Placering af dataansvar

Allocation of data responsibility

Af MARCUS ANDREAS JENSEN

Afhandlingen behandler grænserne mellem definitionerne på databehandler og dataansvarlig. I den forbindelse gives der en praktisk vejledning til, hvordan man vurderer, hvor det primære ansvar i databeskyttelseslovgivningen skal placeres, og om dette skal deles mellem fælles dataansvarlige.

Begreberne har mødt stor kritik, da definitionerne af databehandler hhv. dataansvarlig er baseret på kriterier, der ikke tager højde for den teknologiske og samfundsmæssige udvikling. Til trods herfor, er begreberne blevet videreført i deres oprindelige form fra persondatadirektivet til databeskyttelsesdirektivet.

Indledningsvist konkluderes det, at begreberne er autonome og skal fortolkes i overensstemmelse med EU's databeskyttelseslovgivning. For at beskytte folk skal begrebet dataansvarlig fortolkes bredt. Herefter defineres begreberne "afgør", "formål" og "hjælpemidler". Dernæst udledes det, hvilke kriterier, der kan bruges til at adskille dataansvarlige og databehandlere fra hinanden.

I henhold til definitionerne af dataansvarlig og databehandler er det kun bestemte typer af subjekter, som kan blive disse. Det fundamentale kriterie er, at et subjekt skal være i stand til at være part i en retssag. Dette udgangspunkt er begrænset af databeskyttelsesforordningens anvendelsesområde, og tilfælde hvor der sker identifikation mellem subjekter.

Afhandlingens sidste del søger at klarlægge, hvornår dataansvarlige deler deres ansvar som fælles dataansvarlige. Dette er betinget af at to eller flere parter i fællesskab afgør enten formål eller væsentlige hjælpemidler. Det er ikke nok, at parterne behandler de samme personoplysninger eller it-systemer. For at en afgørelse om formål eller essenstille hjælpemidler kan siges at være truffet i fællesskab, må begge parter have kendskab til og aktivt have indflydelse på beslutningen. Der eksisterer imidlertid en mulighed for, at EU-Domstolen vil statuere fælles dataansvar ud fra mere praktiske overvejelser.

Indholdsfortegnelse

Engelsk resume

Processing of personal data have become a lot more extensive and specialised with ongoing developments in technology and complexities of value chains since the introduction of the concept of controller and processor in Directive 95/46/EC. The concepts have met a lot of criticism because they are based on criteria which, considering the development of society and technology, are not easy to use. Despite this the concepts have not undergone any changes. The General Data Protection Regulation introduces sanctions of up to 20 M € or 4 % of the total worldwide annual turnover, whichever is higher. If someone makes a wrong qualification of their role, they will most likely not live up to their obligations and can be met with sanctions. The purpose of this thesis is to clarify where and how the data responsibility is allocated.

First it is concluded that the concepts are autonomous and should be interpreted in accordance with EU data protection law. To provide protection for people, the concept of controller must be interpreted widely. Secondly, the concepts "determine", "purpose" and "means" are defined. It is then deduced what criteria can be used to distinguish controllers and processors from each other. A processor can only exist if it receives an assignment from a controller which primarily concerns processing of personal data. Most important is that the processor at no point can determine the purpose or essential means of the processing. In doing so the processor will be acting as a controller.

Only certain subjects can according to the definitions of controller and processor become these. The base criteria must be the capacity to be a party in a court case. This starting point is restricted by the law's field of application and when identification between parties is relevant.

Finally, it is concluded when data controllers share their responsibilities as joint controllers. This is conditioned by two or more parties jointly making a decision about either purpose or essential means. Decide, purpose and essential means must be understood in the same way as when accessing individual data controllership. It is not enough that the parties use the same personal data or it-systems. If a service provider uses a standard contract and leaves no room for the data controller to influence the means or purpose in a contract, it doesn't change the fact that the controller still is in control of whether to use the service or not and therefore the decision of both purpose and essential means. For a decision to be made jointly, both parties must have knowledge of and actively have influence on the decision.

Forkortelser

Art.	Artikel.
Bet.	Betænkning.
DBF	Databeskyttelsesforordningen.
DBL	Databeskyttelsesloven.
Dt	Datatilsynet.
ICO	Information Commissioner's Office (det britiske datatilsyn).
J.nr.	Journalnummer.
PDD	Persondatadirektivet.
PDL	Persondataloven.
Pr.	Præmis.
WP	Working paper (Vejledning eller udtalelse udfærdiget af Artikel 29-gruppen).

I denne afhandling vil referencer til retskilder mv. kunne findes i litteraturlisten. Litteraturlisten indeholder først en forkortelse markeret med fed skrift og herefter kildens komplette angivelse.

1. Indledning

1.1. Præsentation af emnet

Den 25.05.2018 trådte DBF i kraft. Forordningen viderefører i stort omfang begreberne og reglerne fra PDD, men tilføjer også nogle nye, herunder forhøjede bødesatser. Nogle af de begreber, som er indeholdt i PDD og videreført til DBF, har imidlertid mødt stor kritik. Især begreberne *dataansvarlig* og *databehandler* samt disses sammenspil. Begrebet dataansvarlig regulerer, hos hvem det primære ansvar for overholdelse af DBF (herefter også benævnt *dataansvaret*) skal placeres, mens databehandler regulerer, hvornår man kan anses for at behandle personoplysninger på vegne af den dataansvarlige og derfor påtage sig mindre forpligtelser. Grundet begrebernes fundamentale rolle i lovgivningen er det essentielt, at man let kan kvalificere en enhed, der behandler personoplysninger som dataansvarlig eller databehandler.

