en måde og under kontrakter, der sætter alle aktører – både (fælles) dataansvarlige og databehandlere – i stand til at overholde forordningen.

I forhold til det af Finans Danmark forespurgte er det den dataansvarliges opgave at vurdere hele behandlingskæden, inden behandlinger overlades til en databehandler, der benytter underdatabehandlere, jf. artikel 28, stk. 1. For at foretage denne vurdering kan den dataansvarlige rent praktisk godt benytte vurderinger foretaget af andre – også en databehandlers beskrivelse af overholdelsen af de databeskyttelsesforpligtelser, som underdatabehandleren foretager som led i de behandlinger, der hidrører fra den dataansvarlige.

Der kan dog aldrig foretages behandlinger, hverken med hensyn til type, formål og midler, der ikke til fulde er omfattet af – og tilgodeser – de databeskyttelsesretlige forpligtelser, der er fastsat i kontrakten mv. mellem den oprindelige databehandler og den dataansvarlige. Dette gælder, uanset hvor mange underdatabehandlere der benyttes. Hvis de behandlinger, hvortil der bruges en underdatabehandler, alene tilsiger anvendelse af en del af de samlede forhold, der udgør databeskyttelsesforpligtelsen i den oprindelige kontrakt mv., kan dette afspejles i aftalen med denne.

Databeskyttelsesforordningens artikel 28, stk. 4, har til formål at sikre, at der ikke ved kæder af databehandlere sker en udvanding af de oprindelige krav, den dataansvarlige har indføjet i kontrakten mv., over for den oprindelige databehandler, ligesom bestemmelsen holder den oprindelige databehandler ansvarlig for eventuel manglede overholdelse i de efterfølgende led

i forholdet til den dataansvarlige. Det er væsentligt at erindre, at det er den dataansvarlige, der ultimativt står til ansvar for overholdelsen af forordningen i forhold til varetagelsen af de registreredes rettigheder, uanset om der benyttes ingen, en eller flere databehandlere.

4. Overførsel til lande uden for EØS (såkaldte tredjelande)

Dansk Erhverv og IT Branchen, DUF, Danske Medier, Danske Regioner, Dansk Industri, DGI, Finans Danmark, FSR – danske revisorer, KL og **Kræftens Bekæmpelse** oplyser, at der er usikkerhed og udfordringer forbundet med overførsel af oplysninger til tredjelande efter Schrems II-afgørelsen, herunder ved anvendelsen af cloud. Det fremhæves i den forbindelse særligt, at dataansvarlige ikke har den nødvendige viden eller kapital til at vurdere forholdene i tredjelandet eller til at fastsætte eventuelle yderligere foranstaltninger, som kan sikre et tilstrækkeligt beskyttelsesniveau, og at der bør arbejdes på en fælles europæisk løsning.

Akademikerne oplyser, at der er udfordringer ved udveksling af personoplysninger med Grønland i forhold til bl.a. fagforeningsaktiviteter, og organisationen efterlyser yderligere vejledning i den forbindelse.

Schrems II-afgørelsen giver anledning til en række overvejelser i forhold til den fremtidige overførsel af personoplysninger til lande uden for EØS, såkaldte tredjelande, og Datatilsynet er enig i behovet for praktisk vejledning i den henseende.

På den baggrund har Datatilsynet – i regi af Det Europæiske Databeskyttelsesråd (EDPB) – udarbejdet anbefalinger om, (1) hvilke kriterier man som dataeksportør skal lægge vægt på ved vurderingen af beskyttelsesniveauet i et tredjeland, og (2) hvilke supplerende foranstaltninger man som dataeksportør kan iværksætte, hvis beskyttelsesniveauet i et tredjeland vurderes utilstrækkeligt. Anbefalingerne indeholder en række eksempler vedrørende praktisk forekommende overførselssituationer, herunder anvendelse af cloud-baserede løsninger. Begge disse anbefalinger har til formål at give praktisk vejledning til dataeksportører i lyset af Schrems II-afgørelsen.

Datatilsynet er endvidere i gang med at opdatere Datatilsynets egen nationale vejledning om overførsel til tredjelande efter Schrems II-afgørelsen. Datatilsynet har som led i arbejdet hermed afholdt et møde med relevante aktører med henblik på, at den opdaterede vejledning kan adressere de udfordringer, man som dataeksportør oplever i praksis. Vejledningen vil også komme til at indeholde en række praktiske eksempler, herunder om anvendelse af cloud-baserede løsninger, ligesom den vil adressere spørgsmålet om overførsel til Grønland. Vejledningen forventes offentliggjort i juli 2021. Datatilsynet vil i øvrigt løbende overveje, om der er behov for yderligere vejledning på området.

I forhold til opfordringen om, at der nationalt eller i EU-regi foretages en generel vurdering af forholdene i relevante tredjelande, kan Datatilsynet oplyse, at man som dataeksportør er ansvarlig for at sikre sig, at man overholder reglerne i databeskyttelsesforordningen, når man overfører personoplysninger til et tredjeland. Det er derfor dataeksportøren, som selv skal sikre sig, at beskyttelsesniveauet i tredjelandet er tilstrækkeligt, hvilket også er bekræftet af EU-Domstolen i Schrems II-afgørelsen.

Ved vurderingen af beskyttelsesniveauet i tredjelandet vil det være naturligt for dataeksportøren at involvere dataimportøren, men også f.eks. brancheorganisationer vil kunne spille en vigtig rolle i den forbindelse. Datatilsynet er opmærksom på, at det kan være en vanskelig vurdering at foretage i praksis, og det er også bagrunden for, at EDPB har udarbejdet anbefalinger herom.

Det bemærkes i øvrigt, at ifølge databeskyttelsesforordningens artikel 45 er det EU-Kommissionen, der kan fastslå, at et tredjeland, et område i et tredjeland, en sektor i et tredjeland eller en internationale organisation beliggende i et tredjeland er sikkert, og dermed har et beskyttelsesniveau, som i det væsentlige svarer til det beskyttelsesniveau, der gælder i EU. Ved sin vurdering foretager EU-Kommissionen bl.a. en analyse af de regler, der gælder for behandling af personoplysninger i tredjelandet eller den internationale organisation, men også en analyse af, hvordan landet eller organisationen efterlever retsstatsprincippet, regler for klageadgang og domstolsprøvelse osv. EU-Kommissionen er i den forbindelse endvidere forpligtet til at indhente en udtalelse fra Det Europæiske Databeskyttelsesråd om, hvorvidt rådet er enig i analysen mv.

Når EU-Kommissionen har truffet afgørelse om, at et tredjeland eller en organisation er sikkert betyder det, at der kan overføres personoplysninger til en modtager i det pågældende land eller i den pågældende organisation, uden at der først skal søges om godkendelse fra en kompetent tilsynsmyndighed eller lignende – dog under forudsætning af, at forordningens øvrige regler, herunder behandlingsreglerne i forordningens kapitel II overholdes.

5. Anmeldelse af brud på persondatasikkerheden

Dansk Erhverv og IT-branchen, Danske Regioner, EjendomDanmark, Finans Danmark og **KL** anfører, at det er uklart, hvornår et brud på persondatasikkerheden er omfattet af pligten til at anmelde til Datatilsynet efter databeskyttelsesforordningens artikel 33, herunder at tilsynets vejledning om brud på persondatasikkerheden bør revideres og gerne angive flere eksempler på, hvornår brud ikke skal anmeldes til tilsynet.

Akademikerne, EjendomDanmark, Fagbevægelsens Hovedorganisation og **KL** anfører, at håndtering af intern dokumentation og anmeldelse af sikkerhedsbrud til Datatilsynet er omfattende og ressourcekrævende. Det synes især uproportionelt, at dokumentationspligten i forbindelse med brud følger samme procedure uanset bruddets omfang og de forbundne risici for de registrerede.

Dataansvarlige skal anmelde brud på persondatasikkerheden til Datatilsynet, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

For at vejlede dataansvarlige om, hvornår det er usandsynligt, at der er risiko for den fysiske persons rettigheder og frihedsrettigheder, har Datatilsynet i februar 2018 udarbejdet en vejledning om håndteringen af brud på persondatasikkerheden. Datatilsynet kommer i den forbindelse med konkrete eksempler for at illustrere, hvornår en anmeldelse til Datatilsynet er påkrævet, herunder også i forhold til tab af fortrolighed for oplysninger der er omfattet af tavshedspligt.

Datatilsynet har også i regi af Det Europæiske Databeskyttelsesråd (EDPB) bidraget til udarbejdelsen af en fælleseuropæisk vejledning fra anmeldelse af brud på persondatasikkerheden (wp 250 rev. 01). Vejledningen, der senest er revideret og vedtaget den 6. februar 2018, indeholder bl.a. eksempler på forskellige typer brud og på, hvem der skal underrettes i de forskellige scenarier. EDPB har den 14. januar i år vedtaget en ny vejledning, som følger op på de erfaringer, de europæiske tilsynsmyndigheder har gjort på området. I vejledningen, der har været sendt i offentlig høring, og som forventes endelig vedtaget i løbet af i år, gennemgår EDPB 18 konkrete eksempler på brud på persondatasikkerheden og redegør for, hvilke handlinger den dataansvarlige bør tage i forlængelse heraf. Kan den dataansvarlige "nøjes" med at skrive bruddet på den liste over alle sikkerhedshændelser, som den dataansvarlige skal føre efter databeskyttelsesforordningens artikel 33, stk. 5, eller skal der ske anmeldelse til tilsynsmyndigheden, ligesom vejledningen også forholder sig spørgsmålet om underretning af de registrerede i hver af de 18 konkrete eksempler på brud på persondatasikkerheden.

Herudover har Datatilsynet i efteråret 2019 udgivet en podcast om databeskyttelsesreglerne, som bl.a. indeholder en episode under titlen "Hvad er et sikkerhedsbrud, og hvad gør jeg, hvis der opstår et sikkerhedsbrud?", som herunder også kommer ind på, hvornår der skal ske anmeldelse til tilsynet.

Datatilsynet har alligevel forståelse for, at afvejningen af, hvorvidt der skal ske anmeldelse til tilsynet, til tider kan være vanskelig. Datatilsynet vil derfor se på en revision af tilsynets vejled-

ning om håndtering af brud på persondatasikkerheden med henblik på at supplere med flere konkrete eksempler.

Datatilsynet kan imidlertid oplyse, at tilsynet i perioden 2018-2020 har modtaget 18.737 anmeldelser om brud på persondatasikkerheden. Kun et fåtal af disse anmeldelser havde en sådan karakter, at de efter Datatilsynets opfattelse ikke burde have været anmeldt til tilsynet.

Endvidere har Datatilsynet i november 2020 afsluttet 15 planlagte tilsyn, der skulle belyse de dataansvarliges evne til at foretage de relevante anmeldelser af brud på persondatasikkerheden. Der blev særligt fokuseret på de dataansvarliges udbredelse af viden og redskaber sådan, at alle relevante medarbejdere ved, hvordan et brud opfanges og indmeldes til den dataansvarliges kontaktpunkt eller direkte til tilsynet. Derudover blev de dataansvarliges dokumentation gennemgået med henblik på at vurdere, om alle relevante brud var blevet indberettet til Datatilsynet.

Der var udvalgt såvel offentlige virksomheder (fem kommuner, en region, to statslige styrelser og to universiteter), som private dataansvarlige (to fagforeninger, en bank, et forsikringsselskab og et privathospital).

Generelt har det været glædeligt at kunne konstatere, at alle de undersøgte dataansvarlige har haft fokus på opgaven, hvor der i de respektive organisationer var den fornødne viden og rutine, sådan at sikkerhedshændelser blev opfanget og indberettet. Det har vist sig, at de dataansvarlige er gode til at vurdere, hvilke af sikkerhedshændelserne der udgør brud på persondatasikkerheden, og hvilke af disse der udgør en risiko for de registreredes rettigheder, og som derfor skal anmeldes til Datatilsynet.

****

Den dataansvarlige skal dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal bruddet anmeldes til Datatilsynet.

Formålet med denne dokumentationspligt er at sætte Datatilsynet i stand til at kontrollere, om forpligtelsen i databeskyttelsesforordningen til at anmelde visse brud på persondatasikkerheden er overholdt, men hænger også sammen med forordningens princip om ansvarlighed ("accountability"). Intern dokumentation er derudover et vigtigt redskab i arbejdet med informationssikkerhed.

For så vidt angår bemærkningen om, at det synes uproportionelt, at dokumentationspligten i forbindelse med databrud følger samme procedure uanset bruddets omfang og de forbundne risici for de registrerede, skal Datatilsynet for en god ordens skyld bemærke, at kravet om dokumentation varierer i forhold til bruddets karakter.

Datatilsynet er opmærksom på, at ressourceforbruget ved håndtering af intern dokumentation og anmeldelse til tilsynet er ressourcekrævende. Datatilsynet er derfor ved at undersøge løsninger, som vil lette ressourceforbruget ved anmeldelser af brud. Datatilsynet vil som nævnt ovenfor endvidere se på en revision af vejledningen om håndtering af brud på persondatasikkerheden med henblik på at supplere med flere konkrete eksempler, og tilsynet vil i den forbindelse også præcisere dokumentationskravet.

Dansk Erhverv og IT-branchen, Danske Regioner, EjendomDanmark, Finans Danmark og **KL** anfører, at det vil lette byrden, hvis der kan etableres en bagatelgrænse i forbindelse med, hvornår et brud skal anmeldes til Datatilsynet, herunder at det vil have en større effekt og værdi for de registrerede, hvis ressourcerne i stedet bruges på de sager, hvor risikoen for den registrerede er moderat eller høj. **KL** foreslår, at stikprøvekontroller af den dataansvarliges hændelseslog eventuelt erstatter anmeldelsesordningen.

Efter Datatilsynets opfattelse vil det ikke være foreneligt med reglerne i databeskyttelsesforordningens artikel 33 at indføre en bagatelgrænse, hvor mindre sikkerhedsbrud undtages fra anmeldelsespligten. Datatilsynet er derudover af den opfattelse, at intern dokumentation og anmeldelse til tilsynet – uanset bruddets karakter – varetager en række saglige hensyn i den dataansvarliges arbejde med at styrke informationssikkerheden.

Finans Danmark anfører, at det vil lette byrden, hvis konsekvenserne ved tab af fortrolighed kan indgå i vurderingen af, hvornår der skal ske anmeldelse og underretning til de registrerede, og at der savnes vejledning om forståelsen af betragtning 85 (”tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt”) i forhold til vurderingen af, hvornår ”det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder”.

Det er Datatilsynets opfattelse, at alle brud på persondatasikkerheden, jf. databeskyttelsesforordningens artikel 4, nr. 12, skal anmeldes til tilsynet, med mindre det er usandsynligt, at der er en risiko for den registreredes rettigheder og frihedsrettigheder, jf. artikel 33, stk. 1. Dette er ikke begrænset til brud på persondatasikkerheden for oplysninger, der er omfattet af tavshedspligt.

Fagbevægelsens Hovedorganisation og **KL** foreslår ændringer til anmeldelsesblanketten, herunder at der eksempelvis udarbejdes en kortere anmeldelsesblanket ved anmeldelsen af mindre brud, og at det bliver muligt at kunne tilføje nye oplysninger til eksisterende anmeldelser.

Anmeldelser af brud på persondatasikkerheden sker via en fællesdigital indberetningsløsning, som administreres af Erhvervsstyrelsen. Datatilsynet er ved at undersøge mulighederne for – og de praktiske konsekvenser af – at revidere anmeldelsesblanketten for at smidiggøre anmeldelsesprocessen for de dataansvarlige. Det bemærkes i den forbindelse, at indholdet af den nuværende anmeldelsesblanket bl.a. er baseret på en skabelon, som Det Europæiske Databeskyttelsesråd (EDPB) har udarbejdet, og at der fra tid til anden er anmeldelser af brud på persondatasikkerheden, som skal håndteres i overensstemmelse med den såkaldte One-Stop-Shop mekanisme.

Dansk Erhverv og IT-branchen anfører, at det bør præciseres, at den dataansvarlige er forpligtet til at meddele databehandleren, hvem der skal modtage oplysning om sikkerhedsbrud, og at denne oplysning jævnligt opdateres.

Danske Regioner anfører, at Datatilsynet bør udarbejde en vejledning om, hvordan ansvaret for et sikkerhedsbrud fastlægges i komplekse databehandlerkonstruktioner, f.eks. tværoffentlige digitale løsninger hvor en myndighed stiller et system til rådighed for andre aktører i sundhedssektoren. **Danske Regioner** anfører endvidere, at der i sagsbehandlingen af konkrete brudsager ofte bruges uforholdsmæssigt meget tid på at afklare det konkrete dataansvar, og at der i nogle situationer sker en dobbeltanmeldelse af bruddet, hvilket er uhensigtsmæssigt for alle parter.

Datatilsynet vil se nærmere på de nævnte udfordringer, herunder i forbindelse med den ovenfor nævnte revision af tilsynets vejledning om brud på persondatasikkerheden.

6. Behandlingssikkerhed, risikovurderinger og konsekvensanalyser

Danske Regioner anfører, at barren for, hvornår der skal udarbejdes metodemæssigt formaliserede risikovurderinger, efter den seneste praksis fra Datatilsynet (j.nr. 2019-441-3399) og Rigsrevisionen (beretning om outsourcede data i det offentlige 15/2019) synes at være meget lav, herunder at praksis tegner et billede af, at der er krav om metodemæssigt formaliserede risikovurderinger for samtlige behandlingsaktiviteter hos den dataansvarlige – store som små, og at dokumenter, der afspejler en reel risikovurdering, ikke bliver anerkendt som en risikovurdering, medmindre dokumentet hedder "risikovurdering" og følger en bestemt metodik. **Danske Regioner** finder, at dette er uhensigtsmæssigt, fordi risikovurderingerne skal fungere i praksis ude hos aktørerne, hvor det ofte er mest hensigtsmæssigt, at risikovurderingerne indbygges i konkrete processer og koncepter, og foreslår derfor, at krav til form og detaljeringsniveau for risikovurderinger bliver mere fleksible, så der bliver mulighed for at tilpasse arbejdet med risikovurderinger til de faktiske organisatoriske forhold og konkrete organisatoriske processer hos den dataansvarlige. **Dansk Regioner** foreslår herudover, at forordningens muligheder for adfærdskodekser og certificeringsordninger udnyttes og anvendes som et led i påvisningen af efterlevelsen af forordningen jf. artikel 24, stk. 3.

Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24 stiller krav om, at den dataansvarlige kan påvise overholdelsen af forordningen. Det fremgår ikke direkte af forordningen, hvordan form eller indhold af denne dokumentation skal være.

Tankegangen om ansvarlighed i artikel 24 udmøntes også i andre bestemmelser i forordningen, såsom artikel 30 om fortegnelser over behandlingsaktiviteter og artikel 35 om konsekvensanalyse vedrørende databeskyttelse.

I forhold til de tidligere regler er der ikke noget nyt i, at der efter forordningens artikel 24 stilles krav om, at den dataansvarlige skal efterleve de databeskyttelsesretlige regler. Størstedelen af de krav, som stilles til den dataansvarlige efter bestemmelsen fandtes således allerede i tidligere lovgivning, om end mindre eksplicit. Se f.eks. Artikel 29-gruppens udtalelse nr. 173/2010 om princippet om ansvarlighed.

Ud over kravet om, at den dataansvarlige skal kunne påvise, at dennes behandling er i overensstemmelse med forordningen, pålægges den dataansvarlige således ikke krav, som ikke var gældende tidligere.

Formålet med en nærmere angivelse af den dataansvarliges ansvar i databeskyttelseslovgivningen er at skabe klarhed over, at det er den dataansvarlige, der som udgangspunkt er ansvarlig for overholdelsen af databeskyttelsesreglerne. Identificeringen af ansvaret for behandlingen betyder ligeledes, at der skabes klarhed over, hvem de registrerede kan udøve deres rettigheder efter databeskyttelsesretten over for, herunder bl.a. retten til at blive glemt, retten til indsigt samt retten til oplysning mv.

Det er Datatilsynets opfattelse, at det direkte af måden, databeskyttelsesforordningen er opbygget på, er forudsat, at der – for en given behandlings udstrækning, fra vugge til grav – foretages en vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder.

Dels fremgår det af artikel 25, at dette skal ske i hele behandlingens livscyklus ("fra fastlæggelse af midlerne"), dels forudsætter artikel 35, at ingen behandling, hvor der er en høj risiko for den registreredes rettigheder og frihedsrettigheder, må påbegyndes, uden en konsekvensanalyse er blevet udført. En sådan analyse kan betragtes som en endnu grundigere risikovurdering, hvortil der er knyttet yderligere formkrav, der skal sikre, at den identificerede høje risiko nedbringes.

Dette kan ses i sammenhæng med databeskyttelsesforordningens artikel 32, hvor fastsættelsen af de "passende tekniske og organisatoriske foranstaltninger" sker i en afvejning af risikoen for de registreredes rettigheder og frihedsrettigheder. Artikel 32, stk. 2, giver herudover en beskrivelse af, hvilke typer af scenarier der navnligt skal indgå i vurderingen.

Samlet set skal den dataansvarlige derfor kunne dokumentere, at disse overvejelser er foretaget, og kunne godtgøre dette også i tilfælde, hvor risikoen for den registrerede er mindre end høj.

Det er Datatilsynets opfattelse, at dette mest hensigtsmæssigt foretages ved en struktureret tilgang, men der er intet krav herom. Uanset tilgang og form er det dog væsentligt, at Datatilsynet – hvis der kommer en klagesag eller ved tilsyn – kan modtage et samlet sæt af informationer fra den dataansvarlige, der betrygger tilsynet i, at vurderingerne er foretaget, og på de påkrævede tidspunkter i behandlingens levetid.

Datatilsynet er herudover af den overbevisning, at der kan være betragtelige forretnings- og udviklingsmæssige synergieffekter ved en sådan struktureret tilgang.

Et godt eksempel er netop sagen, som Danske Regioner henviser til, om en virksomhed, der tre gange inden for kort tid havde sikkerhedsbrud. Datatilsynet var ikke betrygget af de oplysninger, virksomheden fremkom med, dels fordi der ikke var nogen dokumentation af de foretagne vurderinger, dels fordi virksomhedens vurdering af "lav risiko" syntes i strid med de erfaringer, som virksomheden og registrerede havde haft gennem flere brud på persondatasikkerheden.