Den teknologiske udvikling siden 24.10.1995, hvor de to begreber blev vedtaget i deres nuværende form i PDD, har gjort anvendelse af begreberne mere og mere besværlig.[1] Ironisk nok har den samme udvikling bragt anvendelsen af databehandlerkonstruktionen frem.[2] Den teknologiske udvikling har medført, at nogle selskaber har specialiseret sig i levering af tekniske ydelser. Specialiseringen gør, at andre virksomheder ud fra omkostningbesparelseshensyn udliciterer en lang række af tekniske opgaver. Et klassisk eksempel er hosting af hjemmesider og systemer f.eks. via Cloud Computing. Grundet teknologisk specialisering har forretningsmodellerne, der anvender databehandlerkonstruktionen forandret sig således, at det ikke længere er let at sondre imellem de to begreber.[3] Den teknologiske udvikling skal ses i sammenhæng med, at behandling af personoplysninger bliver foretaget i komplekse værdikæder, som gør udfærdigelsen af kontrakter tilsvarende kompleks. I lyset af disse faktorer er det blevet kompliceret at finde frem til hvem af de involverede parter, der afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger, og derved er dataansvarlige.

Begrebernes komplicerede anvendelighed har medført, at de forskellige medlemsstater har udviklet forskellige fortolkninger af, hvordan man foretager vurderingen af, hvor dataansvaret skal placeres.[4] I forbindelse med udfærdigelsen af DBF kunne man have introduceret en ny model, hvor ansvaret f.eks. blev placeret ved den, der var i besiddelse af personoplysningerne, som tilfældet er i Canada, eller have klargjort begreberne på anden vis. Dette blev imidlertid ikke tilgangen. I stedet valgte man at videreføre de hidtil anvendte begreber og placere dataansvaret ved den eller dem, der afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

Uklarheden om hvordan dataansvaret placeres er derfor fortsat et problem, og i lyset af de nye bødesatser, der er indført med DBF, er placeringen særligt vigtig. Bøderne kan nu maksimalt udgøre 20 mio. €, eller hvis det drejer sig om en virksomhed 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere, jf. DBF art. 83, stk. 5. Bødepålæg kommer på tale, når man ikke overholder sine forpligtelser, og alt efter om man er dataansvarlig, databehandler eller deler dataansvar, har man forskellige forpligtelser.

Den dataansvarlige er især forpligtet til, at:

> Sikre, at denne har et selvstændigt behandlingsgrundlag, jf. DBF art. 6, stk. 1,
> Føre fortegnelse, jf. DBF art. 30, stk. 1,
> Føre tilsyn med databehandlere, jf. DBF art. 5, stk. 2,[5]
> Anmelde brud på persondatasikkerheden til tilsynsmyndigheder og underrette registrerede mv., jf. DBF art. 33 og 34,
> Oplyse og besvare anmodninger fra de registrerede om anvendelse af disses rettigheder, jf. DBF kapitel III.

Databehandlere er navnlig forpligtet til, at:

> Handle under den dataansvarliges instruks, jf. DBF art. 28, stk. 3,

[1] Kuner, s. 71 f.
[2] Den nye persondatarets aktører, s. 62.
[3] Kuner, s. 72.
[4] WP 169, s. 2.
[5] Se Dt's vejledende tekst om tilsyn med databehandlere og underdatabehandlere, s. 2.

Bistå den dataansvarlige, jf. DBF art. 28, stk. 3,
Føre en mindre omfangsrig fortegnelse, jf. DBF art. 30, stk. 2.

Fælles dataansvarlige er herudover forpligtet til, at:

Fastlægge deres respektive ansvar for overholdelse af deres forpligtelser i en ordning jf. DBF art. 26, stk. 1.

Sker der en fejlkvalificering, vil parterne formentligt ikke leve op til de korrekte forpligtelser, hvorefter sanktionerne i DBF bliver aktuelle.

DBF har til formål at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder. Dette kan kun lade sig gøre, hvis dem, forordningen finder anvendelse på, er i stand til at identificere deres roller og medfølgende forpligtelser. Der er derfor essentielt at fastlægge, hvordan dataansvaret placeres, så tvivlen ikke kommer til at afskære registrerede fra at anvende deres rettigheder, og derved gøre dem illusoriske eller bliver en hindring for potentielle samarbejder og markedsudviklingen.

1.2. Problemformulering

Denne afhandling vil undersøge og analysere begreberne databehandlere, selvstændig dataansvarlige og fælles dataansvarlige.

1.3. Afgrænsning

Afhandlingen vil ikke behandle definitionen af dataansvarlig, når denne fastsættes gennem EU-retten eller medlemsstaters nationale ret jf. DBF art. 4, nr. 7, 2. led. Ligeledes vil de indholdsmæssige krav til hhv. databehandleraftaler og aftaler om fælles dataansvar samt forpligtelserne, der påhviler hhv. dataansvarlige og databehandlere ikke blive behandlet i andet omfang, end hvor dette er relevant for placeringen af dataansvar. Endeligt vil opgaven ikke behandle afgrænsningen af anvendelsesområdet af DBF overfor aktiviteter i forbindelse med Unionens fælles udenrigs- og sikkerhedspolitik samt overfor retshåndhævelsesdirektivet.

2. Metode og teori

2.1. Metode

For at finde frem til, hvordan dataansvaret placeres, er det nødvendigt at undersøge retstilstanden efter DBF trådte i kraft. Grundet bestemmelsernes videreførelse fra PDD til DBF må retstilstanden under PDD ligeledes undersøges. De traditionelle retskilder vil til dette formål blive inddraget igennem anvendelsen af den retsdogmatiske metode, da gældende ret beskrives, fortolkes, analyseres og vurderes.[6] I denne sammenhæng vil retskildernes styrker og svagheder blive holdt overfor hinanden, og derved vil fortolkningen heraf tage komparativ form.

2.2. Generelle kommentarer vedrørende retskildegrundlaget

I afhandlingen vil de traditionelle retskilder blive inddraget. Retsregler, der har reguleret persondataretten, startede for Danmarks vedkommende med Registerlovene[7] i år 1978. Herefter blev Konvention 108 åbnet for tiltrædelse i 1981, underskrevet af Danmark i år 1989 og trådte i kraft i år 1990.[8] I år 1995 blev PDD vedtaget. PDD blev implementeret i dansk ret igennem PDL som trådte i kraft i år 2000 og erstattede Registerlovene. Den 25.05.2018 fik DBF samt

[6] Evald og Schaumburg-Müller, s, 212.
[7] Lov om offentlige myndigheders registre og lov om private registre.
[8] Chart of signatures and ratifications of Treaty 108.

DBL virkning og erstattede PDD og PDL. DBF har direkte virkning, og findes som bilag 1 til DBL.[9] DBL indeholder de bestemmelser, som er vedtaget inden for det råderum, som DBF har overladt medlemsstaterne.

Med andre ord vil retsgrundlagene Registerlovene, Konvention 108, PDD, PDL, DBF og DBL samt dertil knyttede forarbejder og praksis blive behandlet i denne afhandling, i det omfang det findes relevant. Se hertil også afsnit 3.1.1. Herudover vil relevant retslitteratur blive inddraget.

Særlige bemærkninger skal knyttes til retskildeværdien af Konvention 108, Artikel 29-gruppen og de nationale tilsynsmyndigheder.

Konvention 108 var siden dens åbning for tiltrædelse i 1981, og er fortsat, det eneste juridisk bindende internationale instrument på databeskyttelsesområdet. Begrebet *registeransvarlig* i PDD er baseret på definitionen af *filansvarlig* i Konvention 108.[10] Konvention 108 er blevet modificeret sideløbende med udfærdigelsen af DBF. Begge regeludstedere har været yderst omhyggelige med at sikre sammenhæng og kompatibilitet mellem de to retssystemer.[11] Hvor det findes relevant f.eks. grundet manglende teori eller fortolkningskilder, vil Konvention 108 blive anvendt som et komparativt fortolkningsbidrag grundet den nære sammenhæng mellem den EU-retlige regulering og konventionen.

Artikel 29-gruppen var et rådgivende organ, som har udfærdiget en lang række af vejledninger og udtalelser mv. vedr. persondataret. Artikel 29-gruppen var hjemlet i PDD art. 29 og er nu videreført som Det Europæiske Databeskyttelsesråd, der er hjemlet i DBF art. 68 jf. DBF art. 94, stk. 2, 2. pkt. Artikel 29-gruppen havde ingen kompetence i forhold til afgørelser, og dets arbejde var alene af vejledende karakter. Organet bestod af en repræsentant fra hver tilsynsmyndighed i samtlige medlemsstater, repræsentanter fra EU's persondataretlige organer, samt en repræsentant for Kommissionen.[12] Det må på baggrund af medlemmerne kunne lægges til grund, at organet besad en stor faglig viden indenfor persondataretten, hvorfor deres arbejde må kunne tillægges vægt som specialviden. Artikel 29-gruppens udtalelser og vejledninger er da også nævnt flere gange bl.a. i bet. 1565/2016 om DBF, og i Generaladvokaters forslag til afgørelser.[13] Artikel 29-gruppens arbejde fik også betydning for national praksis, fordi medlemmerne er repræsentanter fra de nationale tilsynsmyndigheder, som i første instans tager stilling til lovligheden af behandling.

De nationale tilsynsmyndigheder har dannet praksis og vejledninger på baggrund af den til enhver tid gældende persondataretlige lovgivning. De har bl.a. kompetence til at udstede advarsler, påtale overtrædelser og indbringe disse for domstolene.[14] Deres administrative praksis er som udgangspunkt første trin i retssager vedr. persondataret. Praksis og vejledninger er derfor relevante kilder.