Det blot at gøre gældende, at "der er gennemført en risikovurdering, og den viste lav risiko" uden nogen dokumentation til at understøtte en sådan påstand, er derfor ikke nødvendigvis nok til at betrygge Datatilsynet. Det er dog væsentligt at fastslå, at Datatilsynet i sin praksis normalt kun spørger til vurderingen i det omfang, der rent faktisk er opstået tvivl om databeskyttelsesreglernes overholdelse. Datatilsynet har herudover oplevet, at "vurderingen" af risiko først er foretaget, efter der er opstået en problematisk situation, som den dataansvarlige er havnet i (f.eks. gentagne sikkerhedsbrud). Dokumentationskravet skal derfor også sikre, at en dataansvarlig ikke blot kan påstå at have foretaget en risikovurdering (uden faktisk at have gjort det) eller påstå, at en databehandling var fundet forsvarlig grundet lav risiko uden dokumentation for, hvordan man har vurderet risikoen til at være lav.

Databeskyttelsesforordningen stiller i øvrigt ingen formkrav til risikovurderinger eller konsekvensanalyser ud over indholdskravet i databeskyttelsesforordningens artikel 35, stk. 7. Dette giver netop råderum til, at den dataansvarlige selv kan vælge en metode.

Datatilsynet vurderer altid sagens oplysninger samlet, og en vurdering eller afvejning af risikoen for den registreredes rettigheder, som den dataansvarlige har foretaget, vil altid indgå heri, selv om den ikke har titlen "Risikovurdering", og uanset hvilken metodik den følger. En

titel på et dokument kan dog indikere noget om formålet/hensigten med dokumentet og kan derved være med til at henlede opmærksomheden på dets relevans.

Datatilsynet udviser en betydelig accept af en mere summarisk beskrivelse af de nødvendige overvejelser, når det gælder de små og mellemstore virksomheder samt for de behandlinger, der generisk (som følge af deres natur og oplysningernes karakter) eller grundet stor ensartethed alene udgør en begrænset risiko for de registreredes rettigheder.

Datatilsynet har igennem en længere periode forsøgt at tydeliggøre dette i afgørelser, der offentliggøres, ligesom tilsynet fremadrettet – i oplysende og vejledende tekster på tilsynets hjemmeside – vil fremkomme med konkrete eksempler på behandlinger af denne karakter.

Datatilsynet tilslutter sig til fulde ønsket om, at forordningens muligheder for anvendelse af adfærdskodeks bliver udnyttet til påvisning af efterlevelsen af forordningen, men det kræver, at sådanne adfærdskodeks eksisterer, og at dataansvarlig/databehandler anvender dem og henviser til dem som en del af påvisningen af efterlevelsen. Det skal endvidere bemærkes, at adfærdskodeks kan udarbejdes af sammenslutninger og andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, jf. databeskyttelsesforordningens artikel 40, stk. 2. Dette kunne f.eks. være Danske Regioner. Datatilsynets rolle i forhold til adfærdskodekser angår godkendelse af disse, jf. forordningens artikel 40, stk. 5.

Akademikerne anfører, at det ved udarbejdelse af risikovurdering og konsekvensanalyse er tæt på umuligt at forudse konsekvenserne i tilfælde af sikkerhedsbrud som følge af de enkelte behandlingsaktiviteter.

Danske Regioner anfører, at det kan være svært at vægte kriterierne for passende sikkerhed, herunder hvor stor en rolle "implementeringsomkostningerne" må spille i forhold til sletning af personoplysninger.

KL anfører, at det er uklart, hvad der konkret skal til for at overholde artikel 32 om behandlingssikkerhed og efterlyser støtte til arbejdet hermed.

Datatilsynet anerkender, at det kan være overvældende for den enkelte dataansvarlige, første gang vedkommende skal foretage en vurdering af risici for registreredes rettigheder.

For mange offentlige og private dataansvarlige er denne type af vurderinger og processerne til at foretage disse dog ikke helt ukendte, da de allerede har en ramme for it-sikkerhed og risikostyring at tage udgangspunkt i. En ramme hvor fokus måske mere har været forretningens risiko og ikke den registreredes rettigheder, men også en ramme hvor de oprindelige redskaber og processer har et betydeligt overlap med de vurderinger, der skal foretages af risikoen for de registrerede. Disse processer og rammeværk kan derfor i stort omfang genbruges.

Datatilsynet kan i lighed med tidligere udgivne vejledninger og betænkningen om databeskyttelsesforordningen pege på internationale standarder som ISO 27001, 27002, 27005, 29151, 29134, 27701. Digitaliseringsstyrelsen udbyder værktøjer, der angår risikovurdering til brug ved implementering af ISO 27001. Dog skal dataansvarlige og databehandlere være opmærksomme på, hvornår et værktøj eller en standard har fokus på organisationen, hvor databeskyttelsesforordningens fokus er på de registrerede. Det betyder, at risici og dermed konsekvenser skal tage udgangspunkt i de registreredes rettigheder og frihedsrettigheder og ikke i f.eks. virksomhedens bundlinje.

Risikovurdering er en særlig disciplin, men der er hjælp at hente. De to centrale elementer i en risikovurdering er sandsynlighed og konsekvens (eller "alvor" som det betegnes i artikel 24 og 32). For så vidt angår vurderinger af sandsynligheder for, at trusler manifesterer sig, og vurdering af deraf følgende potentielle konsekvenser for de registrerede kan der findes inspiration her:

- *Førnævnte værktøjer kan indeholde generelle vurderinger af sandsynligheder for, at trusler manifesterer sig, baseret på internationale erfaringer med f.eks. cyberangreb og insidertrusler.*
- *Nogle af førnævnte internationale standarder indeholder lister over, hvad der bør overvejes.*
- *Trusselsvurderinger fra sikkerhedsfirmaer eller Center for Cybersikkerhed (CFCS), hvoraf sidstnævnte kan være mere målrettet et område, som f.eks. sundhedssektoren i Danmark.*
- *Medieomtaler af sikkerhedsbrud, herunder Datatilsynets afgørelser.*
- *Organisationens egen erfaring med sikkerhedsbrud.*
- *Databeskyttelsesforordningens præambelbetragtning nr. 75.*
- *Justitsministeriets betænkning nr. 1565/2017 (særligt s. 469-490 om forordningens artikel 32)*
- *Danske vejledninger, herunder vejledning af februar 2018 om håndtering af brud på persondatasikkerheden (Datatilsynet), vejledning af juni 2018 om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger (Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen) og den vejledende tekst om risikovurdering af juni 2019, som Datatilsynet har udarbejdet i samarbejde med Rådet for Digital Sikkerhed.*
- *Det Europæiske Databeskyttelsesråds vejledninger, f.eks. vejledning af februar 2018 om anmeldelse af brud på persondatasikkerheden (wp 250 rev. 01) og vejledning 01/2021 om yderligere eksempler på anmeldelse af brud.*
- *Datatilsynets podcastepisode: "Hvad er en risikovurdering, hvornår skal jeg lave den, og hvordan gør jeg".*

Endvidere kan nævnes ISO/IEC DIS 29134 "Information technology – Security techniques – Privacy impact assesment – Guidelines", som er en international standard udarbejdet af den internationale standardiseringsorganisation, International Organization for Standardization, ISO. Standarden er en vejledning i, hvorledes en konsekvensanalyse (Privacy Impact Assesment proces) kan udføres. Standarden beskriver processen i en række trin, hvoraf et trin f.eks. vedrører identifikation af risici, mens et senere trin f.eks. vedrører beslutning om foranstaltninger. Standarden sætter bl.a. fokus på, at behandlingssikkerhed bliver iagttaget og indarbejdet i f.eks. design og implementeringen af IT-løsninger.

Datatilsynet har også bidraget til Det Europæiske Databeskyttelsesråds (EDPB) vejledning af oktober 2017 (wp 248rev.01) om "konsekvensanalyser vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko"", ligesom tilsynet i samarbejde med Justitsministeriet har udarbejdet en national vejledning om konsekvensanalyser, der er offentliggjort i marts 2018. I januar 2019 offentliggjorde Datatilsynet i overensstemmelse med databeskyttelsesforordningen endvidere en endelig liste over situationer, hvor dataansvarlige altid skal udarbejde konsekvensanalyser, efter at listen i udkastform havde været forelagt EDPB til udtalelse.

Angående udtrykket "passende tekniske og organisatoriske foranstaltninger", jf. f.eks. artiklerne 5, stk. 1, litra f, 24, 25 og 32, skal Datatilsynet bemærke, at efter § 41, stk. 3, i persondataloven, som var gældende fra 2000 til 2018, skulle dataansvarlige og databehandlere

træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger. Det er dermed ikke nyt, at det er op til dataansvarlige og databehandlere selv at finde frem til foranstaltninger.

Databeskyttelsesforordningen specificerer, at det tidligere "fornødne" nu skal være "passende" i forhold til risikoen for de registreredes rettigheder. Da der i disse vurderinger er et betydeligt sammenfald, kan de dyder og måder at tænke organisatoriske og tekniske foranstaltninger på, som blev brugt dengang, heldigvis videreføres. Herudover er det Datatilsynets opfattelse, at de foranstaltninger, der korrekt var anset som "fornødne" efter den tidligere retstilstand, generelt også vil være "passende" i dag. Den dataansvarlige skal dog kunne håndtere de få forskelle, der er, f.eks. rettigheden om dataportabilitet. Også ændringer i det generelle trusselsbillede over de seneste år kan indebære et behov for nye/anderledes foranstaltninger – især på cybersikkerhedsområdet.

Det fremgår af vejledningen om behandlingssikkerhed (af juni 2018, ved Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen), at man skal have et passende sikkerhedsniveau for at forhindre, at man behandler oplysninger i strid med forordningen, herunder at de personoplysninger, man behandler, enten hændeligt eller bevidst tilintetgøres, misbruges eller lignende. Hvornår et sådant "passende sikkerhedsniveau" er etableret vil bero på en konkret vurdering. Som vejledende pejlemærke kan nævnes, at et passende sikkerhedsniveau vil afhænge af, hvilke og hvor store risici der er for sikkerhedsbrud og dermed for, at fysiske personers rettigheder og frihedsrettigheder krænkes.

Hertil kan Datatilsynet tilføje, at formuleringen "passende foranstaltninger" giver dataansvarlige/databehandlere flere typer af råderum, som kan være vigtige, f.eks.:

- *I stedet for foranstaltninger, der øger beskyttelsen af personoplysninger mod f.eks. misbrug, kan man vælge foranstaltninger, der begrænser behandlingen, f.eks. sletning eller pseudonymisering.*
- *Man kan justere på forholdet mellem valgte tekniske og organisatoriske foranstaltninger.*
- *Man kan vælge imellem meget forskellige typer foranstaltninger med samme effekt på risikoen.*

Datatilsynet har forståelse for, at det umiddelbart kan føles lettere at få en normativ ramme, der siger, hvad man skal gøre i en given situation, men det er netop det givne råderum, der gør, at den dataansvarlige kan forretningsudvikle eller benytte nye teknologiske muligheder nøjagtig på den måde, som denne dataansvarlige ønsker at gøre det og på den måde, som er mest optimal for netop denne dataansvarlige.

Det er tilsynets opfattelse, at der gennem sammenhængen med artikel 25 og tanken om, at når der laves forretningsudvikling, allerede i designet af behandlingerne af persondata bliver indlejret de fornødne garantier for, at databeskyttelsesforordningen overholdes, ligger en betydelig fokus på redskaber, der netop realiserer det "passende", også set i forhold til det teknologiske niveau og implementeringsomkostninger.

Datatilsynet skal i den anledning henlede opmærksomheden på Det Europæiske Databeskyttelsesråds (EDPB) vejledning nr. 4/2019 af 20. oktober 2020 om artikel 25 og databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

De mange aspekter, som kan påvirke risikoniveauet, betyder også, at der ikke kan defineres et sæt "passende foranstaltninger" alene ud fra information om, hvilken type personoplysninger der behandles. Spørgsmål som "Er TLS-kryptering f.eks. en tilstrækkelig sikkerhedsforan-

staltning til forsendelse af alle typer personoplysninger?" kan derfor ikke umiddelbart besvares. Hvad der er en passende foranstaltning afhænger af flere omstændigheder, f.eks.: Angår spørgsmålet hele eller dele af forsendelsen fra afsender til modtager, eller angår det kun forsendelse mellem to mailservere eller mellem en webserver og en browser? Hvordan er data beskyttet i hele forsendelsen (også den del, som evt. ikke er krypteret)? Hvordan bliver krypteringen etableret? Hvem har mulighed for at dekryptere? Er der tale om en forsendelse, som også kræver validering af den endelige modtager, og altså ikke kun beskyttelse imod uvedkommendes adgang til selve transmissionen? Er der tale om en forsendelse, som også kræver uafviselighed – dokumentation for at indholdet er uændret undervejs fra afsender til modtager?

Dataansvarlige inden for samme område, brancher og lovgivningsområde vil typisk have mange identiske behandlinger og betydeligt sammenfald i opgavetilgangen til løsningen heraf. Det er Datatilsynets opfattelse, at der i disse tilfælde er en stor synergi i at benytte fælles tilgang til at finde et passende niveau af sikkerhed. Det kunne være med fælles udarbejdede vurderinger af behandlinger foretaget med samme software på samme måde i flere kommuner. I den yderste konsekvens ville det antageligt svare til adfærdskodekser, jf. artikel 40, idet et adfærdskodeks netop er tænkt rettet imod specifikke behandlingssektorer, brancher, mv., med sammenlignelige behandlinger af personoplysninger, ensartede behov, ens organisationer, osv.

Adfærdskodekser kan udarbejdes af sammenslutninger og andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, jf. artikel 40, stk. 2. Dette kunne f.eks. være en interesseorganisation, et fagforbund, KL eller Danske Regioner.

Det er dog væsentligt at minde om, at både adfærdskodeks og certificeringer i en eller anden udstrækning begrænser autonomien i opgaveløsningen.

Datatilsynet arbejder på at gøre tilsynets vejledninger mere konkrete, f.eks. ved at lave vejledning om specifikke emner. Dette kunne være forhold om kryptering, sletning, sikkerhed ved flytbare medier, brug af produktionsdata til test og andre emner inden for sikkerhed. Datatilsynet vil have fokus på, at vejledninger så vidt muligt kommer til at indeholde lister over de trusler, som er vigtige at have for øje og undersøge, og forslag til foranstaltninger. Begge dele kan hjælpe ved gennemførsel af risikovurderinger og iværksættelse af passende foranstaltninger.

Datatilsynet opfordrer i øvrigt til, at organisationer, der udfører samme typer af behandlinger under sammenlignelige forhold, kan hjælpe hinanden ved at dele risikovurderinger. Man skal blot være opmærksom på, at ansvaret ikke derved deles eller overføres, og den enkelte dataansvarlige/databehandler skal stadig sikre sig, at risikovurdering også passer til egne behandlinger af personoplysninger.

Hertil kan tilføjes, at databeskyttelsesforordningens frihed til at vælge foranstaltninger også indebærer, at nøjagtig samme risikovurdering for to organisationer ofte vil kunne føre til to fuldt lovlige, men forskellige sæt af foranstaltninger i de to organisationer.

Danske Regioner anfører, at udgangspunktet i dag er, at de enkelte offentlige myndigheder selv skal udføre risikovurderinger af konkrete behandlingsaktiviteter eller systemer. Men i praksis er myndighederne indbyrdes afhængige af hinandens risikovurderinger og sikkerhedsniveau. Et eksempel på dette er videokommunikationstjenester, som blev højaktuelle med COVID-19. Her lavede de offentlige myndigheder forskellige risikovurderinger på baggrund af de trusselsvurderinger, Center for Cybersikkerhed kom med. Dette besværliggjorde samarbejdet på tværs af myndighederne, da myndighederne ikke var enige om, hvordan den digitale

kommunikation på tværs af myndighederne skulle foregå. **Danske Regioner** oplyser endvidere, at i projekter, hvor regionerne enten er pålagt at implementere en bestemt digital løsning, eller der er tale om en tværoffentlig løsning, som skal implementeres hos flere aktører, skal hver enkelt dataansvarlig udarbejde hver deres konsekvensanalyse uden nogen reel mulighed for at vurdere risici i sammenhæng med den samlede tværregionale løsning og uden reelt at have et mitigerende råderum i forhold til eventuelle risici. **Danske Regioner** foreslår på den baggrund bl.a., at der i regi af det fællesoffentlige samarbejde om digitalisering sammen med Justitsministeriet og Datatilsynet hurtigt skabes klarhed i forhold til de juridiske rammer for tværoffentlige it-projekter, herunder indgåelse af databehandleraftaler, risikovurderinger, konsekvensanalyser og modeller for tilsyn på tværs af myndigheder, og at der i forlængelse heraf sættes et arbejde i gang, som skal skabe bedre betingelser for den fællesoffentlige digitalisering og deling af data på tværs af myndigheder, f.eks. igennem øget brug af adfærdskodeks og certificeringer.

Datatilsynet er positivt indstillet over for alle initiativer, der øger databeskyttelsen i situationer, hvor opgaveløsningen går på tværs af flere myndigheder. Datatilsynet medvirker gerne med generel vejledning og sparring til et sådant samarbejde mellem offentlige myndigheder, hvis dette kan reducere den enkelte myndigheds arbejdsbyrde med at lave risikovurderinger. Se også det tidligere anførte om at dele risikovurderinger.

Det er endvidere Datatilsynets erfaring, at sikring af et passende sikkerhedsniveau i grænseflader mellem dataansvarlige kan være en udfordring. En fælles tilgang til både risikovurdering og etablering af passende tekniske og organisatoriske foranstaltninger bydes derfor velkommen.

En udfordring, som også nævnes af Danske Regioner, er, hvis forskellige dataansvarlige har forskellige opfattelser af risici på trods af, at samme trusselsvurdering har været udgangspunktet. Der kan være flere helt reelle forskelle, hvor to dataansvarlige ikke ser samme risiko ved en given behandling, og det kan have en naturlig forklaring i en af følgende årsager:

- *Der er tale om vurderinger af risici, herunder vurderinger af sandsynligheder og potentielle konsekvenser.*
- *Forskellige risikovurderingsmodeller kan med samme input give forskellige resultater.*
- *Risici afhænger af de foranstaltninger, som den enkelte dataansvarlige har gennemført (eller planlægger gennemført), og som derfor indgår i risikovurderingen.*
- *Risici afhænger af, hvilke trusler der er kendt/overvejet i vurderingen. En højere risikovurdering kan skyldes, at én part har kendskab til trusler, som andre ikke har tænkt på/overvejet ved deres egen risikovurdering.*

Selv om den enkelte dataansvarlige har ansvaret for, at der er etableret tilstrækkelig sikkerhed, kan man som dataansvarlige blive bedre og lære af hinanden, og særligt når der er et it-løsningsfælleskab, er dette i højeste grad påkrævet. Men det er også Datatilsynets opfattelse, at databeskyttelsesforordningens hovedregel er, at det er den dataansvarlige, der bestemmer over formål og midler og vurderingen af, hvad den pågældende mener er passende sikkerhed, uanset om der laves en risikovurdering i fællesskab med andre.

Datatilsynet gør endvidere opmærksom på forordningens artikel 35, stk. 10, om muligheden for at udarbejde konsekvensanalyser i forbindelse med lovforslag. Det er dog væsentligt at notere, at dette kræver, at de krav, der er til en konsekvensanalyse, alle er iagttaget under det lovforberedende arbejde. Datatilsynet skal også erindre om, at en sådan fælles konsekvensa-

nalyse skal holdes opdateret i forhold til uforudsete trusler, ændringer i it-miljøer, organisatorisk implementering og ændringer i det generelle trusselsbillede.

Finans Danmark anfører, det i praksis er vanskeligt at afgøre, hvornår pligten i databeskyttelsesforordningens artikel 35, stk. 9, om indhentelse af de registreredes eller deres repræsentanters synspunkter vedrørende en planlagt behandling finder anvendelse, og hvordan den faktisk skal efterleves, herunder hvor meget information de registrerede eller deres repræsentanter skal modtage om den påtænkte behandling – ikke mindst henset til den dataansvarliges forretning (nye forretningsområder) og konkurrenceretlige position.

Datatilsynet og Justitsministeriet har i marts 2018 offentliggjort en vejledning om konsekvensanalyser, hvoraf det bl.a. fremgår (afsnit 8, side 24), at den dataansvarlige – for at sikre den bedste databeskyttelse – bør være omhyggelig ved udførelsen af en konsekvensanalyse, og hvis det er relevant, bør de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling indhentes. Det skal gøres, uden at det berører beskyttelsen af kommercielle eller samfundsmæssige interesser eller behandlingsaktiviteternes sikkerhed. Hvorvidt, det er relevant, afhænger af en konkret vurdering af risiciene for de registrerede, hver gang den dataansvarlige foretager en behandling.

I den danske vejledning er der dette sted endvidere indsat en henvisning til Det Europæiske Databeskyttelsesråds (EDPB) vejledning om konsekvensanalyser fra oktober 2017 (wp 248rev.01). Rådet angiver i denne fælleseuropæiske vejledning, at de registreredes eller deres repræsentanters synspunkter kan indhentes ved hjælp af forskellige midler afhængigt af situationen (f.eks. en generel undersøgelse i relation til formålet med og hjælpemidlerne til behandlingsaktiviteten, et spørgsmål til medarbejderrepræsentanterne eller almindelige undersøgelser, der sendes til den dataansvarliges fremtidige kunder), der sikrer, at den dataansvarlige har et retsgrundlag for behandling af personoplysninger i forbindelse med indhentningen af sådanne synspunkter. EDPB bemærker i forlængelse heraf, at samtykke til behandling ikke er en metode til at indhente synspunkter fra de registrerede.

Det fremgår endvidere af vejledningen fra EDPB, at hvis de registrerede høres, men den dataansvarliges endelige beslutning afviger fra de registreredes synspunkter, skal dette begrundes. De registreredes synspunkt kan således ikke uden videre udelades. Den dataansvarlige bør også dokumentere sin begrundelse for ikke at høre de registrerede.

Det er Datatilsynets vurdering, at det kan være vanskeligt for en dataansvarlig at gennemskue, hvilke konsekvenser en databehandling potentielt kan medføre for enkeltpersoner blandt de registrerede, fordi konsekvenser kan være meget personlige. F.eks. kan sociale konsekvenser være så komplicerede, at det kan kræve personlig erfaring, før man eventuelt kan spotte muligheden for sådanne konsekvenser i en behandling af personoplysninger. Inddragelse af de registreredes synspunkter kan derfor være en forudsætning for en fyldestgørende konsekvensanalyse, men særligt hvor der er høje risici for grupper af registrerede, og hvor der findes organisationer, som varetager disse interesser, bør høring forekomme. Datatilsynet finder, at det i denne situation er relevant at inddrage de registreredes synspunkter, jf. databeskyttelsesforordningens artikel 35, stk. 9.