3. Dataansvarets placering

Denne opgave har til sigte at fastslå, hvordan dataansvaret placeres. Det mål opnås ved først at undersøge, hvilke retskilder der kan anvendes ved fastlæggelsen af begrebet dataansvarlig, og

[9] Debatten, om hvorvidt det er nødvendigt at implementere forordninger i national lov, vil ikke blive behandlet i denne afhandling.
[10] COM (90) 314 final, s. 19 f.
[11] Handbook on European data protection law, s. 12 og 26.
[12] PDD art. 29, stk. 2.
[13] Se bl.a. forslag til sag C-210/16 Wirtschaftsakademie og forslag til sag C-25/17 Jehovan.
[14] Se PDD art. 28, stk. 3 og DBF art. 58.

hvordan begreberne skal fortolkes, hvilket sker i afsnit 3.1. Igennem afhandlingen vil de relevante kilder og fortolkningsfaktorer blive anvendt til at fastlægge, hvor og ud fra hvilke kriterier dataansvaret placeres. I de følgende afsnit 3.2-3.4 vil det blive søgt at klarlægge, hvor og hvordan dataansvaret kan placeres. Strukturen heraf følger de tre elementer, man kan opdele definitionen af den dataansvarlige i. De tre elementer er som følger:

1. *en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ,*
2. *der alene eller sammen med andre*
3. *afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger*

Dataansvaret kan for det første pålægges en nærmere specificeret række af subjekter, for det andet kan ansvaret pålægges et eller flere subjekter i fællesskab, og for det tredje pålægges dataansvaret det eller de subjekter, der afgør formålet eller formålene med og hjælpemidlerne, der må anvendes ved behandlingen af personoplysninger.

I afsnit 3.2 vil der blive set på det tredje element, som er den egentlige kvalificering af ansvaret. Herefter vil rækkevidden af de mulige ansvarssubjekter blive undersøgt i afsnit 3.3. I afsnit 3.4 vil grænserne for ansvarets deling mellem flere subjekter blive vurderet.

3.1. Formelle vurderinger

Begrebet dataansvarlig er defineret i DBF. Definitionen er imidlertid ikke klar eller fyldestgørende, hvorfor fortolkningen af begrebets definition må ske i teori og praksis. DBF fik virkning den 25.05.2018. Fra denne dag blev der indgivet klager på dette lovgrundlag.[15] EU-retspraksis under DBF er dog begrænset, idet behandlingstiden af et præjudicielt spørgsmål gennemsnitligt var 15,7 måneder og behandlingstiden for sager, som afsluttedes ved dom eller kendelse gennemsnitligt var 16,3 måneder i 2017.[16] Dt har da heller ikke i skrivende stund offentliggjort en udtalelse eller afgørelse, der anvender det nye retsgrundlag. Henset til den manglende praksis efter DBF er det derfor essentielt at finde frem til om, og i givet fald hvilken, teori og praksis fra tidligere lovgivning man kan anvende.

3.1.1. Begrebernes autonomi

Det vi i dag betegner som databehandlerkonstruktionen, hvor en part udfører behandling af personoplysninger på vegne af en anden, er ikke ny. Siden de danske registerlove[17] har konstruktionen været kendt,[18] men begreberne har ændret sig i takt med den teknologiske og samfundsmæssige udvikling. Det er derfor væsentligt at få afdækket, om fortolkningen af begreberne fortsat kan bero på teori og praksis tilbage fra registerlovene eller efterfølgende lovgivning.

Grundet Europarådets bekymringer om, at medlemsstaternes nationale lovgivning om beskyttelse af personlige oplysninger var mangelfulde i lyset af den hurtige teknologiske udvikling, valgte Europarådet at udstede Recommendation 509 on Human Rights and Modern and Scientific Technological Developments. På baggrund af denne anbefaling blev resolution 73/22 og

[15] Der blev indgivet klager af bl.a. nonprofitorganisationen noyb.eu (None of your buisness). Se hertil noyb.eu.
[16] EU-domstolens pressemeddelelse nr. 36/18.
[17] Lov om offentlige myndigheders registre og Lov om private registre.
[18] Lov om private registre § 20.

74/29 skabt. Heri blev medlemsstaterne anbefalet at vedtage regler om behandlingen af personlige oplysninger. Som reaktion på disse valgte man i Danmark at vedtage de danske registerlove i år 1978. Reguleringen var således alene på nationalt niveau. I modsætning til DBF anvendte Registerlovene betegnelsen registeransvarlig for det primære ansvarssubjekt i denne lovgivning, og Edb-servicebureauer for en størrelse der lignede databehandlere. Begrebet registeransvarlig blev imidlertid defineret ud fra praksis og ikke direkte i Registerlovene.[19] Begrebet Edb-servicebureauer blev defineret i Lov om private registre § 20, stk. 1 som:

> *"Virksomheder, der for tredjemand, herunder for en offentlig myndighed, ud fører elektronisk databehandling af oplysninger som nævnt i § 1, skal forinden foretage anmeldelse til registertilsynet."*

Som efterfølger til Registerlovene kom PDL, der implementerede PDD. I den danske version af PDD blev begrebet registeransvarlig anvendt, mens PDL anvendte begrebet dataansvarlig. Disse begreber skal forstås som synonymer.[20] PDL § 3, nr. 4 definerede den dataansvarlige som:

> *"Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger."*

Begrebet databehandler blev defineret i PDL § 3, nr. 5 som:

> *"Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne."*

I bet. 1342/1997[21] fremgår det, at begrebet databehandler var nyt, men indholdsmæssigt måtte svare til, hvad der fremgik af Lov om private registre § 20, stk. 1.[22] Begrebet dataansvarlig var ikke defineret i registerlovene, men indholdsmæssigt måtte det svare til begrebet registeransvarlig som defineret i retspraksis efter registerlovene. Herefter antoges det, at praksis fra Registerlovene fortsat kunne tillægges betydning.[23]