Angående hensynet til den dataansvarliges forretning (nye forretningsområder) og konkurrenceretlige position, så nævner EDPB's vejledning virksomheders forretningsplaner som en potentiel begrundelse for ikke at inddrage de registrerede. Efter Datatilsynets opfattelse skal dette imidlertid suppleres med en forklaring på, hvordan den dataansvarlige – uden inddragelse af de registreredes synspunkter – har sikret sig en fyldestgørende konsekvensanalyse. Det samme synes også at være angivet som en forventning i EDPB's vejledning.

Sikkerhedsbranchen efterlyser konkret vejledning om, hvordan manuelle registre og fysisk tilgængelige elektroniske enheder indeholdende persondata skal opbevares.

Datatilsynet har offentliggjort flere sager omhandlende opbevaringen af fysiske registre og bærbare/transportable lagringsmedier.

Det er vurderingen af risikoen for den registreredes rettigheder, der lægger niveauet. Normalt anser Datatilsynet det for en passende sikkerhedsforanstaltning, hvis oplysninger, der foreligger i fysisk format (og er omfattet af databeskyttelsesforordningen), låses ned eller opbevares i faciliteter under fornødent opsyn. Et fastmonteret brandsikret pengeskab vil sædvanligvis være tilstrækkeligt til alle typer oplysninger. Hvis tyveri af oplysninger ikke er den væsentligste risiko kan nedlåsning i skrivebordsskuffer mv. være tilstrækkeligt, hvis offentliggørelse eller uretmæssig adgang ikke vil indebære en vis risiko for den registrerede.

Transportable lagringsmedier bør som udgangspunkt krypteres. Dette gælder i alle tilfælde, hvor oplysningerne medbringes ud af huset.

Danmarks Idrætsforbund og **DUF** angiver, at det er en udfordring at konkretisere den passende sikkerhed i en organisation med frivillige, herunder hvis de frivillige udfører opgaverne med deres egne computere.

Datatilsynet har forståelse for, at der i foreninger, hvor de frivillige benytter egne computere til opgaveløsningen, kan være særlige problemstillinger omkring håndteringen af dataansvaret – særligt de passende sikkerhedsforanstaltninger. Datatilsynet er af den opfattelse, at det bedst håndteres i to tempi. For det første, at man stiller redskaber (eventuelt centralt) til rådighed, hvis der behandles personoplysninger, der bør holdes fortroligt. For det andet, i de tilfælde, hvor dette ikke er muligt, skal der være oplysning af de frivillige om håndteringen af personoplysninger. Hvis der fyldestgørende er instrueret herom, vil dette altovervejende være passende, hvis der fra den dataansvarlige forenings side bliver fulgt op, hvis det konstateres, at behandling sker mod de fastsatte instruktioner.

Datatilsynets generelle retningslinjer for brugen af e-mail og SMS er ikke ufravigelige, men udtryk for det, der normalt må anses for passende sikkerhed ved behandling af følsomme og fortrolige oplysninger. Det er ikke Datatilsynets opfattelse, at der ved behandlingen af lav-risiko personoplysninger (f.eks. hvem der skal vaske holdets trøjer eller køre til næste kamp) normalt skal foretages en individuel vurdering, inden en given e-mail kan afsendes.

Datatilsynet har endvidere stor forståelse for de forhold, foreningskulturen er udtryk for. Der vil forekomme fejl og situationer med brud baseret på det faktum, at det er frivillige, der varetager opgaven ude i foreningerne. Hvis der som anført er foretaget en vejledning af de frivillige om håndtering af de typetilfælde, hvor der påregneligt indgår særligt beskyttelsesværdige personoplysninger, vil dette normalt være passende foranstaltninger. Dette vil naturligvis også blive tillagt vægt ved Datatilsynets eventuelle vurdering af forholdet, f.eks. i forbindelse med en klagesag.

7. Fortegnelse og andre dokumentationskrav

Dansk Arbejdsgiverforening oplever, at mange virksomheder har svært ved at leve op til de omfattende dokumentationskrav, som virksomhederne først har skullet udarbejde og nu skal vedligeholde. Der er hos mange virksomheder og rådgivere en oplevelse af aldrig at være i mål med opfyldelsen og egenkontrollen af reglernes efterlevelse, som beror på en tilbagevendende usikkerhed om, "hvad der er nok". I mindre virksomheder og i særdeleshed enkeltmandsvirksomheder kan udfærdigelsen af skriftlig dokumentation – såsom fortegnelsen – være en selvstændig udfordring. **Dansk Arbejdsgiverforening** foreslår, at Datatilsynet udarbejder en standardfortegnelse, der kun kræver afkrydsning eller lignende. **Dansk Arbejdsgiverforening** oplyser endvidere, at Datatilsynet har foretaget ændringer i tilsynets vejledning om opfyldelsen af fortegnelseskravet i databeskyttelsesforordningens artikel 30 for så vidt angår sammenkædningen mellem kategorier af registrerede og kategorier af oplysninger. Mange virksomheder har arbejdet med databeskyttelse i flere år og kan ikke blot tilføje de supplerende oplysninger. Det vil derfor være hensigtsmæssigt, at Datatilsynet tænker grundigt over, hvilke konsekvenser det har for virksomhederne, og at der gives længere tid til implementering, når tilsynet ændrer fortolkning af kravene.

DUF anfører, at det kan virke meget voldsomt og tidskrævende for en gruppe at skulle dokumentere compliance.

KL mener, at det er uklart, hvilke og hvor mange foranstaltninger den enkelte dataansvarlige kommune skal iagttage for at leve op til kravet om at kunne påvise ansvarlighed i forhold til overholdelsen af behandlingsprincipperne. **KL** oplyser i den forbindelse, at kommunernes opgavevaretagelse, herunder håndtering af persondata, allerede i vidt omfang er detaljeret reguleret ved lov. **KL** efterlyser konkretisering og uddybning af påvisningskravet via mere vejledning, så det undgås, at kommunerne indfører unødvendige procedurer, og at der sker overimplementering af kravet. I den forbindelse bør det ligeledes afklares, hvorvidt der stilles de samme dokumentationskrav til behandlingsaktiviteter, der har fundet sted forud for databeskyttelsesforordningens ikrafttræden, eller om kravet gælder i forhold til behandlingsaktiviteter, som kommunerne har iværksat efter, at databeskyttelsesreglerne trådte i kraft. Ved en eventuel revision af databeskyttelsesforordningen foreslår **KL**, at det overvejes, om de mange dokumentationskrav kan erstattes med andre modeller til sikring af, at reglerne overholdes, f.eks. at registrerede og kommunalt ansatte bliver spurgt, om de føler sig trygge i forhold til kommunens databehandlinger.

Databeskyttelsesforordningen stiller overordnet ingen formkrav til, hvordan dokumentation skal foretages. Dette giver netop råderum til, at den dataansvarlige selv kan vælge en metode. Det væsentlige er, at Datatilsynet bliver betrygget i, at principperne overholdes, og at den dataansvarlige kan demonstrere, hvordan dette sker.

Datatilsynet vurderer altid sagens oplysninger samlet, og alle bidrag omkring den dataansvarliges forretningsvaretagelse kan benyttes til dokumentation. Særligt relevant er de overvejelser, der indeholder en vurdering eller afvejning af risikoen for den registreredes rettigheder, som den dataansvarlige har foretaget.

Datatilsynet udviser en betydelig accept af en mere summarisk beskrivelse af de nødvendige overvejelser, når det gælder behandlinger, der som følge af deres natur og oplysningernes karakter alene udgør en begrænset risiko for de registreredes rettigheder. Her vil kravet efter omstændighederne også kunne dokumenteres i mere generelle brancheanbefalinger eller den blotte konstatering af forholdene omkring behandlingen. Dette gælder også, hvis forholdet er reguleret ved lov.

Konkrete dele af databeskyttelsesforordningen kan give støtte til påvisningen, f.eks. kravene til fortegnelse, konsekvensanalyse og databehandleraftaler.

Kravet om at føre en fortegnelse er ikke helt nyt. Persondatalovens kapitel 12-14 indeholdt således regler om anmeldelse af behandling af personoplysninger til Datatilsynet mv. Ud over denne generelle anmeldelsespligt var den dataansvarlige forpligtet til at stille de i lovens § 43, stk. 2, nr. 1, 2 og 4-6, nævnte oplysninger om alle de behandlinger af personoplysninger, som vedkommende udførte, til rådighed for enhver, som anmodede herom, jf. persondatalovens § 54, stk. 2. Dette betød, at den dataansvarlige på anmodning havde pligt til at udarbejde og inden for rimelig tid udlevere en oversigt over alle behandlinger, denne foretog, herunder behandlingsaktiviteter som ikke var anmeldelsespligtige.

Den generelle forpligtelse til at anmelde behandling af personoplysninger til Datatilsynet medførte en administrativ og finansiel byrde, men den bidrog ikke i alle tilfælde til at forbedre beskyttelsen af personoplysninger. Der var derfor behov for mere effektive procedurer og mekanismer, som fokuserer på de typer behandlingsaktiviteter, der sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder i medfør af deres karakter, omfang, sammenhæng og formål, jf. præambelbetragtning nr. 89, hvilket er baggrunden for, at den generelle anmeldelsespligt med databeskyttelsesforordningen er blevet erstattet af kravet om at føre interne fortegnelser, jf. databeskyttelsesforordningens artikel 30. Dette ligger fint i tråd med forordningens risikobaserede tilgang og fokus på ansvarlighed ("accountability").

Forpligtelsen til at føre fortegnelse gælder såvel behandlingsaktiviteter, der har fundet sted forud for reglernes ikrafttræden, som behandlingsaktiviteter, som er iværksat efter, at reglerne trådte i kraft. Det er endvidere Datatilsynets opfattelse, at formålsafgrænsningen, som dataansvarlige kan foretage i forbindelse med oplysningspligten, også gælder ved kravet om fortegnelse.

For så vidt angår bemærkningerne om Datatilsynets reviderede vejledning om fortegnelseskravet fra august 2020 bemærkes indledningsvis, at opdateringen skete på baggrund af en række erfaringer, som Datatilsynet – som led i sin tilsynsopgave – havde gjort sig efter den 25. maj 2018, hvor databeskyttelsesforordningen begyndte at finde anvendelse. Opdateringen af vejledningen bestod primært i en tydeliggørelse af, at fortegnelsen over behandlingsaktiviteter – efter Datatilsynets vurdering, når man ser på formålene med fortegnelseskravet – skal indeholde en tydelig angivelse af, hvilke kategorier af personoplysninger der behandles om de enkelte kategorier af registrerede. Hvis der bliver eller vil blive videregivet personoplysninger i forbindelse med en behandlingsaktivitet, skal fortegnelsen også indeholde information om, hvilke kategorier af personoplysninger der bliver eller vil blive videregivet til den pågældende modtager. I tilknytning hertil skal det også fremgå, hvilke kategorier af registrerede de pågældende oplysninger vedrører.

Datatilsynet kan ikke afvise, at der vil være dataansvarlige, der vil skulle foretage visse ændringer i deres fortegnelser efter artikel 30 som følge af tilsynets ændringer fra august 2020. Datatilsynet forventer imidlertid ikke, at dataansvarlige – som følge af ændringerne – genåb-

ner deres fortegnelse. Datatilsynet forventer, at eventuelle tilpasninger eller justeringer af fortegnelsen sker løbende, når dokumenterne alligevel skal justeres eller ajourføres.

Når det gælder muligheden for, at Datatilsynet udarbejder en standardfortegnelse, der kun kræver afkrydsning eller lignende fra virksomhedens side af, er der som bilag til tilsynets vejledning om fortegnelse udarbejdet et eksempel på en fortegnelse over behandlingsaktiviteter vedrørende HR. I eksemplet gives der bl.a. mulighed for at afkrydse, hvilke kategorier af registrerede og kategorier af personoplysninger der behandles af den dataansvarlige. Det vil imidlertid være vanskeligt og uhensigtsmæssigt at udarbejde én standardfortegnelse, som dataansvarlige generelt skal kunne benytte sig af, da der kan være mange forskellige formål med behandlingsaktiviteter, som ikke har en sådan sammenhæng, at de kan samles i én fortegnelse.

Hvis en kommune behandler personoplysninger som led i sin myndighedsudøvelse, vil der imidlertid inden for myndighedsudøvelsen ofte kunne rummes en række "delformål", som f.eks. kan bestå i udbetaling af kommunale ydelser, vejledningsopgaver, kommunal indsats vedrørende jobformidling mv. I en sådan situation vil fortegnelseskravet ikke indebære, at kommunen er forpligtet til at lave en fortegnelse til hvert eneste delformål. Delformålene egner sig i stedet til at blive beskrevet under et samlet, logisk og sammenhængende formål, da de enkelte delformål typisk vil have en indbyrdes sammenhæng, eksempelvist fordi er tale om den samme opgave eller samme lovgrundlag for behandlingerne, og vil derfor med fordel kunne indgå i én fortegnelse.

8. Offentlige myndigheders anvendelse af artikel 6, stk. 1, litra e

KL anfører, at der er en udbredt tvivl om afgrænsningen af behandlingsgrundlaget i databeskyttelsesforordningens artikel 6, stk. 1, litra e, og det hertil knyttede nødvendighedskrav, som også findes artikel 5, stk. 1, litra c, om dataminimering. Det gælder i forbindelse med udveksling af oplysninger inden for samme forvaltning, mellem forvaltninger og mellem myndigheder, men også i forbindelse med brug af billeder i kommunernes kommunikationsarbejde, herunder på sociale platforme, og i forbindelse med dagligdagen i kommunale skoler og institutioner. **KL** oplyser, at denne uklarhed fører til, at mange kommuner tyr til samtykke som behandlingsgrundlag.

Det fremgår af databeskyttelsesforordningens artikel 6, stk. 1, litra e, at behandling er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Efter bestemmelsens stk. 2 kan medlemsstaterne opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af forordningens bestemmelser om behandling med henblik på overholdelse af bl.a. artikel 6, stk. 1, litra e, ved at fastsætte mere specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling.

Efter bestemmelsens stk. 3 skal grundlaget for behandling i henhold til forordningens artikel 6, stk. 1, litra e, fremgå af enten EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt. Dette retsgrundlag kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i forordningen.

Bestemmelserne i forordningens artikel 6, stk. 2 og 3, indebærer for det første, at behandlingen – for at kunne ske i medfør af 6, stk. 1, litra e – skal fremgå af EU-retten eller medlemsstaternes nationale ret. Det betyder, at anvendelsen af artikel 6, stk. 1, litra e, kræver, at behandlingen er forudsat i EU-retten eller national ret, men ikke nødvendigvis, at der er en national implementerende hjemmelslovgivning om selve behandlingen.

For det andet indebærer forordningens artikel 6, stk. 2 og 3, at medlemsstaterne har mulighed for at fastsætte krav til behandlingen, som skal være opfyldt, for at behandlingen er lovlig.

Der er i særlovgivningen fastsat en lang række bestemmelser, som fastsætter krav til behandlingen, typisk bestemmelser som kræver borgerens samtykke.

Et sådant eksempel på en national behandlingshjemmel, hvorefter behandling af oplysninger alene kan ske, hvis bestemte betingelser er opfyldt, findes i forvaltningslovens § 29. Det fremgår af denne bestemmelse, at der i ansøgningssager alene må indhentes oplysninger om ansøgerens rent private forhold fra andre dele af forvaltningen eller fra en anden forvaltningsmyndighed, hvis ansøgeren har givet samtykke hertil, andet følger af lov eller bestemmelser fastsat i henhold til lov, eller særlige hensyn til ansøgeren eller tredjemand klart overstiger ansøgerens interesse i, at oplysningen ikke indhentes.

Selvom der i særlovgivningen stilles krav om, at myndigheden indhenter samtykke, betyder dette ikke, at myndighedens hjemmel efter forordningen dermed bliver samtykke. Myndighedens hjemmelsgrundlag vil i disse tilfælde fortsat være forordningens artikel 6, stk. 1, litra e, men myndigheden skal ikke særskilt overveje, om behandlingen er lovlig efter denne bestemmelse, idet behandlingen vil være lovlig, hvis den overholder de krav, som følger af særlovgivningen – f.eks. kravene til et samtykke i den pågældende lovgivning.

I andre og langt de fleste tilfælde vil særlovgivningen imidlertid ikke indeholde specifikke krav til behandlingen af personoplysninger eller i øvrigt foreskrive specifikt, om og hvilke personoplysninger der skal behandles. Behandling af personoplysninger vil imidlertid typisk være en forudsætning for, at myndigheden kan løse de opgaver, som lovgivningen foreskriver. Dette kunne f.eks. være en myndigheds vurdering af en borgers ret til sociale ydelser efter den sociale lovgivning eller lovgivning om myndighedens opgaver på børne- og skoleområdet.

Hvornår behandling i henhold til forordningens artikel 6, stk. 1, litra e, kan anses for nødvendig, skal i disse tilfælde holdes op imod de opgaver og forpligtelser, som myndigheden har i henhold til den lovgivning, som regulerer dens virke. Tilsvarende gælder i forhold til det krav om nødvendighed, som følger af forordningens artikel 5, stk. 1, litra c.

Det er i den forbindelse vigtigt at understrege, at databeskyttelsesreglerne ikke har til formål at stå i vejen for eller besværliggøre offentlige myndigheders opgavevaretagelse. Databeskyttelsesreglerne, herunder kravet om nødvendighed, indebærer således ikke, at offentlige myndigheder for enhver pris skal tilrettelægge deres opgavevaretagelse på en sådan måde, at der behandles færrest muligt personoplysninger, hvis dette vil afskære myndigheden fra at løse sine opgaver på den i lovgivningen tiltænkte måde.

Det databeskyttelsesretlige krav om nødvendighed er derimod fleksibelt og giver den dataansvarlige – i denne kontekst offentlige myndigheder – muligheden for at vurdere, hvad der i det enkelte tilfælde er relevant og sagligt, dvs. nødvendigt, for at myndigheden kan varetage sine opgaver på den måde, som er tiltænkt med lovgivningen. I den forbindelse er det også vigtigt at holde sig for øje, at den myndighed, som i lovgivningen forudsættes at udføre en opgave, i sagens natur har de bedste forudsætninger for at vurdere, hvad der er sagligt og relevant for at løse opgaven, idet det netop er den pågældende myndighed, som har mest kendskab til, hvordan eventuel sektorspecifik lovgivning udmøntes i praksis.

Det vil således ligge inden for rammerne af databeskyttelsesforordningens artikel 6, stk. 1, litra e, hvis myndigheden kan pege på et lovgrundlag som årsagen til behandlingen, og hvis behandlingen ikke – ud fra en generel betragtning – er unødigt indgribende for den registrerede, f.eks. fordi behandlingen udelukkende er en praktisk måde for myndigheden at opfylde formålet på, som ikke tager hensyn til den registrerede.

Med andre ord har offentlige myndigheder ganske vide rammer for at vurdere, hvilken behandling af oplysninger der er nødvendig for at varetage myndighedens opgaver i henhold til lovgivningen.

I forhold til eksemplet fra KL om anvendelsen af billeder i kommunernes kommunikationsarbejde og i forbindelse med dagligdagen i kommunale skoler og institutioner, er det efter Datatilsynets opfattelse vigtigt at skelne mellem de forskellige situationer. Det må antages, at forældreinddragelse, herunder at forældrene orienteres om børnenes dagligdag, er en væsentlig – og vel også nødvendig – forudsætning i medfør af kommunens forpligtelse til at drive dagtilbud/skole. Derfor kan det også anses for en nødvendig del af kommunens opgaver som myndighed, at daginstitutionen/skolen tager billeder og deler dem (internt) med forældrene for

at orientere om børnenes dagligdag, og kommunens mulighed herfor er således ikke betinget af, at der indhentes samtykke fra forældrene. Man skal blot huske på, at man ikke bør tage billeder af børnene (eller personalet) i situationer, som kan opfattes udstillende, ligesom man – i det omfang en forælder af forskellige årsager ikke måtte ønske, at der bliver taget billeder af vedkommendes barn – som en naturlig del af forholdet mellem daginstitution/skole og forældre indgår i en dialog herom.

Det kan heller ikke afvises, at det i andre tilfælde må anses for en del af myndighedens opgaver, at myndigheden informerer offentligheden omkring myndighedens aktiviteter på et givent område – f.eks. skoleområdet. I det omfang dette er tilfældet, vil man også kunne anvende billeder i den sammenhæng, uden at der indhentes samtykke. I disse situationer er det imidlertid vigtigt at være opmærksom på, at offentliggørelse på internettet sædvanligvis må anses for at være mere indgribende end en deling af billeder internt på et (forældre)intranet. Man bør derfor i sådanne tilfælde bruge sund fornuft og ikke vælge billeder, hvor specifikke personer har en fremtrædende rolle – f.eks. portrætfotoer. Derimod er der typisk ikke noget til hinder for at anvende fotos, hvor enkeltpersoner ikke er i særligt fokus, f.eks. et harmløst foto af en gruppe legende børn eller et luftfoto af en hel skole. Hvis man er i tvivl om, hvorvidt nogen med rimelighed kan føle sig udstillet, vil det naturlige være, at man spørger vedkommende, hvilket ikke nødvendigvis betyder, at der skal indhentes et egentligt samtykke.

9. Opbevaringsbegrænsning og sletning

Dansk Industri anfører, at der i praksis opleves usikkerhed og stort ressourceforbrug ved fastlæggelse af slettefrister. Selv om slettefrister ofte afhænger af det konkrete formål, er der også mange opbevaringsperioder, hvor det bør være muligt at lave vejledning fra Datatilsynet til gavn for virksomhederne, f.eks. i forhold til oplysninger om dokumentation efter bogføringsreglerne og skattelovgivningen, tidligere ejere i selskabers ejerbøger, tilbagetrukne markedsføringssamtykker og HR-oplysninger.