PDL er en implementering af PDD, og derfor kan anvendelsen af Registerlovene og deres praksis som fortolkningsbidrag syntes problematisk henset til kravene om en ensartet anvendelse af EU-retten og lighedsprincippet, som er fastslået gentagne gange i EU-retspraksis.[24] I flere afgørelser er det fastslået, at:

> *"ordlyden af en EU-retlig bestemmelse, som ikke indeholder nogen udtrykkelig henvisning til medlemsstaternes ret med henblik på at fastlægge dens betydning og rækkevidde, normalt i hele Unionen skal undergives en selvstændig og ensartet fortolkning, som skal søges under hensyntagen ikke alene til bestemmelsens ordlyd, men ligeledes*

[19] Registerlovene blev erstattet af PDL. I denne forbindelse blev bet. 1342/1997 udfærdiget. Af betænkningens s. 433 fremgår det, at begreberne blev fastsat på ulovbestemt grundlag.
[20] Bet. 1342/1997, s. 210.
[21] Se fn. 19.
[22] Ibid. s. 434.
[23] Ibid. s. 433.
[24] Se bl.a. C-327/82 Ekro, pr. 11; C-34/10 Brüstle, pr. 25; C-201/13 Deckmyn og Vrijheidsfonds, pr. 14; C-544/13 og C-545/13 Abcur, pr. 45.

til den sammenhæng, hvori bestemmelsen indgår, og det formål, som forfølges med den pågældende ordning."

Dette princip indeholder et udgangspunkt om EU-konform fortolkning og en undtagelse. Undtagelsen kommer i form af retten til at fastsætte en bestemmelses betydning og rækkevidde ved udtrykkelig henvisning til EU- eller national ret. I det følgende vil udgangspunktet blive behandlet først, og herefter vil undtagelsen blive adresseret.

Udgangspunktet er, at ordlyden af EU-retlige bestemmelser, såsom definitionen af dataansvarlig og databehandler, skal undergives en selvstændig EU-retlig fortolkning, og er således autonome begreber. Det udelukker dog ikke, at tidligere national retspraksis vedrørende disse eller lignende begreber kan være i overensstemmelse med fortolkningen af de EU-retlige begreber. Det kan imidlertid ikke vides med sikkerhed, forinden EU-begreberne er blevet underkastet en sådan fortolkning. Retspraksis fra registerlovene bør derfor som udgangspunkt ikke anvendes som bidrag til fortolkningen af begreberne.

At begreberne skal fortolkes som autonome EU-retlige begreber stemmer godt overens med baggrunden for både DBF og PDD. PDD blev vedtaget for at harmonisere medlemsstaternes love på det persondataretlige område, for at sikre beskyttelsen af fysiske personer, og for at ophæve hindringerne for udveksling af personoplysninger inden for EUs rammer. De forskellige nationale lovsæt, som regulerede, hvornår personoplysninger kunne overføres imellem medlemsstaterne, var varierende og udgjorde derved en hindring for det indre markeds funktion.[25] Ved harmonisering af reglerne ville hindringerne blive ophævet, og en klarere retsstilling ville sikre bedre beskyttelse af fysiske personer. DBF har til sigte at indføre yderligere harmonisering med henblik på at beskytte medlemsstaternes borgere ens, og derved ophæve hindringer for det indre marked.[26] Begge lovsæt har haft til formål at harmonisere lovområdet. Dette kan ikke opnås, hvis de EU-retlige begreber skal fortolkes i lyset af hver enkelt nationale medlemsstats tidligere praksis.

Det kan konkluderes, at begreberne må fortolkes som EU-retlige begreber. Dette afskærer muligheden for at tillægge national praksis fra før PDD og PDL direkte retskildeværdi. I stedet kan der ved fortolkningen anvendes almindelige fortolkningsprincipper på de EU-retlige kilder.[27]

Da DBF forfølger samme formål som PDD, og viderefører disse,[28] må den viden, vi har om PDDs bestemmelser kunne videreføres, fsv. de ikke indholdsmæssigt afviger fra DBF. Bestemmelserne, der definerer dataansvarlig og databehandler i DBF, er praktisk talt identiske med

[25] COM (90) 314 final, s. 4; PDD præambelbetragtning nr. 8 og 9; PDD art. 1, stk. 1; DBD præambelbetragtning nr. 3.
[26] DBF præambelbetragtning nr. 9 og 10 samt art. 1, stk. 2.
[27] EU-retskilderne omfatter traktaterne, sekundære retsregler (herunder hører nationale implementeringslove), traktater indgået af Unionen med tredjestater eller internationale organisation, domspraksis, retsgrundsætninger og grundrettigheder.
Med fortolkningsprincipperne tænkes der på den sproglige og ordlydsmæssige fortolkning, som kan suppleres af ordlyden af betragtninger til retsakter, formålsfortolkning og den kontekstuelle fortolkning jf. C-283/81 CILFIT, pr. 18-20.
[28] PDD art. 1 beskriver direktivets formål, som er beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder. DBF art. 1, stk. 2 fastslår, at DBF har til formål at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder. Begge lovsæt forfølger altså det samme formål. DBF forfølger dette formål, men medlemsstaternes råderum ved implementering begrænses væsentligt, da der netop er tale om en forordning. Herved sikres større harmonisering. Med andre ord så er midlet med henblik på at forfølge formålet blevet forstærket.

PDD,[29] hvorfor praksis vedr. disse begreber fortsat har præjudikatværdi. Praksis fra EU-domstolen og medlemsstaterne på baggrund af implementeringen af PDD vil derfor blive inddraget i denne afhandling.

Undtagelsen til udgangspunktet er aktuel, når en EU-retlig bestemmelse *indeholder en udtrykkelig henvisning til medlemsstaternes ret med henblik på at fastlægge dens betydning og rækkevidde*. Dette findes i definitionen af dataansvarlig i DBF art. 4, nr. 8, 2. led. I bestemmelsen står der, at:

> *"hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret.*"

Denne undtagelse tillader EU og medlemsstaterne ved ret at fastsætte, hvem der er dataansvarlig eller hvilke kriterier, der skal anvendes til udpegelse af en dataansvarlig på betingelse af, at både formålene og hjælpemidlerne er fastlagt i ret. Hvis fortolkningen af et retsgrundlag ikke fører til identifikation af den dataansvarlige, vil en normal vurdering af dataansvaret placering skulle gennemføres.[30]

Henset til opgavens afgrænsning som fastsat i afsnit 1.3 vil undtagelsen ikke blive behandlet yderligere.

3.1.2. Begrebets relative størrelse i lyset af formål og kontekst

Det følger yderligere af princippet om EU-konform fortolkning ovenfor, at fortolkningen af en EU-retlig bestemmelse skal ske under hensyntagen til bestemmelsens ordlyd, sammenhængen den indgår i, samt formålet, der forfølges med den pågældende ordning. I det følgende vil "sammenhængen bestemmelserne indgår i" blive betegnet som bestemmelsernes kontekst.

Her skal det undersøges, hvilke formål bestemmelserne forfølger, og hvilken kontekst disse indgår i. Bestemmelsernes ordlyd vil blive behandlet nedenfor i afsnit 3.2-3.4.

I forhold til begrebernes kontekst er det i princippet om EU-konform fortolkning ikke nærmere specificeret hvilken kontekst, der kan inddrages i fortolkningen af begreberne. Den lovmæssige kontekst er imidlertid nærliggende at starte med.

PDD og DBF har til formål at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder.[31] Dette mål opnås igennem to typer af bestemmelser.[32] For det første med proaktive bestemmelser, som pålægger et subjekt at implementere beskyttelsesforanstaltninger. For det andet igennem reaktive bestemmelser, der pålægger sanktioner og tillader erstatningssøgsmål. De to typer af bestemmelser er naturligt sammenhængende. Proaktive bestemmelser pålægger forpligtelser, og reaktive fastsætter følgerne af manglende overholdelse. I lovkonteksten er den dataansvarlige og databehandleren altså pligtsubjekter. PDD og DBF opnår deres formål bl.a. ved anvendelsen af begrebet dataansvarlig, som primært pligtsubjekt for lovgiv-

[29] Den eneste forskel er at PDD anvender ""den" fysiske eller juridiske…" hvorimod DBF anvender ""en" fysisk eller juridisk…" Der er alene tale om en grammatisk forskel, som ingen betydning har på definitionerne.
[30] Motzfeldt, s. 73.
[31] Se fn. 27.
[32] WP 169, s. 4 f.

ningens forpligtelser. Dette blev også fastslået af EU-domstolen i bl.a. sag C-210/16 Wirtschaftsakademie hvori formålet med definitionsbestemmelsen af den dataansvarlige blev fastslået. EU-domstolen udtalte, at definitionsbestemmelsens formål er:

> *"at sikre en effektiv og fuldstændig beskyttelse af de berørte personer ved at fastsætte en bred definition af begrebet »dataansvarlig«."*[33]

Den dataansvarlige er det primære ansvars- og pligtsubjekt og med henblik på at sikre en effektiv og fuldstændig beskyttelse af de berørte personer, må begrebet fortolkes udvidende. Eftersom databehandleren er en, der behandler personoplysninger på vegne af den dataansvarlige, vil den udvidede fortolkning af begrebet dataansvarlig ske på bekostning af databehandlerbegrebets anvendelsesområde.

Denne konklusion støttes da også af begrebernes kontekst i lovgivningen. Det følger af PDD art. 6, stk. 2 og DBF art. 6, stk. 2, at den dataansvarlige er ansvarlig for, at principperne for behandling af personoplysninger overholdes. Herudover er den dataansvarlige ansvarlig for overholdelsen af de registreredes rettigheder. Ud fra lovkonteksten er det altså klart, at formålet med begrebet "Dataansvarlig" er at placere det primære ansvar for overholdelse af PDD og DBF. Dette synspunkt støttes også af Artikel 29-gruppen.[34]

En anden kontekst, der er relevant for fortolkningen, er den praktiske og samfundsmæssige kontekst, som begreberne anvendes i. At bestemmelserne må ses i denne kontekst synes også logisk henset til, at DBFs formål er at beskytte medlemsstaternes borgere ens, og derved ophæve hindringer for det indre marked. Dette opnås kun i praksis, såfremt begreberne kan vurderes ud fra den samfundsmæssige kontekst og i lyset af den teknologiske udvikling. DBF har da også direkte nævnt disse faktorer i præambelbetragtning nr. 6 og 7.