Danske Regioner oplyser, at spørgsmålet om sletning af oplysninger i patientjournaler giver anledning til diskussioner om samspillet mellem journalføringsbekendtgørelsen og databeskyttelsesreglerne, da det følger af journalføringsbekendtgørelsen, at der ikke må slettes eller rettes i patientjournaler. Diskussionen omhandler, hvornår fejlagtige oplysninger i patientjournaler som følge af f.eks. systemtekniske fejl, anvendelsesfejl og forvekslingsfejl kan/må slettes. Det er ikke altid klart, hvilket regelsæt der regulerer hvad og hvornår. **Danske Regioner** anfører endvidere, at der mangler afklaring af det mere generelle spørgsmål om, hvor lang tid patientjournaler må opbevares, når de 10 års opbevaringspligt i journalføringsbekendtgørelsen er gået.

Danske Medier oplyser, at medier i enkelte situationer oplever en diskrepans mellem sletteforpligtelsen og andre lovgivningskrav, der giver anledning til tvivl om den rette databeskyttelsesretlige håndtering. Forbrugeraftalelovens regler om uanmodede henvendelser og adgangen til at foretage telefonsalg af abonnementer på aviser, ugeblade og tidsskrifter, indebærer en forpligtelse for mediet til at notere, når en person i forbindelse med telefonopkaldet frabeder sig yderligere henvendelse fra den erhvervsdrivende. Dette medfører, at medierne for at undgå at kontakte pågældende fører lister over personer, som ikke ønsker yderligere opringninger. Spørgsmålet er, hvor længe disse lister bør opbevares. Mediet har ingen interesse i at opbevare kontaktoplysninger på en forbruger i længere tid end nødvendigt, men ønsker heller ikke at overtræde forbrugeraftelovens regler om uanmodede henvendelser. Da lovgivningen som udgangspunkt ikke giver mulighed for at kontakte forbrugeren for at høre, hvorvidt pågældende fortsat ønsker at stå på listen, kan dette i yderste konsekvens føre til, at disse lister opbevares i meget lang tid.

DGI anfører, at det er en udfordring at fastlægge, hvor længe og hvor mange oplysninger en forening kan gemme om udmeldte medlemmer. **DGI** har overvejet, at foreningen i et år efter udmeldelsen kan gemme alle data af hensyn til genaktivering, at foreningen i 5 år efter udmeldelse kan gemme alle stamdata af hensyn til dokumentation over for kommunen ved tilbudskontrol efter folkeoplysningsloven, og at foreningen efter interesseafvejningsreglen kan gemme de persondata, herunder resultater, der har historisk værdi. I forhold hertil er det – ud fra Datatilsynets udtalelse om at kunne invitere til jubilæum – imidlertid usikkert, hvor mange data der kan gemmes alene for at kunne kontakte et tidligere medlem.

EjendomDanmark oplyser, at et flerårigt lejeforhold kan generere en del dokumenter med persondata, hvoraf langt de fleste vil indeholde de samme data, som f.eks. navn og adresse, der har karakter af almindelige personoplysninger. Som eksempel herpå nævnes breve med oplysninger om ny kontaktperson hos administrator og breve med varsling af lejestigninger, som begge er dokumenter, som indeholder navn og adresse på lejeren, hvoraf det ene ikke

har værdi efter fraflytning, hvorimod varsling af lejestigning bør opbevares af hensyn til risiko for at blive mødt med et retskrav. Disse dokumenter har således forskellige forældelsesfrister, og en løbende sletning af dokumenterne i forbindelse med forældelse medfører et omfattende administrativt arbejde.

Finans Danmark anfører**,** at det i praksis er vanskeligt for dataansvarlige at vurdere, hvad der udgør det rette tidsrum.

Folkeoplysningens Brancheorganisation anfører, at reglerne om opbevaringsbegrænsning kræver, at foreninger – årligt – gennemgår de steder, hvor foreninger opbevarer persondata, for at sikre, at der sker rettidig sletning, hvilket kræver mange ressourcer. **Folkeoplysningens Brancheorganisation** foreslår derfor bedre og mere præcise vejledninger til foreninger.

Det er et grundlæggende princip, at personoplysninger ikke må opbevares længere, end det er nødvendigt i forhold til de(t) formål, hvortil de behandles. Når det ikke længere er nødvendigt at opbevare oplysningerne for at opfylde formålet, skal oplysningerne således slettes. Alternativt kan der ske anonymisering af oplysningerne, så de ikke længere er personhenførbare. Dog gælder der en undtagelse, hvis oplysningerne udelukkende behandles til arkivformål, til videnskabelige formål eller til statistiske formål. Dette princip er i øvrigt ikke nyt, idet der er tale om en videreførelse af en tilsvarende regel i den tidligere gældende persondatalov (lovens § 5, stk. 5).

Hvis der gælder et krav om opbevaring af personoplysninger i anden lovgivning, skal en sådan opbevaringsfrist overholdes. Der gælder f.eks. særlige krav i forhold til opbevaring af personoplysninger efter reglerne i bogføringsloven og journalføringsbekendtgørelsen.

Hvis et forhold ikke reguleres af anden lovgivning, gælder de almindelige databeskyttelsesregler. I de tilfælde er det ikke altid lige let at fastlægge, for hvilket tidsrum opbevaring af personoplysninger kan ske, idet databeskyttelsesreglerne ikke indeholder faste grænser herfor.

Den omstændighed, at databeskyttelsesreglerne ikke specifikt angiver, hvor længe personoplysninger må opbevares, er dog ikke nødvendigvis en dårlig ting, idet databeskyttelsesreglerne herved giver den enkelte dataansvarlige mulighed for at fastsætte slettefrister, som passer til deres virksomhed, myndighed mv. Reglerne giver således den enkelte dataansvarlige et råderum til at vurdere, hvor længe det er nødvendigt at opbevare personoplysninger for at opfylde de(t) formål, som den enkelte dataansvarlige har.

At den enkelte dataansvarlige har et råderum til at vurdere, hvor længe det er nødvendigt at opbevare personoplysninger for at opfylde de(t) formål, som den enkelte dataansvarlige har, indebærer samtidig, at Datatilsynet som udgangspunkt ikke vil tilsidesætte fastsatte slettefrister, som bygger på relevante og saglige overvejelser, da det jo netop er den virksomhed, myndighed mv., som behandler personoplysninger, der også ved, hvor længe der et formål, som nødvendiggør behandling (f.eks. opbevaring) af personoplysninger.

Det skal i øvrigt påpeges, at dataansvarlige – så længe der er fastsat procedurer, som sikrer sletning i overensstemmelse med fastsatte slettefrister – ikke har pligt til løbende at gennemgå samtlige sager eller dokumenter mv. med henblik på at sikre, at der ikke opbevares enkeltstående personoplysninger i strid med reglerne om opbevaringsbegrænsning.

Selv om det således i udgangspunktet er den dataansvarlige, som i første omgang er nærmest til at vurdere, hvor længe det er nødvendigt at opbevare personoplysninger, vil Datatil-

synet også løbende gennem tilsynets vejledninger og praksis mv. fastsætte kriterier, som dataansvarlige kan lade indgå i sin vurdering af slettefrister.

Datatilsynet har bl.a. – i forhold til noget af det, der her spørges ind til – i forbindelse med et konkret tilsyn udtalt, at der ikke var grundlag for at tilsidesætte en virksomheds vurdering af, at oplysninger om ansøgere efter endt rekrutteringsforløb kan opbevares i op til seks måneder, uagtet om formålet med behandlingen er at tilbyde ansøgeren en anden stilling eller at dokumentere, hvorledes udvælgelsen er sket i rekrutteringsprocessen. Det betyder imidlertid ikke, at det ikke efter omstændighederne kan være berettiget at opbevare sådanne oplysninger i en længere periode end seks måneder, hvis dette vurderes nødvendigt.

I forhold til det, som Danske Regioner oplyser, skal man se på, om reglerne i journalføringsbekendtgørelsen regulerer forholdet. Er dette tilfældet, vil man overholde databeskyttelsesreglerne, hvis man gør som bekendtgørelsen foreskriver. Reguleres forholdet derimod ikke af journalføringsbekendtgørelsen – enten fordi det falder helt uden for bekendtgørelsens anvendelsesområde eller fordi opbevaringskravet på 10 år er udløbet – gælder de almindelige databeskyttelsesregler, herunder også at oplysninger kan behandles, så længe det er nødvendigt af hensyn til formålet.

Særligt for så vidt angår de slettefrister, som DGI har overvejet, så synes disse efter Datatilsynets opfattelse umiddelbart velbegrundede. Spørgsmålet om slettefrister skal dog ses i sammenhæng med princippet om dataminimering, og det er derfor vigtigt at være opmærksom på, at man ikke opbevarer flere oplysninger, end det der er nødvendigt. F.eks. synes det ikke nødvendigt at opbevare andet end en e-mailadresse – eventuelt i kombination med et navn – for at kunne invitere tidligere medlemmer til jubilæumsarrangementer.

10. Oplysningspligt

Dansk Arbejdsgiverforening anfører, at der er uklarhed om omfanget af oplysningspligten i forbindelse med brugen af kontrolforanstaltninger over for medarbejdere, og at Datatilsynets seneste afgørelser har efterladt et indtryk af, at der kræves mere, end der umiddelbart fremgår af Datatilsynets egen skabelon. **Dansk Arbejdsgiverforening** bemærker i den forbindelse, at uklarheden i et vist omfang kan imødegås ved en opdatering af vejledningen om de registreredes rettigheder.

Danske Advokater angiver, at der foreligger tvivl om rækkevidden af oplysningspligten efter databeskyttelsesforordningens artikel 14 i forhold til advokaters tavshedspligt og de begrænsninger af de registreredes rettigheder, som følger af databeskyttelseslovens § 22. **Danske Advokater** oplyser i den forbindelse, at advokater i deres arbejde modtager en række oplysninger om registrerede, herunder vidner, skønsmænd mv., som stammer fra advokatens klienter, og som udgør en grundforudsætning for advokatens rådgivning af klienten.

Danske Regioner er i tvivl om, hvor konkret og specifikt den registrerede skal oplyses om formålene med den behandling, som personoplysningerne skal bruges til, og i hvor stort et omfang den dataansvarlige kan gå ud fra, at den registrerede allerede er bekendt med formålet, når behandlingen af personoplysninger sker med henblik på at løse myndighedens kerneopgaver, f.eks. patientbehandling.

DGI anfører, at det er uklart, hvornår undtagelserne til oplysningspligten kan anvendes, og at der savnes praktiske eksempler på, hvornår oplysningspligten ikke skal opfyldes af foreninger.

EjendomDanmark anfører, at oplysningspligten ikke skal opfyldes i forhold til bipersoner. **EjendomDanmark** savner dog en klar definition af en biperson, og om der kan skelnes mellem forbrugere og erhvervsdrivende. **EjendomDanmark** oplyser endvidere, at der ved afgørelse af tvister inden for lejeretten er behov for at indsamle og eventuelt udlevere oplysninger om sammenligningslejemål og i forbindelse hermed behandles der personoplysninger i form af adresse og eventuelt navn. Det er uklart for **EjendomDanmark**, om denne behandling udløser en oplysningspligt, eller om forholdet er omfattet af undtagelsesbestemmelserne i databeskyttelsesforordningens artikel 14, stk. 5.

KL angiver, at der i kommunerne ofte er tvivl om, hvordan og i hvilke tilfælde oplysningspligten skal opfyldes. Tvivlen opstår bl.a. i forhold til, hvornår der er tale om et nyt formål, hvor bredt et formål må være, og hvor specifikt oplysningspligten skal gives. **KL** oplyser endvidere, at oplysningspligten over for bipersoner er en udfordring for kommunerne.

Databeskyttelsesforordningens artikel 13 og 14 pålægger den dataansvarlige at give den registrerede en række oplysninger om den behandling af personoplysninger, som den dataansvarlige foretager, når oplysningerne er indsamlet fra den registrerede eller fra andre. Det betyder bl.a., at den dataansvarlige skal oplyse om de formål, som personoplysningerne skal bruges til, samt retsgrundlaget for behandlingen.

Reglerne om oplysningspligt er ikke nye, selvom forordningen med artikel 13 og 14 generelt udvider omfanget af den dataansvarliges oplysningspligt. Reglerne om oplysningspligt blev allerede indført i dansk ret i forbindelse med, at den tidligere gældende persondatalov trådte i kraft den 1. juli 2000.

Formålsangivelsen har til formål at sikre en gennemsigtig behandling, og den registrerede skal derfor have tilstrækkelig information til, at den pågældende bliver klar over, hvad der er baggrunden for, at der indsamles oplysninger om vedkommende.

Forordningens artikel 12, stk. 1, stiller krav om, at den dataansvarlige skal træffe foranstaltninger til at give enhver oplysning som omhandlet i artikel 13 og 14 i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog, navnlig når oplysningerne specifikt er rettet mod et barn.

Hvis den dataansvarlige agter at viderebehandle personoplysninger til et andet formål end de(t) oprindelige, skal den dataansvarlige forud for behandlingen bl.a. give den registrerede oplysninger om det nye formål. Formålet hermed er at sikre, at behandling af personoplysninger ikke kommer bag på den registrerede.

Arbejdsgivere skal bl.a. iagttage oplysningspligten i forbindelse med, at der iværksættes kontrolforanstaltninger over for medarbejderne, hvilket indebærer, at arbejdsgiveren skal give de ansatte information om behandlingen forud for, at kontrolforanstaltningen iværksættes. Informationen skal (udover at opfylde kravene efter forordningens artikel 13 eller artikel 14) gives i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog, således at den ansatte sættes i stand til at forstå de(n) pågældende kontrolforanstaltning(er), herunder særligt kontrolformålet. Datatilsynets skabelon til oplysningspligten skal i denne henseende ses som en vejledende skabelon, som skal tilrettes og eventuelt suppleres i forhold til den kontrolforanstaltning, som arbejdsgiveren ønsker at iværksætte. Oplysning om visse forhold kan efter omstændighederne undlades, hvis den ansatte allerede er bekendt med oplysningerne.

Arbejdsgiver vil efter omstændighederne ikke være forpligtet til forud at underrette den ansatte om en konkret kontrolforanstaltning, hvis oplysningspligten sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med kontrollen.

Der gælder en række undtagelser til den dataansvarliges oplysningspligt, hvorefter den dataansvarlige ikke er forpligtet til at opfylde oplysningsforpligtelsen for så vidt angår samtlige oplysninger. Det gælder bl.a., hvis det vurderes, at den registrerede allerede er bekendt med (en del af) de oplysninger, der skal gives.

Dette gælder også ved offentlige myndigheders behandling af oplysninger i forbindelse med f.eks. patientbehandling. Myndigheden vil dog, hvis den én gang har opfyldt oplysningspligten i forbindelse med patientbehandling, forholdsvis ofte kunne gå ud fra, at den registrerede allerede er bekendt med oplysningerne, medmindre behandlingens karakter har ændret sig, eller hvis det er længe siden, den registrerede har modtaget de pågældende oplysninger, som oplysningspligten foreskriver.

Oplysningspligten er i et vist omfang også begrænset i forhold til bipersoner, jf. forordningens artikel 14, stk. 5, litra b, hvorefter oplysningspligten bl.a. ikke finder anvendelse, hvis og i det omfang meddelelse af oplysningerne viser sig umulig eller vil kræve en uforholdsmæssig stor indsats.

Ved en biperson forstås en person, der ikke er genstand for behandlingen af personoplysninger, men derimod alene optræder accessorisk i tilknytning til oplysninger om den registrerede. Det kan f.eks. være pårørende til en registreret eller en fagperson som en læge eller lign. En

biperson er således en person, som alene har en perifer eller underordnet betydning i forhold til den behandling, som den dataansvarlige foretager.

Det er i forhold til behandling af personoplysninger ved brugen af sammenligningslejemål Datatilsynets umiddelbare vurdering, at oplysningspligten ofte vil kunne undlades i medfør af artikel 14, stk. 5, litra b, da personoplysningerne, efter det af EjendomDanmark oplyste, synes at være accessoriske i forhold til det formål, hvortil oplysningerne om sammenligningslejemålene behandles til.

For så vidt angår advokaters behandling af personoplysninger bemærkes, at i det omfang advokaten kommer i besiddelse af personoplysninger, som ikke er indsamlet fra den registrerede selv (modparten, vidner, skønsmænd mv.), skal det overvejes, om oplysningspligten i artikel 14, skal iagttages.

Det fremgår bl.a. af artikel 14, stk. 5, litra d, at oplysningspligten ikke finder anvendelse, hvis og i det omfang personoplysningerne skal forblive fortrolige som følge af tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret, herunder lovbestemt tavshedspligt. Undtagelsen finder bl.a. anvendelse i forhold til advokaters tavshedspligt, jf. retsplejelovens § 129. Oplysningspligten gælder derfor ikke, hvis oplysningspligten efter omstændighederne vil medføre en overtrædelse af advokatens tavshedspligt.

I det omfang oplysningspligten ikke kan undlades efter artikel 14, stk. 5, litra d, vil advokaten efter omstændighederne kunne undlade at opfylde oplysningspligten (eller en del heraf), hvis oplysningerne vedrører bipersoner, eller efter databeskyttelseslovens § 22, stk. 1 og 2, hvis oplysningspligten bør vige for afgørende hensyn til private eller offentlige interesser.

Foreninger kan som øvrige dataansvarlige undlade at opfylde oplysningspligten, hvis én eller flere af undtagelserne i databeskyttelsesforordningen eller –loven gør sig gældende. F.eks. vil foreninger kunne undlade at opfylde oplysningspligten, hvis og i det omfang den registrerede allerede er bekendt med oplysningerne, f.eks. hvis medlemmer har fået oplysningerne i forbindelse med indmeldelse.

Datatilsynet vil løbende offentliggøre afgørelser, som kan belyse omfanget af oplysningspligten, ligesom tilsynet arbejder på en opdatering af vejledningen om de registreredes rettigheder.

11. Retten til indsigt

Dansk Arbejdsgiverforening oplyser, at der blandt virksomheder er tvivl om omfanget af retten til indsigt, når nuværende eller tidligere medarbejdere anmoder om indsigt, herunder i hvilket omfang der skal udleveres arbejdsdokumenter og oplysninger om interne vurderinger.

Dansk Industri anfører, at det er uklart, hvilke oplysninger en medarbejder har ret til at få indsigt i, og hvilke dokumenter som er undtaget fra indsigtsretten. Mere konkret anfører **Dansk Industri**, at der særligt er tvivl om omfanget af undtagelserne i forordningens artikel 15, stk. 4, databeskyttelseslovens § 22, stk. 1, og udstrækningen af eksempel 2 i afsnit 4.2. i Datatilsynets vejledning om databeskyttelse i forbindelse med ansættelsesforhold (tidligere version fra november 2018) uden for de tilfælde, som er indeholdt i eksemplet.

EjendomDanmark oplyser, at retten til indsigt benyttes af de registrerede til at skaffe sig adgang til dokumenter, som den registrerede tidligere har modtaget, eller som den registrerede selv har fremsendt til den dataansvarlige, og dette gøres for at omgå andre regler, hvorefter den registrerede skal betale administrationsgebyr herfor. **EjendomDanmark** anfører endvidere, at der opbevares en stor mængde dokumenter om beboere, som f.eks. lejevarslinger og opkrævninger, hvoraf de samme personoplysninger fremgår. **EjendomDanmark** er i tvivl om, hvorvidt disse dokumenter skal udleveres, eller om det er tilstrækkeligt at udlevere oplysninger om, hvilke personoplysninger som behandles, og i hvilke sammenhæng oplysninger behandles.

Finans Danmark angiver, at der generelt er tvivl om årtier gamle transaktionsdata og kontoudtog kan undtages fra retten til indsigt, eller om indsigt skal gives i det samlede datamateriale gennem en livsalder. **Finans Danmark** oplyser i forhold hertil, at et kundeforhold kan strække sig over mange årtier. **Finans Danmark** anfører endvidere, at der savnes mere bevågenhed og klarhed i forhold til undtagelserne til retten til indsigt.

SMVdanmark ønsker afklaring af, hvornår og i hvilket omfang virksomheder kan kræve et gebyr, jf. forordningens artikel 15, stk. 3, hvis den registrerede ønsker at få udleveret oplysninger, som vedkommende allerede har fået en gang tidligere. **SMVdanmark** oplyser, at en medlemsvirksomhed i en opsigelsessituation modtog en anmodning om at få udleveret lønsedler fra 5 år tilbage på trods af, at disse oplysninger var modtaget tidligere, og at retten til indsigt generelt kan bruges af den registrerede i chikanøst øjemed i konfliktsituationer.

Reglerne om indsigt er ikke nye. De blev indført i dansk ret i forbindelse med, at den tidligere gældende persondatalov trådte i kraft den 1. juli 2000, men forordningen udvider med artikel 15 generelt omfanget af den information, som den dataansvarlige skal give den registrerede, herunder i henhold til bestemmelsens stk. 1, litra a-h.

Den registrerede har efter databeskyttelsesforordningens artikel 15 ret til at få den dataansvarliges bekræftelse på, om personoplysninger vedrørende den pågældende behandles, og i givet fald adgang til personoplysningerne og informationer om den dataansvarlige og dennes behandling af de pågældende personoplysninger. Om formålet med indsigtsretten fremgår det af databeskyttelsesforordningens præambelbetragtning nr. 63, at en registreret bør have ret til indsigt i personoplysninger, der er indsamlet om vedkommende, og til let og med rimelige mellemrum at udøve denne ret med henblik på at forvisse sig om og kontrollere en behandlings lovlighed.

Den dataansvarlige skal i forbindelse hermed udlevere en kopi af de personoplysninger, som behandles. Ønsker den registrerede yderligere kopier, kan den dataansvarlige opkræve et rimeligt gebyr herfor som baseres på de administrative omkostninger.

Det er indsigt i indholdet af de personoplysninger, som den dataansvarlige behandler, der skal udleveres. Dette kan gøres ved at udlevere kopier af originale dokumenter, sagsmapper, tv-overvågningsoptagelser, loggede teletrafikoplysninger mv. Den dataansvarlige kan dog også vælge at kopiere oplysningerne om den registrerede over i et nyt dokument eller lignende. Det vigtigste er, at den registrerede modtager en egentlig kopi af selve oplysningerne.

Kravet om kopi af oplysningerne, jf. forordningens artikel 15, stk. 3, kan ikke opfyldes ved, at der blot udleveres en liste over de personoplysninger, som den dataansvarlige behandler. Dette gælder, uagtet om personoplysninger går igen eller ej i de forskellige dokumenter. Der skal gives en egentlig kopi af de pågældende personoplysninger. Kravet kan eksempelvis opfyldes ved at give den registrerede fjernadgang til et sikkert system, som giver den registrerede direkte adgang til vedkommendes personoplysninger.