Det kan konkluderes på baggrund af lovens formål og præambelbetragtninger, at det er et beskyttelseshensyn overfor borgerne og et effektivitetshensyn overfor det indre marked, som må inddrages i det følgende. Det må også konkluderes, at der ikke kan opstilles en udtømmende liste af hvilke kontekster, der kan inddrages, når et EU-retligt begreb skal fortolkes. Den manglende specificering af "kontekst" i princippet om EU-konform fortolkning taler i sig selv for, at relevante kontekster kan inddrages. I resten af denne afhandling vil kontekst derfor få betydning for fortolkningen af begreber. Særligt vedr. begrebet dataansvarlig er det bl.a. i sag C-210/16 Wirtschaftsakademie fastslået, at dette begreb må fortolkes bredt for at sikre lovgivningens formål.

3.2. Afgør, formål og hjælpemidler

På baggrund af det ovenfor gennemgåede skal det nu undersøges, hvordan dataansvaret skal placeres. Det første af de tre elementer i definitionen, der skal behandles, er, hvornår man afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

For at besvare dette spørgsmål, vil det først blive undersøgt, om vurderingen af hvem der afgør, skal bero på de faktiske omstændigheder, eller om det må vurderes ud fra en formel udpegning i f.eks. en kontrakt. Dernæst vil begreberne formål og hjælpemidler blive defineret. Til sidst

[33] C-210/16 Wirtschaftsakademie, pr. 28.
[34] WP 169, s. 4.

vil der ske en afgrænsning af dataansvaret overfor databehandlervirksomhed, for klart at fastlægge, hvornår dataansvaret aktualiseres.

3.2.1. Formel eller faktuel vurdering af "at afgøre"

For at kunne placere et dataansvar, er det nødvendigt at vide, om et sådant skal placeres ud fra de faktiske omstændigheder eller ud fra hvem, der er blevet tildelt kompetencen til at agere som dataansvarlig f.eks. igennem en kontrakt.

Definitionen af dataansvarlig anvender begrebet "afgør", hvilket taler for, at den dataansvarlige er den, der faktisk træffer afgørelse om formål og hjælpemidler, og at dataansvaret ikke pålægges den, der alene formelt har en kompetence til at træffe en sådan afgørelse. Undtagelsen i DBF art. 4, nr. 8, 2. led medfører dog, at der kan anvendes en rent formel vurdering, såfremt dette er fastsat i lov. Undtagelsen vil ikke blive selvstændigt behandlet henset til denne opgaves afgrænsning, men indførelsen af en sådan undtagelse sammenholdt med hovedreglens formulering må tages som udtryk for, at udgangspunktet er, at der skal foretages en faktuel vurdering af, hvem der træffer afgørelse over formål og hjælpemidler. Dersom dette ikke var udgangspunktet, kunne hovedreglen være formuleret anderledes f.eks. ved at anføre, at den dataansvarlige er "den der er kompetent til at afgøre" frem for at være den, der "afgør". Det første udkast til PDD taler dog imod denne forståelse. Heraf fremgår det, at den dataansvarlige er den, *der i henhold til fællesskabsretten eller en medlemsstats lovgivning er beføjet til at afgøre*.[35] Denne formulering blev dog ændret inden vedtagelsen af direktivet, således at bestemmelsen blev toleddet som behandlet i afsnit 3.1.1.

I litteraturen har der også været delte meninger.[36] Artikel 29-gruppen kom med et bidrag til diskussionen i en udtalelse om begreberne "dataansvarlig" og "databehandler". Artikel 29-gruppen anførte, at det er naturligt, at placeringen af dataansvar må gennemføres ud fra de faktiske omstændigheder og ikke en formel kompetence til at træffe afgørelse.[37] At foretage vurderingen på baggrund af formelle kriterier såsom fastsættelse i en kontrakt ville i visse tilfælde være utilstrækkeligt og ikke reflektere virkeligheden.

Et krav om formel kompetence vil også at give anledning til problemer i tilfælde, hvor behandling foretages ulovligt. Modsat vil en faktuel vurdering tillade muligheden for at placere et ansvar ved den, der foretager ulovlig behandling, såfremt denne afgør formål og hjælpemidler.[38] Et eksempel herpå er, at en person, der opnår ulovlig adgang til personoplysninger som dankortinformationer for at videresælge disse, kan pålægges dataansvar.

Vurderingen af de faktiske omstændigheder har også vundet støtte i Europarådets Konvention 108, der blev ændret den 18.05.2018.[39] I denne sammenhæng blev definitionen af dataansvarlig ændret. I en forklarende rapport til konventionsændringen uddybes definitionen af "Dataansvarlig" med følgende:

[35] KOM (90) endelig udg. — SYN 287.
[36] Se Motzfeldt, s. 74. Her fastslår forfatteren, at der ikke i dansk litteratur er taget direkte stilling til spørgsmålet, men flere synes at have tilsluttet sig en faktuel fortolkning, og at de norske persondataeksperter Dag Wiese Schartum og Lee A. Bygrave har tilsluttet sig den formelle fortolkning.
[37] WP 169, s. 8 f.
[38] Ibid.
[39] Den moderniserede Konvention 108.

> *"Dataansvarlig refererer til den person eller organisation, der har kompetencen til at træffe afgørelse om formål og midler til behandlingen,* ***omend denne kompetence stammer fra en juridisk udpegning eller faktiske omstændigheder****, som skal vurderes fra sag til sag."*[40]

Der sondres her ligeledes mellem en formel udpegning i lov eller andet juridisk bindende dokument, og såfremt dette ikke er sket, foretages vurderingen ud fra de faktiske omstændigheder.