Retten til indsigt og til at modtage kopi af de personoplysninger, som behandles, skal være gratis, jf. databeskyttelsesforordningens artikel 12, stk. 5.

Er anmodninger åbenbart grundløse eller overdrevne, især fordi de gentages, kan den dataansvarlige enten opkræve et rimeligt gebyr eller afvise at efterkomme anmodningen, jf. artikel 12, stk. 5, 2. pkt. Anmodninger af chikanøs karakter vil ofte kunne anses for åbenbart grundløse. Der kan i øvrigt henvises til eksempel 1 og 2 i Datatilsynets vejledning om de registreredes rettigheder fra juli 2018.

Den registrerede har ret til at udøve retten til indsigt med rimelige mellemrum, og dette må indgå i vurderingen af, om der er tale om "gentagne" anmodninger, således at en anmodning f.eks. kan afslås.

Retten til indsigt gælder som udgangspunkt alle personoplysninger om den registrerede, som anmoder om indsigt, uanset om personoplysningerne er meget omfangsrige eller gamle. Den dataansvarlige kan bede den registrerede præcisere anmodningen i forhold til år, dato, indhold eller lignende, men den dataansvarlige må som udgangspunkt ikke afvise den registreredes anmodning, hvis den registrerede ikke ønsker at præcisere anmodningen.

I forhold til medarbejdere gælder indsigtsretten f.eks. indsigt i og kopi af bl.a. dokumenter på en personalesag, vagtplaner, telefonoptagelser, videoovervågninger, medarbejderudviklingssamtaler, korrespondance med den registrerede, personoplysninger fra et intranet mv.

For så vidt angår interne vurderinger mv., som vedrører medarbejderen, kan hensynet til f.eks. en arbejdsgivers forhandlingsposition i forbindelse med lønforhandlinger og hensynet til generelle forhold på arbejdspladsen, herunder forholdet mellem arbejdsgiver og den ansatte, imidlertid efter omstændighederne begrunde, at retten til indsigt ikke gælder, jf. databeskyttelseslovens § 22, stk. 1. En arbejdsgiver kan endvidere som udgangspunkt undtage dokumenter, som er udarbejdet af den pågældende medarbejder som led i dennes arbejde under hensyn til bl.a. arbejdsgiverens forretningsgrundlag.

Det følger af forordningens artikel 15, stk. 4, at retten til at modtage kopi ikke må krænke andres rettigheder og frihedsrettigheder. Hertil kommer bestemmelserne i databeskyttelseslo-

vens § 22 om begrænsning af retten til bl.a. indsigt, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private eller offentlige interesser.

Den registreredes ret kan bl.a. begrænses, hvis indsigt vil krænke andres (private eller virksomheder) rettigheder eller frihedsrettigheder, som f.eks. forretningshemmeligheder eller intellektuel ejendomsret.

Den registrerede har ikke i forbindelse med en anmodning efter artikel 15 ret til at få indsigt i personoplysninger om andre end den pågældende selv. Efter omstændighederne kan dette indebære, at dokumenter helt undtages, hvis dokumenterne indeholder oplysninger om andre, jf. hhv. forordningens artikel 15, stk. 4, eller databeskyttelseslovens § 22. Dette vil normalt kun kunne komme på tale, hvis den registrerede, som anmoder om indsigt, må anses for at være biperson i forhold til de pågældende dokumenter.

Endelig kan indsigtsretten i forhold til oplysninger, der behandles for den offentlige forvaltning som led i administrativ sagsbehandling, også begrænses i samme omfang som efter §§ 19-29 og 35 i lov om offentlighed i forvaltningen, jf. databeskyttelseslovens § 22, stk. 3.

12. Forskning

Danske Regioner anfører, at kravet om et behandlingsgrundlag ofte giver anledning til usikkerhed i forbindelse med forskningsprojekter, herunder hvornår personoplysninger i forskningsprojekter behandles på baggrund af et databeskyttelsesretligt samtykke eller med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, eller databeskyttelseslovens § 10. Det er ifølge **Danske Regioner** endvidere uklart, om der kan ske skift af behandlingsgrundlag, f.eks. hvis oplysningerne er indhentet med samtykke i forbindelse med en spørgeskemaundersøgelse, og man senere ønsker at skifte til databeskyttelsesforordningens artikel 6, stk. 1, litra e, eller databeskyttelseslovens § 10. Herudover ønsker **Danske Regioner** oplyst, om oplysninger, som er indhentet med hjemmel i sundhedslovens § 46, og som ønskes videregivet fra ét forskningsprojekt til et andet, kan videregives med hjemmel i databeskyttelseslovens § 10, eller om videregivelsen skal ske med fornyet hjemmel i sundhedsloven, og om der i den forbindelse skal sondres mellem rådata og berigede data fra patientjournalen.

Enhver behandling af personoplysninger kræver, at den dataansvarlige har et lovligt behandlingsgrundlag. Behandling af personoplysninger kan som udgangspunkt altid ske, hvis den dataansvarlige har fået samtykke fra den registrerede, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra a og artikel 9, stk. 2, litra a.

Særligt i forbindelse med forskning er det vigtigt ikke at forveksle samtykke til at behandle personoplysningerne med krav om samtykke, som følger af eventuel anden lovgivning. Det kan følge af anden lovgivning, at der kræves "samtykke", men dette samtykke er ikke ensbetydende med, at der er givet et samtykke i databeskyttelsesretlig forstand. Et sådant "samtykke" vil ofte udgøre en garantiforskrift for borgerne, men er ikke nødvendigvis grundlaget for behandlingen af personoplysningerne.

For yderligere information om gyldighedsbetingelserne for et samtykke kan Datatilsynet henvise til tilsynets vejledning om samtykke. Datatilsynet kan endvidere oplyse, at tilsynet i samarbejde med Sundhedsministeriet forventer at udarbejde en vejledning vedrørende forskellige former for samtykke i forbindelse med sundhedsvidenskabelig forskning.

Ud over samtykke findes der andre behandlingsgrundlag, og hvis behandlingen kan baseres på et andet behandlingsgrundlag, behøver man ikke at indhente et databeskyttelsesretligt samtykke. Personoplysninger kan bl.a. behandles, hvis behandlingen af oplysningerne er nødvendig for at udføre en opgave i samfundet interesse, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra e. Behandling af særlige kategorier af oplysninger, f.eks. helbredsoplysninger, er som udgangspunkt ikke lovlig, jf. databeskyttelsesforordningens artikel 9, stk. 1. Særlige kategorier af oplysninger må imidlertid ifølge databeskyttelseslovens § 10, jf. forordningens artikel 9, stk. 2, litra j, behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelsen.

I forbindelse med forskningsprojekter, hvori der indgår helbredsoplysninger eller andre følsomme oplysninger omfattet af forordningens artikel 9, vil databeskyttelseslovens § 10 oftest være det mest hensigtsmæssige behandlingsgrundlag. Databeskyttelseslovens § 10, stk. 1 og 2 – og de næsten tilsvarende bestemmelser i den tidligere gældende persondatalov – hviler på en forudsætning om, at behandlingen af personoplysninger sker på en ansvarlig måde, her-

under at behandlingen er underlagt fornødne garantier for registreredes rettigheder og frihedsrettigheder, jf. databeskyttelsesforordningens artikel 89.

Den dataansvarlige må på forhånd overveje, hvilket behandlingsgrundlag der er relevant og hensigtsmæssigt at benytte i forbindelse med det konkrete projekt. Det er vigtigt, at den dataansvarlige på forhånd nøje foretager denne overvejelse, bl.a. fordi et skift af behandlingsgrundlag ikke altid er muligt. Eksempelvis er det som udgangspunkt ikke muligt at skifte fra (databeskyttelsesretligt) samtykke til et andet behandlingsgrundlag, da et samtykke efter databeskyttelsesforordningen er udtryk for, at den registrerede gives et reelt valg og kontrol over, hvordan vedkommendes personoplysninger behandles, og det derfor ikke er rimeligt over for den registrerede, hvis behandlingsgrundlaget ændres.

For så vidt angår spørgsmålet om sundhedslovens § 46 er det ud fra bestemmelsens ordlyd Datatilsynets umiddelbare forståelse, at bestemmelsen sætter rammer for, hvornår sundhedsvæsnet kan videregive personoplysninger. Når den dataansvarlige for et forskningsprojekt modtager oplysningerne, skal denne som beskrevet ovenfor vurdere, hvilket behandlingsgrundlag den dataansvarlige kan benytte som grundlag for behandling af oplysningerne. I den forbindelse vil det som nævnt ovenfor være naturligt at tage udgangspunkt i databeskyttelseslovens § 10.

Danske Universiteter anfører, at det er uklart, hvorvidt man skal have tilladelse til videregivelse af oplysninger omfattet af databeskyttelseslovens artikel 6, eftersom lovens § 10, stk. 3, henviser til "oplysninger omfattet af stk. 1 og 2", og § 10, stk. 2, både omfatter oplysninger i forordningens artikel 6, 9 og 10. **Danske Universiteter** anfører endvidere, at der er tvivl om, hvordan begrebet "tredjemand" i § 10, stk. 3, skal forstås, herunder hvorvidt en deltager i et forskningssamarbejde uden fælles dataansvar er en "tredjemand", og der derfor ikke skal indhentes tilladelse til videregivelse til andre universiteter eller forskningsinstitutioner, som indgår i et forskningssamarbejde, som omfatter de omhandlede oplysninger.

Kræftens Bekæmpelse bemærker, at Danmark er forpligtet til at fortolke databeskyttelsesforordningens artikel 1, stk. 3, således, at den gælder hele EØS og ikke kun EU, og der bør derfor ikke være nogen begrænsninger for eksempelvis overførsel til Norge eller Island.

Det følger af databeskyttelseslovens § 10, stk. 3, at videregivelse af oplysninger omfattet af bestemmelsens stk. 1 og 2 til tredjemand kræver forudgående tilladelse fra tilsynsmyndigheden, når videregivelsen

1) *sker til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde, jf. databeskyttelsesforordningens artikel 3,*
2) *vedrører biologisk materiale eller*
3) *sker med henblik på offentliggørelse i et anerkendt videnskabeligt tidsskrift el.lign.*

Databeskyttelseslovens § 10, stk. 3, indebærer, at den dataansvarlige i de nævnte tilfælde skal have forudgående tilladelse fra Datatilsynet, hvis den dataansvarlige har behandlet oplysningerne med hjemmel i lovens § 10, stk. 1, og ønsker at videregive oplysningerne med henblik på behandling i overensstemmelse med § 10, stk. 2. Hvis der alene er tale om videregivelse af personoplysninger omfattet af databeskyttelsesforordningens artikel 6, vil videregivelsen ikke være omfattet af tilladelseskravet.

Det følger af databeskyttelsesforordningens artikel 4, stk. 1, nr. 10, at "tredjemand" er en anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarlige eller databehandlerens direkte myndighed, der er beføjet til at behandle personop-

lysninger. Begrebet "tredjemand" i databeskyttelsesloven må fortolkes i overensstemmelse hermed.

En tredjemand kan således være alle udenforstående, som bliver selvstændig dataansvarlig for oplysningerne. Hvis et universitet indgår i et forskningssamarbejde med et andet universitet, og det andet universitet anses for selvstændig dataansvarlig, vil der være tale om en videregivelse til tredjemand, som kræver Datatilsynets tilladelse i de i § 10, stk. 3, nr. 1-3, nævnte tilfælde.

Som følge af databeskyttelseslovens § 10, stk. 3, nr. 1, skal Datatilsynet give tilladelse, når videregivelsen sker til behandling uden for databeskyttelsesforordningens territoriale anvendelsesområde, jf. databeskyttelsesforordningens artikel 3.

Efter spørgsmålet har været forelagt EU-Kommissionen og Justitsministeriet er det (nu) Datatilsynets opfattelse, at databeskyttelsesforordningens artikel 3, stk.1, skal fortolkes således, at forordningen gælder for såvel EU-lande som EØS-lande, hvilket indebærer, at videregivelse til EØS-lande ikke længere vil kræve Datatilsynets forudgående tilladelse.

Danske Universiteter foreslår, at der udarbejdes standardkontrakter for videregivelse og overladelse af forskningsdata til universiteter i usikre tredjelande.

Det er Datatilsynets forståelse, at EU-Kommissionens nye standardkontrakter bliver mere anvendelige i forbindelse med overførsel af personoplysninger til et (usikkert) tredjeland i forbindelse med forskning.

Kræftens Bekæmpelse anfører, at rollefordelingen i forskningsmæssige samarbejder er vanskelig, og at vurderingen af dataansvar bliver yderligere kompliceret af, at forskere i forbindelse med sager om påstået videnskabelig uredelighed skal kunne stille rådata til rådighed, hvilket udelukker rollen som databehandler, da parten vil skulle råde over data til eget formål. Vurderingen ender derfor ofte med at være, at der er fælles dataansvar, hvilket er kompliceret i forhold til bl.a. oplysningspligten.

Danske Regioner anfører, at der er tvivl om, hvad der helt konkret skal til for at klarlægge ansvarsfordelingen mellem parterne i forbindelse med fælles dataansvar og i hvor høj grad en region kan risikere kritik og bøder, hvis den anden part ikke lever op til sine forpligtelser.

Danske Universiteter oplyser, at hvis der er tale om længerevarende databehandlerkonstruktioner, skal universiteterne – som dataansvarlige – kontrollere, at databehandleren fortsat lever op til de aftalte sikkerhedskrav. Denne kontrol kan være bekostelig, hvis kontrollen gennemføres af en uvildig tredjepart. **Danske Universiteter** oplyser endvidere, at der er tilbageholdenhed med at indgå i fælles dataansvar, og at der er behov for flere retningslinjer på området. **Danske Universiteter** forespørger, i hvilket omfang det er muligt at anvende fælles dataansvar i forbindelse med forskningssamarbejder, hvor der deltager universiteter fra usikre tredjelande. Datatilsynet har på et møde oplyst, at det er lovligt at inddrage universiteter i usikre tredjelande i et fælles dataansvar, hvis en konkret risikovurdering fører til, at det er forsvarligt.

En dataansvarlig er den fysiske eller juridiske person, offentlige myndighed mv., der bestemmer, med hvilke formål personoplysningerne må behandles (formålet), og hvordan personoplysningerne må behandles (hjælpemidlerne), jf. databeskyttelsesforordningens artikel 4, stk. 1, nr. 7.

En databehandler er derimod en fysisk eller juridisk person, offentlig myndighed mv., der behandler personoplysninger på vegne af den dataansvarlige, jf. databeskyttelsesforordningens artikel 4, stk. 1, nr. 8. Databehandleren bestemmer i modsætning til den dataansvarlige hverken hvordan eller med hvilke formål, der må behandles personoplysninger, og databehandleren behandler således oplysningerne efter den dataansvarliges instruks.

Det er således afgørende for vurderingen at fastlægge, hvem der reelt bestemmer formål og hjælpemidler for behandlingen af oplysningerne. Det kan være behjælpeligt at se det som en vurdering af, hvem der reelt har kontrollen med oplysningerne og således kan bestemme, hvad der skal ske med oplysningerne, f.eks. om oplysningerne skal slettes eller videregives. Hvis det viser sig, at begge parter i forbindelse med den pågældende behandling kan bestemme disse væsentlige sagsbehandlingsskridt, kan der i stedet for en databehandlerkonstruktion være tale om to selvstændige dataansvarlige, eller efter omstændighederne fælles dataansvar.

I det omfang der er tale om en databehandlerkonstruktion, skal der indgås en databehandleraftale. Den dataansvarlige må endvidere føre et (større eller mindre) tilsyn med databehandleren for at sikre, at den indgåede databehandleraftale overholdes, herunder de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Datatilsynet bemærker i den forbindelse, at den dataansvarlige kan vælge at lade kontrollen udføre af en uvildig tredjepart, men at det ikke er et krav. Den dataansvarlige kan således udføre kontrollen selv, hvilket kan være en fordel, da den dataansvarlige ofte har bedre kendskab til de konkret aftalte foranstaltninger og således ved, hvad det vil være relevant at påse i forbindelse med et tilsyn.

Ved vurderingen af, hvilke roller de forskellige parter har, kan det i nogle tilfælde være relevant at overveje, om der foreligger fælles dataansvar, jf. databeskyttelsesforordningens artikel 26, stk. 1.

Hvis to eller flere parter i fællesskab bestemmer, hvorfor der skal behandles personoplysninger (formålet), og hvordan der skal behandles personoplysninger (hjælpemidlerne), er de fælles dataansvarlige for behandlingen. Fælles dataansvar kan altså kun komme på tale, hvis en dataansvarlig og en eller flere andre parter sammen har ansvaret for en behandling, og hvis de alle har ret til at bruge oplysningerne til egne formål. Der er altså ikke tale om et fælles dataansvar, hvis en behandling kun foretages til den ene parts formål.

Hvis man vurderer, at der er tale om fælles dataansvar, skal de dataansvarlige på en gennemsigtig måde fastlægge deres respektive ansvar for overholdelse af de forpligtelser, som følger af databeskyttelsesreglerne, navnlig hvad angår udøvelsen af de registreredes rettigheder. De dataansvarlige skal således sammen lave en aftale og fordele forpligtelserne i forbindelse med overholdelse af databeskyttelsesreglerne. Hensynet bag reglerne er at sikre, at de dataansvarlige ikke bare forventer, at en anden dataansvarlig opfylder forpligtelserne med den konsekvens, at databeskyttelsesreglerne slet ikke iagttages.

Den aftalte og "interne" ansvarsfordeling mellem de dataansvarlige ændrer imidlertid ikke på, at de dataansvarlige – over for de registrerede – er fælles ansvarlige for hele behandlingen. De personer, der behandles oplysninger om, kan derfor stadig henvende sig til enhver af de dataansvarlige for at udøve deres rettigheder, f.eks. indgive en klage eller en anmodning om indsigt.

Fælles dataansvar indebærer grundlæggende, at man har et fælles ansvar, hvorfor man også bør forsikre sig om, at den anden part iagttager sine ansvarsområder. Hvorvidt man kan blive genstand for bøde eller kritik, hvis en anden dataansvarlig i det fælles dataansvar ikke lever op til sine forpligtelser, må bero på en konkret vurdering, hvor der bl.a. ses på indholdet af aftalen, herunder hvor detaljeret ansvarsfordelingen er, og hvordan parterne har handlet i overensstemmelse med aftalen.

Datatilsynet anser det ikke i sig selv for problematisk, at en dansk dataansvarlig indgår i et fælles dataansvar med f.eks. et universitet i et usikkert tredjeland. Man skal imidlertid have et overførselsgrundlag, jf. forordningens kap. V, hvis oplysninger overføres til en dataansvarlig i et usikkert tredjeland.

Datatilsynet er opmærksom på, at det kan være vanskeligt at vurdere roller og ansvar i forbindelse med forskningsprojekter, og tilsynet vil derfor i sit arbejde med vejledninger på området bl.a. have fokus på dataansvar og roller i forbindelse med forskningsprojekter.

Danske Universiteter anfører, at der er forskellige fortolkninger af præambelbetragtning nr. 26, og at andre universiteter i Europa ikke betragter pseudonymiserede oplysninger som personoplysninger hos modtageren/databehandleren, idet pseudonymiseringsnøglen ikke er tilgængelig hos modtageren/databehandleren. Dette støttes på EU-Domstolens dom C582/14, Patrick Breyer. **Danske Universiteter** bemærker, at modtagererklæringer eller databehandleraftaler ikke har betydning for den registreredes rettigheder eller frihedsrettigheder, når der alene videregives eller overlades pseudonymiserede oplysninger, da oplysningerne ikke kan misbruges uden adgang til pseudonymiseringsnøglen.

Danske Regioner anfører, at det er vanskeligt at vurdere, hvornår oplysninger er tilstrækkeligt anonymiserede, således at databeskyttelsesreglerne ikke længere finder anvendelse.

Kræftens Bekæmpelse forespørger, om det er muligt at anonymisere oplysninger, f.eks. biologisk materiale, som anvendes i sundhedsvidenskabelige forskningsprojekter, herunder, jf. præambelbetragtning nr. 26, hvornår de givne foranstaltninger, der ville skulle iværksættes for at kunne identificere en fysisk person, vil være så avancerede eller kræve så stor ekspertise, at de vil være ud over det, man med rimelighed vil kunne iværksætte, og man dermed kan betragte oplysningerne som anonymiserede.

I databeskyttelsesretten skelnes der mellem pseudonymisering og anonymisering. Pseudonymisering defineres som behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person.

Det er væsentligt at holde sig for øje, at behandling af pseudonymiserede personoplysninger er omfattet af databeskyttelsesreglerne, idet oplysningerne fortsat kan henføres til en fysisk person ved brug af de supplerende oplysninger. Anvendelsen af pseudonymisering kan imidlertid gøre det lettere for dataansvarlige og databehandlere at opfylde deres databeskyttelsesforpligtelser samt mindske risikoen for de registrerede.

Oplysninger, der er gjort anonyme, sådan at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger, er imidlertid ikke beskyttet af databeskyttelsesreglerne, idet der ikke længere vil være tale om personoplysninger.

Vurderingen af, om oplysninger er anonymiserede og således falder uden for reglernes anvendelsesområde, afhænger af, om det er muligt at identificere en fysisk person ud fra oplysningerne. For at afgøre, om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende. For at fastslå, om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning, såsom omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling, jf. databeskyttelsesforordningens præambelbetragtning nr. 26.

Ved vurderingen må man derfor overveje, hvilke midler der kan benyttes for at identificere de fysiske personer, oplysningerne omhandler. Her kan det bl.a. overvejes, om oplysningerne kan kombineres med andre oplysninger, eksempelvis hvis ét datasæt kan kombineres med et andet datasæt, som medfører, at ét eller flere individer kan identificeres.

Herefter må det overvejes, om midlerne med rimelighed kan tænkes bragt i anvendelse. Muligheden for at kombinere oplysningerne med supplerende oplysninger kan eksempelvis ikke betragtes som et rimeligt hjælpemiddel, hvis det ville være ulovligt for indehaveren af de supplerende oplysninger at give oplysningerne til den dataansvarlige.

I forbindelse med store datasæt, som anvendes i forbindelse med forskning, må det efter Datatilsynets opfattelse umiddelbart antages at være vanskeligt at anonymisere oplysningerne på en sådan måde, at databeskyttelsesreglerne ikke længere finder anvendelse, uden at datasættet ikke samtidig mister sin værdi.

Det er endvidere Datatilsynets forståelse, at der på nuværende tidspunkt ikke er påvist en kombination af teknologiske og organisatoriske midler, som effektivt kan anvendes for at udelukke biologisk materiale fra databeskyttelsesforordningens anvendelsesområde.

Datatilsynet anser de angivne problemstillinger for yderst relevante, og tilsynet er også bevidst om, at det kan være svære vurderinger at foretage. Datatilsynet har derfor til hensigt at udarbejde en vejledning om anonymisering og pseudonymisering. Endvidere pågår der i regi af Det Europæiske Databeskyttelsesråd (EDPB) for tiden et arbejde – som Datatilsynet deltager aktivt i – om udarbejdelse af en vejledning om behandling af personoplysninger i forbindelse med forskning, hvor det forventes, at spørgsmålet om pseudonymisering og anonymisering vil blive inddraget.

Kræftens Bekæmpelse anfører, at det ikke er hensigtsmæssigt, at dataansvarlige skal navigere gennem et meget komplekst regelsæt, der som udgangspunkt giver forsøgspersoner i videnskabelige forskningsprojekter en række rettigheder, men som de facto kan vise sig at være meget beskedne eller helt uden indhold. **Kræftens Bekæmpelse** angiver, at forskningslivet har behov for lempelse af oplysningspligten. **Kræftens Bekæmpelse** forespørger, om man skal opfylde oplysningspligten i artikel 13 eller 14, når oplysninger oprindeligt er indhentet fra én dataansvarlig, og der efterfølgende vurderes at være tale om fælles dataansvar, og om man kan bruge undtagelsesbestemmelsen i artikel 14, stk. 5, litra b, i den forbindelse.

Danske Universiteter oplyser, at den samfundsvidenskabelige og humanistiske forskning i stigende grad anvender data fra sociale medier, og at det i den forbindelse ikke giver mening at overholde oplysningspligten, hvis der f.eks. er tale om debatindlæg på Twitter fra statsoverhoveder i andre lande. **Danske Universiteter** forespørger i den forbindelse, om forskning i

indlæg på sociale medier kan undtages fra reglerne om oplysningspligt med afsæt i forordningens artikel 85, da artikel 85 specifikt nævner akademisk virksomhed.

Den registrerede har efter databeskyttelsesforordningens artikel 13-22 en række rettigheder, herunder retten til indsigt samt retten til berigtigelse og sletning. Rettighederne i databeskyttelsesforordningen indebærer, at den registrerede kan udøve en vis kontrol med behandlingen af personoplysninger, som vedrører den pågældende.

Den dataansvarlige kan kun undlade at imødekomme en anmodning fra den registrerede om f.eks. indsigt eller sletning, hvis der er en relevant undtagelse i databeskyttelsesforordningen eller databeskyttelsesloven. I forbindelse med behandling af personoplysninger i videnskabeligt eller statistisk øjemed findes der flere undtagelser til de registreredes rettigheder, jf. databeskyttelseslovens § 22, stk. 5, og databeskyttelsesforordningens artikel 17, stk. 3, litra d.

Den dataansvarlige skal imidlertid altid overveje, om den konkrete anmodning kan imødekommes, og herefter besvare anmodningen, samt imødekomme anmodningen, hvis ingen af undtagelsesbestemmelserne finder anvendelse.

Hvis personoplysninger ikke er indsamlet hos den registrerede, jf. artikel 14 – eksempelvis hvis oplysningerne er indsamlet via offentligt tilgængelige kilder – kan det i forbindelse med forskning være relevant at overveje, om oplysningspligten kan undlades som følge af artikel 14, stk. 5, litra b.

Det følger af artikel 14, stk. 5, litra b, at artikel 14, stk. 1-4, ikke finder anvendelse, hvis og i det omfang meddelelse af sådanne oplysninger viser sig umulig eller vil kræve en uforholdsmæssigt stor indsats, navnlig i forbindelse med behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål underlagt de betingelser og garantier, der er omhandlet i artikel 89, stk. 1, eller i det omfang den forpligtelse, der er omhandlet i nærværende artikels stk. 1, sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med denne behandling. I sådanne tilfælde træffer den dataansvarlige passende foranstaltninger for at beskytte den registreredes rettigheder og frihedsrettigheder samt legitime interesser, herunder ved at gøre informationerne offentligt tilgængelige.

Ved ovenstående vurdering kan man tage hensyn til antallet af registrerede, oplysningernes alder og eventuelle fornødne garantier, der er stillet, jf. forordningens præambelbetragtning nr. 62.

Det følger af databeskyttelsesforordningens artikel 85, stk. 1, at medlemsstaterne ved lov forener retten til beskyttelse af personoplysninger i henhold til denne forordning med retten til ytrings- og informationsfrihed, herunder behandling i journalistisk øjemed og med henblik på akademisk, kunstnerisk eller litterær virksomhed. Af bestemmelsens stk. 2 fremgår det, at medlemsstaterne fastsætter undtagelser til behandling i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed eller fravigelser fra bl.a. forordningens kapitel III, om de registreredes rettigheder.

Bestemmelsen giver mulighed for at fastsætte undtagelser til bl.a. oplysningspligten, hvis det er nødvendigt for at forene retten til beskyttelse af personoplysninger med retten til ytrings- og informationsfrihed, og dette nationale råderum er i Danmark udmøntet i databeskyttelseslovens § 3. Det er Datatilsynets umiddelbare opfattelse, at artikel 85 ikke giver mulighed for at fastætte nationale undtagelser til oplysningspligten i forbindelse med forskning i debatindlæg fra sociale medier.

For så vidt angår spørgsmålet om, hvorvidt man skal opfylde oplysningspligten igen, hvis man senere vurderer, at der er tale om fælles dataansvar, kan Datatilsynet oplyse, at hvis der sker et skift i den dataansvarliges identitet, er det Datatilsynets umiddelbare opfattelse, at den registrerede skal orienteres herom som følge af artikel 13 og 14 og ud fra et synspunkt om gennemsigtighed. Hvis man allerede har opfyldt oplysningspligten i artikel 14, er det endvidere som udgangspunkt svært at se, at det skulle være uforholdsmæssigt eller kræve en uforholdsmæssig stor indsats, jf. artikel 14, stk. 5, litra b, at oplyse den registrerede om identitetsskiftet hos den dataansvarlige.

Datatilsynet kan oplyse, at de registreredes rettigheder i forbindelse med forskning er et af de emner, som Datatilsynet forventer at behandle i forbindelse med tilsynets vejledningsarbejde på forskningsområdet.

13. Arkivering

Danske Arkiver anfører, at der helt overordnet savnes en tilkendegivelse af, hvad begrebet "arkivformål i samfundets interesse" dækker over. **Danske Arkiver** anfører i den forbindelse, at mens det synes rimeligt klart, at offentlige arkiver kan modtage personoplysninger til opbevaring, er det uklart, hvordan disse personoplysninger senere kan benyttes.

Det kan ikke udledes af databeskyttelsesforordningen, hvad der skal forstås ved "arkivformål i samfundets interesse" og derved den nærmere rækkevidde af dette begreb i databeskyttelsesforordningens artikel 9, stk. 2, litra j, og artikel 89.

Det fremgår imidlertid af Justitsministeriets betænkning nr. 1565/2017, at den tidligere gældende forudsætning for forholdet mellem persondataloven og arkivlovens regler vil kunne videreføres inden for rammerne af forordningens artikel 89, stk. 1, jf. artikel 9, stk. 2, litra j. Datatilsynet kan i den forbindelse henvise til Registerudvalgets betænkning nr. 1345/1997 og bemærkningerne til persondataloven, hvoraf det fremgår, at den tidligere forudsætning var, at spørgsmålet om arkivmæssig anvendelse af personoplysninger skulle afgøres efter arkivlovgivningens regler herom, og dermed ikke efter reglerne i (den daværende) registerlov og persondatalov.

Fastlæggelsen af den nærmere rækkevidde af begrebet "arkivformål i samfundets interesse" må efter Datatilsynets opfattelse således bero på arkivlovgivningen og arkivmyndighedernes vurdering.

Rigsarkivet oplyser, at arkivet oplever usikkerhed om konsekvensen af persondatareglerne i forhold til ikke-offentlige arkivers bevaring af persondata.

Ikke-offentlige arkiver (lokalarkiver) ses – uanset deres organisationsform eller finansiering – ikke at være omfattet af arkivlovgivningen, da det kun er de offentlige arkivers virksomhed, der direkte er reguleret i denne lovgivning. Det betyder bl.a., at de særlige regler om arkivers behandling af personoplysninger ikke gælder for lokalarkiverne. Dette var også tilfældet, før databeskyttelsesforordningen fandt anvendelse.

Lokalarkiverne skal således overholde de databeskyttelsesretlige regler i forbindelse med enhver behandling af personoplysninger til arkivformål. For at overholde databeskyttelsesreglerne skal lokalarkiverne bl.a. kunne identificere et lovligt grundlag for behandling af personoplysninger i databeskyttelsesforordningens artikel 6, stk. 1, for behandling af personoplysninger til arkivformål.

Efter databeskyttelsesforordningens artikel 6, stk. 1, vil behandling af personoplysninger bl.a. kunne ske, hvis den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål (litra a), eller hvis behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn (litra f).

Hvis lokalarkiverne behandler personoplysninger på baggrund af interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f, vil lokalarkiverne skulle foretage en konkret afvejning mellem arkivformålet over for hensynet til den registrerede. Afgørende for en så-

dan afvejning er, at hensynet til den registrerede ikke overstiger lokalarkivernes legitime interesse i behandlingen af personoplysninger. Ved afvejningen kan lokalarkiverne bl.a. lægge vægt på materialets alder og karakteren af oplysningerne heri. Hvis der er tale om følsomme oplysninger, skal man tillige kunne identificere en undtagelse til forbuddet imod behandling af sådanne oplysninger, jf. databeskyttelsesforordningens artikel 9, stk. 2.

Lokalarkiverne skal også (løbende) overveje, hvilke personoplysninger det er nødvendigt at bevare.

Databeskyttelsesforordningen udelukker således ikke eksistensen af lokalarkiver, og det vil være muligt inden for forordningens og databeskyttelseslovens rammer fortsat at finde grundlag for at bevare materiale fra borgere, organisationer og virksomheder i lokalarkiver.

Endelig skal Datatilsynet pege på muligheden for at ændre arkivlovgivningen – alternativt udarbejde en særskilt lov omfattende private arkiver – hvorved arkivernes aktiviteter vil kunne reguleres af særlige regler om behandling af personoplysninger til arkivformål.

Rigsarkivet anfører, at rækkevidden af databeskyttelsesforordningens artikel 17, stk. 1 (retten til at blive glemt), er uklar – herunder i forhold til undtagelsesbestemmelser i artikel 17, stk. 3, og betydningen heraf bl.a. i forhold til vejledning af myndigheder om adgang til at slette personoplysninger inden aflevering.

Spørgsmålet om, hvorvidt behandling (opbevaring) af oplysninger er nødvendig til arkivformål i samfundets interesse, skal afgøres efter arkivlovgivningens regler. Hvis det følger heraf, at oplysninger er bevaringsværdige og skal afleveres til arkiv, kan en myndighed efter omstændighederne afvise en anmodning om sletning under henvisning til artikel 17, stk. 3, litra d.

Rigsarkivet forespørger, hvorfor den registreredes ret til indsigelse (modsætte sig arkivering) efter databeskyttelsesforordningens artikel 21 ikke er omfattet af undtagelserne i databeskyttelseslovens § 22, stk. 5.

Datatilsynet er ikke bekendt med, hvorfor arkivmæssige formål ikke er medtaget i undtagelsesbestemmelsen i databeskyttelseslovens § 22, stk. 5. Datatilsynet bemærker, at indsigelse mod behandling til videnskabelige eller historiske forskningsformål eller statistiske formål efter omstændighederne kan afskæres i medfør af artikel 21, stk. 6, hvis behandlingen er nødvendig for at udføre en opgave i samfundets interesse.

Rigsarkivet oplyser, at der som følge af vejledning om videregivelse fra Datatilsynet er opstået modstand hos en myndighed om Rigsarkivets ret til at forestå udlevering af afleveret data fra en myndighed. **Rigsarkivet** anfører i den forbindelse, at der er tvivl om, hvorvidt Datatilsynet har inddraget forbindelsen til arkivloven, da vejledningen om videregivelse blev udarbejdet.

Datatilsynet forudsætter, at tvivlen vedrører Datatilsynets vejledning til bekendtgørelse nr. 1509 af 18. december 2019 om videregivelse af personoplysninger omfattet af databeskyttelseslovens § 10, stk. 1 og 2.

Udlevering af oplysninger fra arkiv vil som udgangspunkt ikke være omfattet af databeskyttelseslovens § 10, men derimod af arkivlovens regler. Datatilsynet kan på den baggrund ikke umiddelbart se, hvilken relevans den omhandlede vejledning kan have for udlevering fra arkiv.

Rigsarkivet oplyser, at arkivet ofte oplever, at forskere lover respondenter, at data ikke kommer videre. Når data skal anmeldes (og afleveres) til Rigsarkivet, oplever forskerne aflevering som stridende mod deres aftale med respondenterne, bl.a. fordi data efter 20 eller 75 år bliver tilgængelige i henhold til gældende frister.

Datatilsynet kan ikke udtale sig om forskeres pligt til at anmelde og aflevere oplysninger til Rigsarkivet, da denne forpligtelse ses at følge af arkivlovgivningen.

Som udgangspunkt anbefaler Datatilsynet imidlertid, at der ikke foretages forskning på baggrund af et databeskyttelsesretligt samtykke, men at forskningsprojekter så vidt muligt baserer sig på databeskyttelseslovens § 10, som ikke forudsætter samtykke fra den registrerede.

Hvis en forsker vælger at foretage sin forskning på baggrund af et databeskyttelsesretligt samtykke, er det op til forskeren – som den dataansvarlige – ved indhentelse af samtykket at sikre, at de registrerede informeres fyldestgørende om, hvad oplysningerne vil kunne blive anvendt til, herunder at oplysningerne på sigt – på baggrund af reglerne i arkivloven – vil blive overleveret til Rigsarkivet, og at de herefter vil være tilgængelige for offentligheden efter 20 eller 75 år.

14. Diverse spørgsmål

14.1 Ansættelse og fagforening

Dansk Arbejdsgiverforening mener, at det bør klarlægges, hvordan straffeattester tilvejebringes i forbindelse med ansættelsesforhold, hvor løbende indhentelse af straffeattester er en forudsætning for ansættelse. Brugen af samtykke opleves som problematisk, idet det ikke må have negativ effekt på ansættelsen, hvis den ansatte afviser at give sit samtykke til indhentelsen.

Arbejdsgivere kan have et velbegrundet behov for at indhente oplysninger om ansattes strafbare forhold under ansættelsesforholdet som følge af f.eks. stillingens karakter.

En arbejdsgiver må imidlertid kun anmode om eller indhente oplysninger om en ansøgers eventuelle strafbare forhold, hvis det er relevant i forhold til den stilling, som den pågældende bestrider. Dette skal forstås således, at det i forhold til den konkrete stilling – i overensstemmelse med principperne i databeskyttelsesforordningens artikel 5 – skal være sagligt og proportionalt, at arbejdsgiveren indhenter eller anmoder om oplysninger om den ansattes strafbare forhold under ansættelsen.

Datatilsynet behandler for tiden spørgsmålet om behandling af personoplysninger i forbindelse med indhentelse af straffeattester ved ansættelse og under ansættelsesforholdet i forbindelse med en konkret sag, som tilsynet har indledt af egen drift. Resultatet forventes offentliggjort senere i år.

Datatilsynet bemærker i øvrigt, at på politiets hjemmeside, www.politi.dk, findes oplysninger om samtykke og fremgangsmåden ved indhentelse af straffe- og børneattester.

Akademikerne anfører, at der er behov for en nærmere afklaring af, hvornår oplysninger kan anses for at være ”offentliggjort af den registrerede selv” i henhold til databeskyttelsesforordningens artikel 9, stk. 2, litra e. **Akademikerne** forespørger, om dette gælder i situationer, hvor den registrerede er indforstået med eller har accepteret, at oplysninger om vedkommende er gjort tilgængelige på en hjemmeside, og fagforeningen oplyser, at der som følge af uklarhed herom for nuværende indhentes samtykke til offentliggørelse af f.eks. billeder om personer, der tegner fagforeningen udadtil. Tilsvarende er der behov for at definere begrebet ”samfundsinteresse”, som anvendes i bl.a. forordningens artikel 9, stk. 2, litra g.

Det følger af databeskyttelsesforordningens artikel 9, stk. 2, litra e, at forbuddet mod behandling af oplysninger om bl.a. fagforeningsmæssigt tilhørsforhold ikke finder anvendelse, hvis behandlingen vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede.

Oplysningerne skal uden tvivl (”tydeligvis”) være offentliggjort af den registrerede selv eller på den registreredes foranledning, f. eks. fordi den registrerede utvivlsomt har taget initiativ til eller medvirket til offentliggørelsen. Omvendt betyder dette, at bestemmelsen ikke finder anvendelse, hvis f.eks. pressen, en forening, en myndighed eller en anden aktør har offentliggjort oplysningen på eget initiativ.

Datatilsynet har i praksis fundet, at bestemmelsen i artikel 9, stk. 2, litra e, kunne finde anvendelse, hvor den registrerede havde fremsat oplysningen i et interview til en landsdækkende avis og i et tilfælde, hvor der var sket offentliggørelse af en oplysning om den registreredes opstilling på et politisk partis hjemmeside i forbindelse med valg til Folketinget.

Begrebet "samfundets interesse", som anvendes bl.a. i forordningens artikel 9, stk. 2, litra g, omfatter behandling af personoplysninger til formål, som kan anses for at være af almen interesse, dvs. behandlinger af betydning eller interesse for en bredere kreds af personer. I forordningens præambelbetragtning nr. 52-56 nævnes en række eksempler på sådanne samfundsinteresser. Eksempelvis henvises heri til statistiske, historiske, ansættelses-, sundheds- og socialretlige forhold og afholdelse af valg.

Dansk Arbejdsgiverforening oplyser, at det kræver et uforholdsmæssigt stort arbejde at indhente et skriftligt samtykke, hver gang fotos af medarbejdere skal anvendes eksternt, ligesom det er stort arbejde at "tagge" de enkelte, således at relevante billeder sidenhen kan fremsøges. **Dansk Arbejdsgiverforening** peger endvidere på, at kravet om samtykke kan have store økonomiske konsekvenser, hvis billedet f.eks. indgår i materiale, som ikke kan anvendes alligevel som følge af, at samtykket trækkes tilbage. **Dansk Arbejdsgiverforening** forespørger, om en løsning herpå kunne være at anvende modelkontrakter frem for samtykke.

3F finder, at det er administrativt krævende at indhente samtykke fra medlemmer til at offentliggøre et billede af medlemmet fra et arrangement. **3F** oplyser, at der i praksis er tale om offentliggørelse af fotos mv., som er nødvendig for at synliggøre afdelingens aktiviteter og sætte fokus på samfundsmæssige emner, ligesom der kan være tale om offentliggørelse af billeder på hjemmesiden eller i et nyhedsbrev fra et julearrangement eller et gå-hjem-møde.

Vurderingen af, om et billede eller en filmoptagelse af medarbejdere må offentliggøres uden samtykke, afhænger af billedets karakter og de konkrete omstændigheder i øvrigt, herunder navnlig formålet med offentliggørelsen. Det skal også indgå i vurderingen, om de pågældende med rimelighed kan føle sig krænket, udnyttet eller udstillet.

Efter Datatilsynets nuværende praksis kan billeder af ansatte på arbejde som udgangspunkt ikke offentliggøres uden den ansattes samtykke. Dette gælder også, hvis arbejdsgiveren bruger billeder af ansatte i materiale, f.eks. til brug for reklame. Det skyldes, at der er et større hensyn at tage til medarbejderens interesser end virksomhedens behov.

I visse tilfælde, hvor det findes sagligt begrundet, kan der ske offentliggørelse af billeder af ansatte uden samtykke, hvis den pågældende ikke med rimelighed kan føle sig udstillet eller udnyttet. Arbejdsgivere vil således kunne offentliggøre fotos og film af ansatte i det omfang billedet eller filmen har en naturlig sammenhæng med eller er nødvendig for de funktioner, som medarbejderen skal udføre. Det er dog væsentligt, at der alene er tale om arbejdsrelaterede oplysninger og at der ikke sker offentliggørelse af oplysninger om den pågældende medarbejders private forhold, ligesom det er vigtigt, at billedet/optagelsen ikke efter en almindelig opfattelse kan anses for at være krænkende. F.eks. vil offentliggørelse af en film eller lydoptagelse af en medarbejder om et fagligt, arbejdsrelateret emne, som den pågældende beskæftiger sig med, normalt kunne ske uden samtykke, da der vil være en naturlig sammenhæng med den ansattes funktioner, og det vil falde inden for dennes forventede arbejdsopgaver, ligesom der vil være et klart legitimt formål med offentliggørelsen (f.eks. oplysningsvirksomhed). Omvendt vil offentliggørelse af et billede eller filmoptagelse af en medarbejder til f.eks. et medarbejderarrangement, i fitnesslokalet eller under frokosten efter Datatilsynets opfattelse normalt ikke kunne ske uden samtykke.

Hvis et samtykke trækkes tilbage, indebærer det, at behandlingen skal ophøre – dvs. de pågældende fotos skal fjernes. Medarbejderen må så vidt muligt i den forbindelse forventes at bistå med at identificere de relevante billeder mv. Det vil bero på de konkrete omstændigheder, om det – f.eks. på bagrund af de økonomiske konsekvenser og billedets karakter – kan kræves, at trykt materiale destrueres.

Anvendelse af modelkontrakter vil give arbejdsgiveren mulighed for at behandle billederne på et andet grundlag end samtykke. I hvilket omfang det i øvrigt måtte være en hensigtsmæssig løsning ligger uden for Datatilsynets område at vurdere.

Datatilsynet har forståelse for, at der kan være et legitimt behov for at synliggøre en fagforenings aktiviteter og dermed samfundsmæssige relevans ved anvendelsen af billeder, men omvendt er oplysning om en persons fagforeningsmæssige tilhørshold en særlig beskyttelsesværdig oplysning, jf. databeskyttelsesforordningens artikel 9. Derfor kræver offentliggørelse heraf et samtykke, medmindre en anden undtagelse fra behandlingsforbuddet finder anvendelse, f. eks. at vedkommende selv har offentliggjort oplysning om fagforeningsmæssigt tilhørsforhold.

For så vidt angår spørgsmålet om indhentelse af samtykke har Datatilsynet i en konkret sag fundet, at et samtykke til at blive fotograferet og få billedet offentliggjort kan indhentes ved, at den pågældende person tager opstilling på et bestemt sted eller område, hvis vedkommende forinden har fået tilstrækkelig specifik og klar information om behandlingen, herunder om både optagelse af billedet og offentliggørelsen af dette.

Fagbevægelsens Hovedorganisation anfører, at der er behov for standardmateriale og vejledning rettet mod freelancere, der som enkeltpersoner oplever overholdelse af databeskyttelsesregler for særligt krævende – såvel administrativt som økonomisk.

Branchespecifik vejledning om freelancere kan være vanskelig. Det skyldes, at der findes utallige typer af freelancere. Lidt groft sagt er ansættelsesformen gruppens eneste fællesnævner, altså at der er tale om selvstændige erhvervsdrivende, der arbejder på kontraktbasis. Gruppen spænder således over journalister, musikere, it-eksperter til ansatte i bygge- og anlægsbranchen eller hotel- og restaurationsbranchen mv.

Datatilsynet har produceret en række podcasts, der er let tilgængelige og er et godt sted at starte for den enkelte freelancer og mindre erhvervsdrivende. Herudover har tilsynet udarbejdet vejledende tekster om vikarer og konsulenter til brug for afklaring af rollefordelingen som hhv. dataansvarlig og databehandler. I samarbejde med Erhvervsstyrelsen har Datatilsynet endvidere lavet PrivacyKompasset, som er rettet mod bl.a. mindre erhvervsdrivende.

Datatilsynet vil i sin fremtidige prioritering af vejledning være opmærksom på de behov, der er hos mindre og mellemstore erhvervsvirksomheder, for vejledning på en række forskellige områder, herunder i forhold til spørgsmål om sikkerhed.

Fagbevægelsens Hovedorganisation oplyser, at deltagere til medlemsmøder på forhånd gerne vil vide, hvem der deltager, f.eks. for at kunne planlægge transport til mødet, og derfor synes, at det er et problem, at det åbne modtagerfelt ikke kan anvendes ved indkaldelse til medlemsmøder pr. e-mail. **Fagbevægelsens Hovedorganisation** oplever endvidere praktiske udfordringer i forbindelse med brug af Outlook-kalenderen til udsendelse af invitationer, ligesom det opleves problematisk, at der ikke uden samtykke kan udleveres en deltagerliste efter et medlemsmøde, da deltagerne gerne vil have et overblik over, hvem der deltog, bl.a. for at kunne koordinere tiltag mv.

Hvis f.eks. en fagforening masseudsender en invitation pr. e-mail eller gennem en Outlook-invitation til alle medlemmer, skal foreningen være opmærksom på, om modtagerne kan se hinandens oplysninger. Baggrunden herfor er, at åben angivelse af fysiske personers e-mailadresser eller navne ved masseudsendelse af en mødeinvitation pr. e-mail eller gennem Outlook-kalenderen vil udgøre en videregivelse af personoplysninger. Tilsvarende gælder for videregivelse af oplysninger fra deltagerlister. Oplysning om en persons fagforeningsmæssige tilhørsforhold er omfattet af artikel 9 i databeskyttelsesforordningen og må som udgangspunkt kun behandles, hvis der er en undtagelse til behandlingsforbuddet, som kan finde anvendelse. Som regel vil dette betyde, at det forudsætter, at der er givet samtykke.

Ved anvendelse af e-mail til udsendelse af invitationer mv. til arrangementer for fagforeningens medlemmer vil det være nødvendigt at anvende bcc-feltet, så medlemmerne ikke kan se hinandens oplysninger, hvis behandlingen ikke sker på grundlag af samtykke.

Fagbevægelsens Hovedorganisation oplyser, at nogle arbejdsgivere oplever udfordringer i forbindelse med, at deres ansatte anvender deres arbejdsudstyr (computer, telefon, tablet mv.) til private formål (f.eks. private opkald, e-mails mv.), hvorved oplysninger om de ansattes private forhold bliver lagret på arbejdsgiverens materiel, hvorfor der kan opstå vanskelige situationer, hvis og når arbejdsgiveren får behov for at tilgå udstyret. **Fagbevægelsens Hovedorganisation** ser således behov for et regelsæt til håndtering af såvel arbejdstagers som arbejdsgivers interesser, således at hensynet til arbejdsgivers interesser i at afdække eventuelle regelbrud og pligtforsømmelser ikke går videre end hensynet til beskyttelsen af arbejdstagers private oplysninger.

De databeskyttelsesretlige regler giver på den ene side en arbejdsgiver mulighed for at tilgå de nødvendige oplysninger, hvis der er et lovligt behandlingsgrundlag, og de overordnede betingelser om saglighed og proportionalitet er opfyldt. Datatilsynet har i konkrete sager udtalt, at en arbejdsgiver kan have en legitim interesse i f.eks. at gennemgå en medarbejders e-mailkonto, hvorved arbejdsgiveren – eventuelt utilsigtet – kan komme i berøring med oplysninger af privat karakter. Det kan f.eks. være tilfældet, hvis der er en konkret begrundet mistanke om brud på loyalitetsforpligtelsen eller interne retningslinjer. På den anden side varetages den ansattes interesser og rettigheder i øvrigt ved, at den ansatte skal være informeret klart på forhånd om arbejdspladsens retningslinjer for brug af udstyr til privat brug samt hvilken kontrol og formålet hermed, som kan iværksættes fra arbejdsgiverens side med henblik på gennemgang af arbejdspladsens udstyr.

I Datatilsynets vejledning om databeskyttelse i forbindelse med ansættelsesforhold (december 2020) fremgår det således også, at gennemgang af medarbejderes hjemmesidebesøg ved mistanke om misbrug af internettet og kontrol af e-mails kan ske under visse betingelser. Denne vejledning indeholder også retningslinjer om opbevaring af oplysninger efter ansættelsesophør og om oplysningspligten ved kontrolforanstaltninger. Datatilsynet modtager gerne konkrete forslag fra arbejdsmarkedets parter, hvis der er behov for at udbygge vejledningen yderligere på specifikke områder.

14.2 Private virksomheder og foreninger

Dansk Erhverv og IT-branchen ønsker klarhed om, i hvilket omfang databeskyttelsesreglerne gælder for personer, der agerer på vegne af en virksomhed. **Dansk Erhverv og IT-branchen** peger i den forbindelse på det forhold, at de fleste business-to-business-virksomheder ikke har forbrugerdata i deres CRM-systemer (kundedatabaser), idet de typiske personoplys-

ninger, som en sådan virksomhed håndterer – når man ser bort fra data om virksomhedens egne medarbejdere – er telefonnumre og e-mailadresser på kontaktpersoner hos virksomhedens kunder og leverandører. **Dansk Erhverv og IT-branchen** oplyser i tilknytning hertil, at der hersker usikkerhed om, hvordan personoplysninger, der er indeholdt i mailsystemer som f.eks. Outlook, skal behandles i forhold til oplysninger i CRM- eller ERP-systemer m.fl., bl.a. i relation til sletning og indsigtsret, og at der er behov for vejledning i forhold til håndtering af disse systemer.

Databeskyttelsesreglerne skelner ikke mellem personoplysninger, der bliver behandlet i forbindelse med B2B-virksomheder eller i forbindelse med andre kommercielle virksomheders aktiviteter. Databeskyttelsesreglerne gælder således også for oplysninger om fysiske personer, selv om de agerer på vegne af en virksomhed.

I forbindelse med B2B er behandlingen af personoplysninger imidlertid ikke i fokus, og personoplysningerne vil formentlig alene blive behandlet som led i den normale drift af virksomheden. Som anført af Dansk Erhverv og IT-branchen vil der typisk blive behandlet oplysninger om telefonnumre og e-mailadresser på kontaktpersoner hos B2B-virksomhedens kunder eller leverandører. Dertil kommer, at der sandsynligvis også vil blive behandlet oplysninger om kontaktpersonens navn og andre oplysninger, der knytter sig til den pågældende persons ansættelse hos enten virksomhedens kunde eller leverandør.

Når de databeskyttelsesretlige regler finder anvendelse på en behandling af personoplysninger, afgøres lovligheden af forskellige faktorer, heriblandt formålet med behandlingen og oplysningernes karakter. Det har således betydning for anvendelsen af de databeskyttelsesretlige regler i forbindelse med B2B, at de personoplysninger, der bliver behandlet, er af begrænset omfang, og at oplysningerne f.eks. telefonnumre og e-mailadresser formentlig stilles til rådighed af arbejdsgiveren og dermed ikke er den pågældende persons private kontaktoplysninger. Intensiteten af den behandling af personoplysninger, som finder sted i forbindelse med B2B, vil også gøre sig gældende i forhold til f.eks. håndtering af indsigtsanmodninger, hvor det således formentlig vil være ret begrænset, hvor mange oplysninger man som dataansvarlig skal forholde sig til.

Databeskyttelsesreglerne er teknologineutrale, og det har derfor ikke betydning for reglernes anvendelse, om behandling af personoplysninger foretages i et mailsystem, CRM-system, ERP-system eller et andet system. Det afgørende er, om behandlingen af personoplysningerne helt eller delvist foretages ved hjælp af automatisk databehandling eller er indeholdt i et register, for i så fald finder databeskyttelsesreglerne anvendelse.

Det betyder også, at personoplysninger – uanset om de er indeholdt i et mailsystem, CRM-system eller ERP-system – skal slettes, når den fortsatte opbevaring ikke længere er nødvendig. Tilsvarende indebærer indsigtsretten en ret til indsigt i personoplysninger, uanset om de ligger i et mailsystem, CRM-system, ERP-system eller andet system. En anmodning om indsigt fra en registreret vil således også omfatte de personoplysninger, som behandles i f.eks. en virksomheds mailsystem. Datatilsynet bemærker i den forbindelse, at en anmodning om indsigt indebærer, at den dataansvarlige som udgangspunkt skal udlevere en kopi af de personoplysninger, der behandles. Kopien skal indeholde den registreredes personoplysninger, men retten til indsigt indebærer ikke, at den dataansvarlige skal udlevere samtlige e-mails, hvori den registreredes navn fremgår.

Ovenstående betyder ikke, at en virksomhed ikke må opbevare personoplysninger i deres e-mailsystemer, CRM- eller ERP-systemer, så længe virksomheden har et sagligt behov for at behandle og opbevare oplysningerne, f.eks. hvis virksomheden har en aktiv dialog med en

kontaktperson hos en leverandør. Når en sådan dialog er overstået, kan der være fremkommet oplysninger, som en virksomhed har behov for at kunne dokumentere.

Som udgangspunkt er det uproblematisk, hvis en medarbejder gemmer interne e-mails i sin e-mailkonto, så længe der er et behov herfor, f.eks. for at en medarbejder kan varetage sit arbejde på en tilfredsstillende måde, da de interne e-mails kan indeholde relevante instrukser, vejledninger eller aftaler.

Datatilsynet anbefaler i øvrigt, at en dataansvarlig udarbejder en politik og procedurer for opbevaring og sletning af personoplysninger i den dataansvarliges systemer, herunder for personoplysninger der opbevares i mailsystemer.

Dansk Industri anfører, at det i visse tilfælde er uklart, om følsomme personoplysninger, f.eks. oplysninger om medarbejderes helbredsforhold, må anvendes til organisatoriske formål, der ikke er konkret knyttet til den pågældendes eget ansættelsesforhold, uden samtykke fra medarbejderen. Som eksempel nævner **Dansk Industri** rapportering af antallet af fleksarbejdere i en given afdeling med henblik på at øge andelen af fleksarbejdere fremadrettet, hvor det er uklart, om det forhold, at en medarbejder har nedsat arbejdsevne, er en helbredsoplysning, og om bredere organisatoriske formål – f.eks. at øge andelen af fleksarbejdere – kan anses for omfattet af den dataansvarliges arbejdsretlige forpligtelser. Efter **Dansk Industris** opfattelse begrænser databeskyttelsesreglerne mulighederne for at arbejde med CSR-mål på et mere oplyst grundlag.

Dansk Industri oplyser endvidere, at det giver anledning til tvivl, hvornår virksomheder må videregive oplysninger om medarbejderes personnumre til offentlige myndigheder, hvis videregivelsen ikke følger af lovgivningen. **Dansk Industri** henviser for eksempel til, at virksomheder, der indgår kontrakter med offentlige myndigheder, bliver bedt om at oplyse personnumre på de medarbejdere, der arbejder på kontrakterne for det offentlige. Det ses bl.a. i forbindelse med indgåelse af arbejdsklausuler, men også i tilfælde hvor den offentlige myndighed skal bruge personnummer til oprettelse af virksomhedens medarbejdere i IT-systemer. **Dansk Industri** anfører, at der er tvivl om, hvorvidt virksomheder har hjemmel til en sådan videregivelse, bl.a. fordi virksomheden ofte ikke kan indhente et gyldigt samtykke fra medarbejderen, og fordi det er uklart, hvornår videregivelsen kan anses for at være et naturligt led i den normale drift af virksomheden. **Dansk Industri** har i den forbindelse også peget på, at det er tvivlsomt, om en sådan videregivelse vil være i overensstemmelse med dataminimeringsprincippet, da den offentlige myndighed typisk vil kunne identificere medarbejderen med færre oplysninger.

Det faktum, at en medarbejder har nedsat arbejdsevne, udgør ikke i sig selv en helbredsoplysning, da årsagen til den nedsatte arbejdsevne ikke kan udledes.

Personoplysninger, der er indsamlet i tilknytning til ansættelsesforhold, må gerne viderebehandles til f.eks. statistiske formål. Ved statistiske formål forstås enhver indsamling og behandling af personoplysninger, der er nødvendig for statistiske undersøgelser eller frembringelse af statistiske resultater. Det statistiske formål indebærer, at resultatet af behandling til statistiske formål ikke er personoplysninger, men aggregerede data, og at personoplysningerne ikke senere må anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer. Databeskyttelsesreglerne begrænser derfor ikke mulighederne for, at en virksomhed behandler personoplysninger med henblik på at opnå et mere oplyst grundlag for at arbejde med CSR-mål, som f.eks. diversitet.

Hvad angår virksomheders videregivelse af oplysninger om medarbejderes personnumre er der i databeskyttelseslovens § 11, stk. 2, oplistet en række mulige behandlingsgrundlag, herunder også i de tilfælde, hvor videregivelse ikke følger af lovgivning eller sker på baggrund af et samtykke fra den registrerede. Private virksomheder vil således kunne videregive oplysninger om personnummer, bl.a. hvis videregivelsen sker som et naturligt led i den normale drift af virksomheder mv. af den pågældende art, hvis det enten er af afgørende betydning for at sikre entydig identifikation af den registrerede, eller hvis videregivelsen kræves af en offentlig myndighed.

Den dataansvarlige, som indsamler personoplysningerne, skal naturligvis forholde sig til, at indsamlingen sker under iagttagelse af dataminimeringsprincippet i forordningens artikel 5, stk. 1, litra c.

I forhold til det af Dansk Industri anførte eksempel – videregivelse af personnummer til offentlige myndigheder – vil en sådan videregivelse efter Datatilsynets opfattelse være uproblematisk. Der vil således ikke være krav om, at virksomheden fjerner oplysninger om medarbejderes personnumre i forbindelse med fremsendelse af dokumentation til myndigheden.

Dansk Industri anfører, at det i tilfælde, hvor en virksomhed har sin egen historiske afdeling eller historiske arkiver, f.eks. i form af billeder, er uklart, om det virksomhedshistoriske arbejde er omfattet af de databeskyttelsesretlige regler, som regulerer behandling af personoplysninger til "arkivformål i samfundets interesse" og/eller "historiske forskningsformål".

Dansk Industri oplyser endvidere, at der tilsvarende opleves tvivl om, i hvilket omfang virksomhedsjournalistik i form af f.eks. interne medarbejderblade eller medlemsblade udgør "journalistik" i en databeskyttelsesretlig kontekst – særlig henset til databeskyttelseslovens § 3, stk. 8.

En virksomheds historiske afdeling eller historiske arkiver ses ikke at være omfattet af arkivlovgivningen, da det kun er de offentlige arkivers virksomhed, der direkte er reguleret i denne lovgivning. Det betyder, at databeskyttelsesforordningens og databeskyttelseslovens regler om behandling af personoplysninger til arkivformål ikke sådan uden videre kan anvendes af virksomheder. Om virksomhedshistorisk arbejde kan anses for at være omfattet af databeskyttelsesforordningens og databeskyttelseslovens bestemmelser om forskning vil bero på en nærmere vurdering af, bl.a. hvad formålet med det pågældende arbejde er, herunder om det er et arbejde, som kan anses for at være forskning i samfundets interesse.

Om journalistisk arbejde kan Datatilsynet oplyse, at medier generelt er undtaget fra de databeskyttelsesretlige regler. Hvis en behandling af personoplysninger er omfattet af lov om massemediers informationsdatabaser, er behandlingen således undtaget fra databeskyttelsesloven og databeskyttelsesforordningen, jf. databeskyttelseslovens § 3, stk. 4. I databeskyttelseslovens § 3, stk. 5-7, begrænses anvendelsen af databeskyttelsesreglerne også i forbindelse med, hvad der generelt kan karakteriseres som behandling, der sker i relation til "nyhedsformidling/journalistisk virksomhed".

Det er ikke udelukket, at "virksomhedsjournalistik" kan være omfattet af undtagelserne i databeskyttelseslovens § 3, stk. 4-8, hvis betingelserne herfor er opfyldt. Databeskyttelseslovens § 3, stk. 8, er imidlertid i lovens forarbejder forudsat et snævert anvendelsesområde, og det er derfor tvivlsomt, om "virksomhedsjournalistik" kan anses for undtaget reglerne i medfør af denne bestemmelse. Den endelige vurdering heraf må imidlertid foretages af domstolene.

Finans og Leasing anfører, at der er behov for oplysning om, hvordan virksomheder inden for rammerne af databeskyttelsesreglerne kan arbejde med at forhindre svindel, således at der kan videregives personoplysninger med henblik på at advare herom.

Finans Danmark anfører, at det i praksis er vanskeligt at vurdere, hvornår et register er oprettet med det primære formål at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret og dermed anses for at være et advarselsregister, som kræver tilladelse fra Datatilsynet. **Finans Danmark** ønsker flere konkrete eksempler i Datatilsynets vejledning fra 2019 om advarselsregistre.

Afgørende for, om en behandling er omfattet af databeskyttelseslovens § 26, stk. 1, nr. 1, om advarselsregistre, er, om registret er oprettet med henblik på videregivelse. At der jævnligt sker videregivelse af oplysninger fra et register, der primært er oprettet med et andet formål, medfører således ikke, at registret udgør et advarselsregister. Omfattet af reglerne om advarselsregistre vil typisk være et register, der er oprettet af en forening eller en brancheorganisation med henblik på at videregive oplysninger til foreningens eller brancheorganisationens medlemmer om medlemmernes forretningsforbindelser og disses betalingsevne.

Et advarselsregister vil altid kræve forudgående tilladelse fra Datatilsynet. Datatilsynet vil i den forbindelse tage stilling til, om der kan meddeles tilladelse til advarselsregistret, og på hvilke nærmere vilkår en sådan tilladelse vil kunne meddeles. Datatilsynet vil bl.a. vurdere, om advarselsregistret kan anses for at tjene anerkendelsesværdige interesser, og heri vil navnlig indgå en vurdering af registrets formål i forhold til den risiko for krænkelse af privatlivets fred, som oprettelsen og brugen kan medføre.

Datatilsynet har på sin hjemmeside offentliggjort en række sager, som både er eksempler på ansøgninger, hvor tilsynet har givet afslag, og ansøgninger, som Datatilsynet har imødekommet. Derudover har Datatilsynet også offentliggjort de standardvilkår, som tilsynet som udgangspunkt stiller som vilkår for at opnå tilladelse til at oprette et advarselsregister. Datatilsynet har imidlertid noteret sig ønsket om, at der indarbejdes flere konkrete eksempler i vejledningen om advarselsregistre.

Finans Danmark oplyser, at der i den finansielle sektor opleves samspilsproblemer mellem den finansielle lovgivning og databeskyttelsesreglerne. Det er oplevelsen, at det ikke altid er muligt at efterleve begge regelsæt samtidig, bl.a. fordi der er forskellige hensyn bag de to regelsæt. **Finans Danmark** peger særligt på, at de grundlæggende principper for behandling af personoplysninger efter databeskyttelsesforordningens artikel 5 giver anledning til tvivl i den finansielle sektor, f.eks. om hvor uforenelighedsgrænsen efter artikel 5, stk. 1, litra b, går ved viderebehandling til et andet formål, herunder hvornår der kan ske viderebehandling til statistiske formål, idet der er store samfundsmæssige gevinster forbundet med dataanalyse. **Finans Danmark** efterspørger derfor bl.a. konkret vejledning eller fortolkningsbidrag til definitionen af ”viderebehandling til statistiske formål”.

Håndtering af de nævnte problematikker vedrørende samspillet mellem databeskyttelsesreglerne og den finansielle lovgivning forudsætter et indgående kendskab til en række forskellige regelsæt på det finansielle område. Datatilsynet er løbende i dialog med relevante aktører i den finansielle sektor om drøftelse af problemstillinger relateret til samspillet mellem den finansielle lovgivning og databeskyttelsesreglerne.

Datatilsynet deltager endvidere aktivt i regi af Det Europæiske Databeskyttelsesråd (EDPB) i udarbejdelsen af vejledninger om samspillet mellem databeskyttelsesforordningen og forskellig finansiel lovgivning. Der er netop vedtaget en vejledning om samspillet mellem det andet

betalingstjenestedirektiv (PSD2) og databeskyttelsesforordningen (vejledning 06/2020). Endvidere vil Datatilsynet – i forlængelse af et netop igangsat europæisk studie heraf – arbejde aktivt på, at der udarbejdes en tilsvarende vejledning om samspillet mellem databeskyttelsesforordningen og hvidvaskreglerne.

Grundlæggende kan Datatilsynet gøre opmærksom på, at der er en række muligheder for at behandle personoplysninger, selv om der ikke foreligger en egentlig retlig forpligtelse til at indsamle og behandle oplysningerne.

Endvidere kan Datatilsynet oplyse, at når en behandling af personoplysninger sker til et andet formål, end det, som oplysningerne blev indsamlet til, og dette ikke er baseret på den registreredes samtykke, EU-retten eller national ret, skal den dataansvarlige bl.a. tage hensyn til en række faktorer, der er oplistet i databeskyttelsesforordningens artikel 6, stk. 4. Som eksempel på viderebehandling har Finans Danmark henvist til indsamling og behandling af transaktionsoplysninger med hjemmel i betalingsloven, hvor visse af sådanne oplysninger også er relevante i forbindelse med rådgivning og budgetplanlægning. Finans Danmark har oplyst, at der i dag indhentes samtykke ved en sådan viderebehandling, men efterspørger samtidig, om det egentlig er nødvendigt at indhente et samtykke fra den registrerede i disse tilfælde. Datatilsynet har ikke nærmere kendskab til, hvilke(t) formål/hensyn der ligger bag den behandling af personoplysninger, som følger af betalingsloven og kan derfor ikke på det foreliggende grundlag komme med en klar tilkendegivelse af, i hvilket omfang personoplysninger indsamlet på baggrund af betalingslovens bestemmelser kan anvendes til f.eks. budgetplanlægning. Som tidligere tilkendegivet er Datatilsynet imidlertid som altid åben over for en dialog om konkrete udfordringer i samspillet mellem den finansielle lovgivning og databeskyttelsesreglerne, herunder om mulighederne for genanvendelse af oplysninger til andre formål.

Finans Danmark oplyser endvidere, at det i praksis forekommer, at ikke-relevante personoplysninger uanmodet modtages via e-mail eller oplyses under telefonsamtaler, som der er pligt til at optage og gemme i henhold til den finansielle lovgivning, selv om kunder opfordres til ikke at indsende flere oplysninger end nødvendigt. Udfordringen består bl.a. i, at det påvirker integriteten af materialet, hvis de overflødige data slettes, ligesom det kan være særdeles vanskeligt at slette dele af en telefonsamtale.

Det er Datatilsynets opfattelse, at det i langt hovedparten af sådanne tilfælde ikke vil være i strid med dataminimeringsprincippet i databeskyttelsesforordningens artikel 5, stk. 1, litra c, hvis de "overflødige" data gemmes.

DUF anfører, at det er omstændigt at skulle indhente samtykke til eksempelvis at måtte behandle medlemmers allergier i forbindelse med ture og kurser, hvor oplysningerne indhentes i medlemmernes interesse og for at kunne tilgodese medlemmernes behov. **DUF** forespørger, om der kan indhentes et samtykke til behandling af helbredsoplysninger (f.eks. oplysninger om allergier) ved medlemmets indmeldelse i stedet for indhentelse af samtykke ved den enkelte tilmelding til hver tur eller kursus, som er meget ressourcekrævende. **DUF** forestiller sig, at det f.eks. kan fremgå af det enkelte medlems profiloplysninger (med et flueben), om der er givet samtykke til behandling af oplysninger om f.eks. allergier.

Det af Dansk Ungdoms Fællesråd skitserede forslag vil efter Datatilsynets opfattelse være en fornuftig løsning. Dansk Ungdoms Fællesråd skal i den forbindelse være opmærksom på, at det samtykke, som medlemmet afgiver i forbindelse med indmeldelse, skal opfylde databeskyttelsesforordningens artikel 4, nr. 11, og artikel 7, om at være udtryk for en frivillig, specifik, informeret og utvetydig viljestilkendegivelse, hvilket bl.a. indebærer, at et nægtet samtykke ikke må medføre negative konsekvenser for medlemmet (f.eks. udelukkelse fra at deltage).

Dansk Ungdoms Fællesråd nævner, at samtykket skal dokumenteres ved et flueben på medlemmets profil, så relevante personer kan se, om der er givet samtykke. Dertil bemærker Datatilsynet, at Dansk Ungdoms Fællesråd skal være opmærksom på at kunne dokumentere, at medlemmet har afgivet et gyldigt samtykke.

DGI oplyser, at det giver anledning til tvivl, i hvilket omfang en forening må kommunikere oplysninger om strafbare forhold i forhold til såvel intern som ekstern kommunikation. **DGI** oplyser, at det f.eks. kunne dreje sig om oplysninger om økonomisk kriminalitet mod en forening begået af foreningens leder eller om seksuelle krænkelser begået i en forening. **DGI** anfører, at det ofte er nødvendigt med kommunikation for at kunne informere og afværge unødig uro.

Datatilsynet anerkender, at der – f.eks. for at undgå rygtedannelse og "uro" i en forening – kan være behov for, at en forening informerer sine medlemmer om, f.eks. at en leder er fratrådt. En forenings mulighed for at informere medlemmerne om ændringer i organisationen må normalt anses for at veje tungere end hensynet til den pågældende, ligesom det kan tillægges vægt, at medlemmerne efterfølgende ved selvsyn vil kunne konstatere, at den pågældende ikke længere er ansat eller er en del af foreningen. Derimod vil det som udgangspunkt ikke være nødvendigt for at varetage dette formål at oplyse om baggrunden for, at den pågældende er stoppet.

I nogle helt konkrete tilfælde kan der imidlertid være tungvejende hensyn, som medfører, at en forening undtagelsesvis kan videregive visse overordnede oplysninger om årsagen. I den forbindelse kan det tillægges betydning, hvilken stilling eller rolle den pågældende har haft i foreningen, f.eks. at der er tale om en leder.

Hvis en afskedigelse skyldes en underbygget mistanke om strafbare forhold, må denne oplysning ikke deles med andre i organisationen, i større omfang end hvad der er strengt nødvendigt. Der må derfor som det klare udgangspunkt ikke deles oplysninger på f.eks. foreningens medlemsside eller i en e-mail til medlemmer om, at en navngiven medarbejder er blevet afskediget grundet f.eks. en mistanke om svindel.

DGI forespørger endvidere, hvor længe en indhentet børneattest må opbevares. **DGI** har overvejet, om en forening kan gemme attester uden anmærkninger, så længe den pågældende arbejder i foreningen, og at attesten bør slettes et år efter, at den pågældende er ophørt med at virke i foreningen. Hvis en forening modtager en attest med anmærkninger, anfører **DGI**, at idrætsorganisationernes interne regelsæt tilsiger, at den pågældende som udgangspunkt ikke må fungere i en forening, men at der efter ansøgning kan gives tilladelse til det. Kommer den pågældende ikke til at virke i foreningen, bør attesten kunne gemmes i op til et år.

Adgangen til at indhente børneattester er reguleret af lov om indhentelse af børneattester i forbindelse med ansættelse af personale mv., som hører under Kulturministeriets ressortområde. Spørgsmålet om, hvor længe børneattester kan opbevares, reguleres imidlertid af de databeskyttelsesretlige regler.

Personoplysninger indeholdt i en børneattest må ikke opbevares i et længere tidsrum end det, der er nødvendigt, henset til det formål, hvortil børneattesten er indhentet. Datatilsynet kan ikke identificere et sagligt formål med, at en forening opbevarer børneattester med anmærkninger i op til et år fra indhentelsen, eller at børneattester uden anmærkninger opbevares i op til et år efter ophøret af en ansættelse i foreningen. Datatilsynet har i den forbindelse lagt vægt på, at den lovpligtige indhentelse af børneattester skal ske forud for en ansættelse eller ind-

gåelse af aftale med en person med henblik på, om den pågældende skal ansættes eller virke for foreningen.

Det er Datatilsynets opfattelse, at en forening – i overensstemmelse med Kulturministeriets vejledning – bør destruere en børneattest efter modtagelsen, medmindre andre regler, f.eks. på det ansættelsesretlige område, kræver opbevaring af attesten. I så fald bør en forening kun opbevare attesten i det omfang, sådanne regler kræver det.

Det forhold, at idrætsorganisationernes interne regelsæt tilsiger, at den pågældende kan indbringe en børneattest med anmærkninger for idrætsorganisationernes seksualkrænkelsesnævn, ændrer ikke ved Datatilsynets vurdering af, at en forening som helt klart udgangspunkt ikke kan anses for at have et sagligt formål med at skulle opbevare børneattester med anmærkninger i op til et år. Datatilsynet lægger i den forbindelse vægt på, at adgangen til at indbringe en børneattest for seksualkrænkelsesnævnet alene tilkommer den pågældende person og ikke foreningen, og at den pågældende person til brug for nævnets vurdering selv skal indsende en kopi af børneattesten. Der ses således heller ikke i dette tilfælde at være et sagligt behov for, at foreningen opbevarer børneattesten.

EjendomDanmark oplyser, at det giver anledning til tvivl, om en udlejer må udlevere oplysninger om lejere i form af navn og adresse til beboerrepræsentationen i en udlejningsejendom. **EjendomDanmark** henviser til, at udlejer i henhold til lejeloven er forpligtet til at oplyse beboerrepræsentationen om, at der er sket lejerskifte, men at der ikke er et krav i loven om, at navn og kontaktoplysninger oplyses. **EjendomDanmark** anfører, at beboerrepræsentationen i princippet kan kontakte vedkommende på adressen, hvorfor det ikke er strengt nødvendigt, at beboerrepræsentationen får oplysning om navn og kontaktinformation. Det vil imidlertid lette beboerrepræsentationens arbejde samt forholdet mellem beboerrepræsentationen og udlejer, hvis udlejer kan udlevere oplysningen til beboerrepræsentationen.

Det fremgår af lejelovens § 65, at en beboerrepræsentation skal varetage lejernes interesser i forhold til udlejeren og medvirke til at sikre det bedst mulige grundlag for samarbejdet mellem lejeren og udlejeren. Videre fremgår det, at beboerrepræsentationen i den forbindelse bl.a. skal holdes orienteret, når der foretages genudlejning af lejligheder i ejendommen. Det er Datatilsynets vurdering, at det vil være sagligt og relevant, at en udlejer videregiver oplysninger om navn og adresse til en beboerrepræsentation ved lejerskifte, bl.a. henset til beboerrepræsentationens opgaver i henhold til lejeloven, og at videregivelsen kan ske med hjemmel i interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f. Dog skal udlejer være opmærksom på, hvis der er tale om oplysninger, som er navne- og adressebeskyttede efter CPR-loven.

14.3 Ikke kategoriserede spørgsmål

Dansk Erhverv og IT-branchen anfører, at der er usikkerhed omkring anonymisering af data og forespørger, hvornår data er anonyme, herunder om syntetiske data kan siges at være anonyme.

Personoplysninger er anonyme og falder uden for databeskyttelsesreglerne, hvis ingen fysisk person kan identificeres ud fra oplysningerne i sig selv eller i kombination med andre oplysninger. De adskiller sig således fra pseudonymiserede oplysninger, som er oplysninger, der i sig selv ikke kan henføres til en bestemt fysisk person, men hvor anvendelsen af supplerende oplysninger vil gøre dette muligt, og som derfor er omfattet af databeskyttelsesreglerne.

Hvis der med udtrykket "syntetiske data" menes data i form af konstruerede/fiktive datasæt, som er skabt ud fra rigtige data, og har bevaret ligheder hermed, men som ikke er personhenførbare og dermed ikke alene eller ved anvendelsen af hjælpemidler kan benyttes til at identificere en fysisk person, vil syntetiske data være anonyme og således ikke være omfattet af databeskyttelsesreglerne.

Danske Advokater har givet udtryk for at være i tvivl om opfyldelsen af forpligtelser efter databeskyttelsesforordningen i forhold til personoplysninger, der indgår i en konkursramt virksomhed, f.eks. om kurator har pligt til at besvare indsigtsanmodninger.

Det følger af Datatilsynets praksis, at kurator også i databeskyttelsesretlig forstand som udgangspunkt må antages at træde i ledelsens sted i en konkursramt virksomhed, og at der som følge heraf som udgangspunkt ikke indtræder krav om f.eks. opfyldelse af en oplysningspligt i anledning af konkursen som sådan, da der ikke er tale om en videregivelse af oplysninger. Heri ligger dog også, at kurator som enhver anden dataansvarlig i øvrigt vil skulle overholde databeskyttelsesforordningen, herunder tage stilling til f.eks. indsigtsanmodninger fra registrerede.

Danske Medier oplyser, at når dataansvarlige vil anvende cookies på en hjemmeside, er det påkrævet at indhente et samtykke i overensstemmelse med ePrivacy-direktivet og databeskyttelsesforordningen. Disse regler og de konkrete forhold på en hjemmeside eller anden digital tjeneste har betydning for, hvordan man indhenter et juridisk gyldigt samtykke. Forskel på databeskyttelsesimplementering og fortolkning på tværs af lande og datatilsyn medfører ulige konkurrencevilkår. Dette er tilfældet med det danske datatilsyns fortolkning, idet det tilsyneladende er det eneste tilsyn i EU (så vidt vides), der kræver granuleret valgmuligheder i første lag (og ikke i det næste lag) i forbindelse med cookiesamtykke til flere formål.

Det følger af databeskyttelsesforordningens artikel 4, nr. 11, at et samtykke skal være frivilligt, specifikt, informeret og udtryk for en utvetydig viljestilkendegivelse fra den registrerede.

Det er Datatilsynets opfattelse, at et samtykke ikke kan antages at være givet frivilligt, hvis proceduren til opnåelse af samtykke ikke giver den registrerede mulighed for at give særskilt samtykke til behandling af personoplysninger til forskellige formål, og den registrerede dermed tvinges til at give samtykke til samtlige formål. Samtykke skal med andre ord opfylde princippet om granularitet.

I Datatilsynets afgørelse fra februar 2020 om Dansk Meteorologisk Instituts (DMI) behandling af personoplysninger om hjemmesidebesøgende udtalte tilsynet – efter at sagen havde været forelagt Datarådet – at det samtykke, der blev indhentet ved DMI's løsning, ikke gav de besøgende et tilstrækkeligt frit valg i forhold til at kunne identificere og til- og fravælge, hvilke formål den besøgende reelt ønskede at give samtykke til. Datatilsynet noterede sig i den forbindelse, at det var muligt at til- og fravælge indsamling af personoplysninger til forskellige formål ved at vælge funktionen "Vis detaljer", men at denne mulighed var placeret "et-klik-væk", og det dermed ikke var muligt ved det indledende besøg på hjemmesiden. Datatilsynet udtalte endvidere, at en sådan et-klik-væk fremgangsmåde ikke er gennemsigtig, da det dels kræver et ekstra skridt for den registrerede at afslå at give samtykke til behandling af personoplysninger, dels ikke er klart for den registrerede, at det er muligt at undlade at give samtykke til behandling af personoplysninger ved at vælge "Vis detaljer".

I forhold til at Datatilsynet generelt skulle anlægge en strengere praksis for så vidt angår kravet om, at den besøgende skal have mulighed for at give særskilt samtykke til forskellige behandlinger i samtykkeløsningens første lag, er tilsynet ikke bekendt med, at andre tilsynsmyn-

digheder skulle anlægge en mere lempelig praksis. Det er Datatilsynets umiddelbare opfattelse, at tilsynet ikke er det eneste tilsyn, som er af den overbevisning, at dataansvarlige, som indhenter samtykke ved behandling af oplysninger om hjemmesidebesøgende til flere forskellige formål, som udgangspunkt skal give brugerne mulighed for at foretage et granuleret valg i samtykkeløsningens første lag.

Datatilsynet skal imidlertid understrege, at en vurdering af en hjemmesides behandling af personoplysninger, herunder vurderingen af om betingelserne for samtykke er opfyldt, altid hviler på en konkret stillingtagen i det enkelte tilfælde. Det er derfor vanskeligt på generel basis at diktere udformningen af en hjemmesides samtykkeløsning, idet Datatilsynet ikke på forhånd kan afvise, at der i visse situationer kan være omstændigheder, som nødvendiggør en anderledes fremgangsmåde til indsamling af samtykke.

Datatilsynet er endvidere opmærksom på de udfordringer, der består i at skabe en ensartet forståelse og anvendelse af de databeskyttelsesretlige regler på tværs af de europæiske lande, hvor f.eks. problemstillinger vedrørende behandling af personoplysninger om hjemmesidebesøgende fortsat er relativt nye og derfor måske kan give anledning til forskellige opfattelser. Dette er samtidig en af grundene til, at Datatilsynet har et stort fokus på, at reglerne på området overholdes, og tilsynet forventer således også at offentliggøre flere afgørelser om behandling af personoplysninger om hjemmesidebesøgende i 2021, ligesom tilsynet forventer at iværksætte flere sager af egen drift vedrørende emnet.

DGI forespørger, fra hvilken alder et barn selv kan afgive personoplysninger uden godkendelse fra forældre.

Når den dataansvarlige – f.eks. en forening – behandler personoplysninger om et barn på baggrund af et samtykke, skal den dataansvarlige overveje, om barnet selv kan give samtykke, eller om samtykket skal indhentes hos indehaveren af forældremyndigheden.

Denne vurdering skal tage udgangspunkt i det enkelte barns modenhed og vil således være en konkret vurdering i det enkelte tilfælde. Som det klare udgangspunkt vil et barn på 15 år have tilstrækkelig modenhed og forståelse til at give samtykke på egne vegne. I enkelte tilfælde vil yngre børn dog også have den fornødne modenhed til at give samtykke på egne vegne, hvis den behandling, der gives samtykke til, er let overskuelig og er forbundet med minimale risici – eksempelvis sædvanlige foreningsaktiviteter.

EjendomDanmark er i tvivl om, hvorvidt offentligt tilgængelige adresseoplysninger nyder beskyttelse i medfør af databeskyttelsesreglerne.

Hvis en oplysning – enten alene eller i kombination med andre oplysninger – kan henføres til en bestemt person, er der tale om personoplysninger omfattet af databeskyttelsesreglerne, herunder reglerne i GDPR. Dette gælder således også oplysninger om en persons adresse, uanset om oplysningen måtte være offentligt tilgængelig.

Alt andet lige skal en adresse, som er tilgængelig i et offentliggjort register, imidlertid ikke undergives samme sikkerhedsforanstaltninger, som en hemmelig (beskyttet) adresse. Det følger endvidere af Datatilsynets praksis, at private dataansvarlige som udgangspunkt lovligt kan indsamle, registrere, bearbejde og videregive personoplysninger, herunder adresser, der er indhentet fra offentligt tilgængelige registre som eksempelvis Statstidende, CVR, Bilbogen, Motorregistret o. lign.

Kræftens Bekæmpelse oplyser, at afgrænsningen af, hvornår en frivillig optræder på vegne af den dataansvarlige, kan være svær at foretage og implikationerne heraf endnu sværere at omsætte til virkelighed ude i den enkelte forening.

Hvis man er ansat eller arbejder som frivillig for en forening, vil det som udgangspunkt være foreningen og ikke den fysiske person, som betragtes som dataansvarlig.

PROSA oplyser, at det er problematisk, at sundhedsdata er undtaget fra GDPR, da sundhedsdata er noget af det mest følsomme data.

Sundhedsdata, hvorved der forstås helbredsoplysninger, er omfattet af databeskyttelsesforordningen (GDPR). Helbredsoplysninger er i forordningens artikel 9 kategoriseret som en følsom oplysning. Det er i den forbindelse ikke afgørende, om der måtte være anden (national) lovgivning, som tillige regulerer behandling af sundhedsdata, f.eks. reglerne i sundhedsloven. Databeskyttelsesforordningen forudsætter i mange tilfælde, at der i national lovgivning fastsættes nærmere supplerende regulering.

Sikkerhedsbranchen oplever, at der er stor usikkerhed om, hvornår der er tale om behandling af persondata. **Sikkerhedsbranchen** er endvidere i tvivl om, hvad forskellen er på personfølsomme og særligt følsomme personoplysninger, herunder hvordan de to kategorier af oplysninger skal behandles. Herudover oplyser **Sikkerhedsbranchen**, at foreningen ser en klar tendens til, at vejledninger fra Det Europæiske Databeskyttelsesråd (EDPB), f.eks. vejledning nr. 3/2019 om TV-overvågning, er udtryk for stramninger af den gængse fortolkning af GDPR, og at kunder, f.eks. kommunerne, misforstår disse vejledninger og tror, det er gældende ret.

Begrebet "behandling" er i databeskyttelsesforordningen defineret som enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for.

En behandling kan efter databeskyttelsesforordningen omfatte enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse. Begrebet "behandling af personoplysninger" er med andre ord så bredt defineret, at man som regel vil anses for at udføre en behandling, så snart man kommer i kontakt med personoplysninger om andre.

"Personfølsomme" oplysninger er ikke et begreb, som findes i databeskyttelsesforordningen eller anden databeskyttelseslovgivning. Ifølge databeskyttelsesforordningen kan man inddele personoplysninger i to kategorier. Den første er oplysninger, som udelukkende er omfattet af databeskyttelsesforordningens artikel 6 – såkaldte "almindelige personoplysninger". Den anden er en særlig kategori af oplysninger, som er udtømmende oplistet i forordningens artikel 9 – såkaldte "følsomme personoplysninger". Det drejer sig om personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

I langt de fleste tilfælde vil det være artikel 6, der er den relevante behandlingshjemmel. Dette vil eksempelvis være tilfældet, hvis der behandles navn, telefonnummer og/eller e-mailadresse. Dette indebærer, at personoplysninger – der ikke er særligt reguleret som f.eks.

personnummer eller oplysninger om strafbare forhold – lovligt kan behandles, hvis én af betingelserne i forordningens artikel 6, stk. 1, litra a-f er opfyldt. Behandler man en af de førnævnte "følsomme personoplysninger" skal der tillige være en undtagelse til forbuddet imod behandlingen heraf i databeskyttelsesforordningens artikel 9, stk. 2, eller EU og/eller national ret.

Groft sagt kan man sige, at desto mere beskyttelsesværdig en oplysning er, desto mere skærpede krav til behandlingen heraf gælder der. Dette gælder såvel i forhold til spørgsmålet om hjemmel som i forhold til andre regler i databeskyttelsesforordningen, herunder f.eks. reglerne om behandlingssikkerhed.

I forhold til Sikkerhedsbranchens bemærkninger om vejledninger og/eller retningslinjer fra Det Europæiske Databeskyttelsesråd (EDPB) er disse, som det er tilfældet med Datatilsynets nationale vejledninger, såkaldt "Soft law". Vejledningerne er således ikke i selv bindende over for dataansvarlige, men de vil ofte være udtryk for den forståelse af reglerne, der vil blive håndhævet af de nationale tilsyn.

Den endelige fortolkning af databeskyttelsesreglerne hører imidlertid til hos domstolene, herunder navnlig EU-Domstolen.

Bidrag fra Datatilsynet

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

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