Dt har i dets vejledning om dataansvarlige og databehandlere ligeledes understreget, at de anvender en faktuel fortolkning.[41]

> *"Når du og dine medparter indgår en aftale -, der indebærer at der vil blive behandlet personoplysninger - og i den forbindelse fastlægger hver af jeres ansvar for behandlingen, er det* ***i alle tilfælde vigtigt, at denne aftale afspejler virkeligheden.*** *I kan således f.eks. ikke beslutte en rollefordeling, der går ud på, at du er dataansvarlig og at en anden part er databehandler, hvis det i virkeligheden er den anden part, der træffer alle væsentlige beslutninger om behandlingens formål og hjælpemidler."*

Den svenske tilsynsmyndighed Datainspektionen har i dets praksis efter PDD fastslået, at det er de faktiske omstændigheder, som afgør, hvem der pålægges dataansvaret.[42]

Modsat synes det ikke at være klart tilkendegivet fra den norske tilsynsmyndighed, om denne tilslutter sig Artikel 29-gruppens, Dt's og det svenske Datainspektions fortolkning. Bl.a. anvender de alene definitionens ordlyd og forholder sig ikke konkret til spørgsmålet i deres vejledning om databehandleraftaler.[43] Der er imidlertid god sandsynlighed for, at det norske datatilsyn vil tilslutte sig den øvrige konsensus. Den 08.05.2018 indgik de nordiske tilsynsmyndigheder en københavner-erklæring.[44] I denne erklæring fremgår det, at tilsynsmyndighederne vil dele hinandens materiale for at undgå, at de enkelte tilsynsmyndigheder enkeltvis skal skabe de samme informationer og herved yde mere vejledning. Det antydes klart med tilkendegivelsen, at tilsynsmyndighederne skal have de samme resultater eller fortolkninger i og med, at de danner de samme informationer. En konform fortolkningsstil vil derfor være en naturlig følge.

I forslag til sag C-210/16 Wirtschaftsakademie anførte Generaladvokat Y. Bot, at dataansvaret må placeres ud fra en vurdering af de faktiske omstændigheder, som Artikel 29-gruppen også gør gældende.[45]

Sagen omhandlede bl.a. hvorvidt Facebook kunne anses for at dele dataansvar med administratorerne af fansider på platformen. Han pointerede, at det fremgår af sagens akter, at Facebook Inc. og Facebook Ireland generelt havde anført Facebook Ireland som dataansvarlig i EU.[46] Facebook havde begrundet dette med, at Facebook Ireland traf afgørelse, både om hvilke af de universelle funktioner de ønskede at udbyde, og hvilke nye funktioner de ønskede at indføre eksklusivt for registrerede i EU.[47] Dette kan tolkes således, at Facebook foretog en formel an-

[40] Explanatory Report to CETS No. [223], s. 4.
[41] Dt's vejledning om dataansvarlige og databehandlere, s. 10.
[42] Datainspektionen, j.nr. 111-2014, s. 3.
[43] Datatilsynet (Norge) vejledning om databehandleraftaler.
[44] Se litteraturliste under København-erklæring.
[45] Forslag til sag C-210/16 Wirtschaftsakademie, pr. 46.
[46] Ibid. pr. 49.
[47] Ibid. fn 22.

svarsplacering. Generaladvokat Y. Bot tilsidesatte denne formelle ansvarsplacering, og på baggrund af de faktiske omstændigheder anførte han, at der måtte forelægge fælles dataansvar mellem Facebook Inc. og Facebook Ireland.[48]

Dommen i sagen er imidlertid noget mindre nuanceret. EU-domstolen slog fast, at det fandtes ubestridt, at Facebook Inc. og Facebook Ireland var dataansvarlige.[49] Retskildeværdien må derfor anses som værende meget begrænset.

Spørgsmålet må imidlertid anses for at være afgjort i sag C-25/17 Jehovan. Sagen omhandlede bl.a., hvorvidt trossamfundet Jehovas Vidner var fælles dataansvarlige med de medlemmer af samfundet, som gik fra dør til dør, for så vidt angår de personoplysninger, der blev indsamlet i denne sammenhæng. Her fastslog EU-domstolen, at fælles dataansvar indebærer, at flere parter kan anses for ansvarlige for samme behandling af personoplysninger.[50] Dette betyder ikke, at et fælles dataansvar medfører, at parterne har lige stort ansvar.[51] EU-domstolen fulgte med:

> *"67 I denne forbindelse giver hverken ordlyden af artikel 2, litra d), i direktiv 95/46 eller nogen anden bestemmelse i dette direktiv anledning til at antage, at fastlæggelsen af formålet med og hjælpemidlerne ved behandlingen skal gennemføres ved skriftlige retningslinjer eller anvisninger fra den registeransvarlige.*
>
> *68 En fysisk eller juridisk person, der til eget formål udøver indflydelse på behandlingen af personoplysninger og grundet den omstændighed deltager i fastlæggelsen af formålene med og hjælpemidlerne ved denne behandling, kan til gengæld anses for registeransvarlig som omhandlet i artikel 2, litra d), i direktiv 95/46."*

EU-domstolen fastslog, at skriftlighed eller anvisning ikke er en betingelse for at placere et dataansvar. Den, der aktivt deltager i fastlæggelsen af formål og hjælpemidler, kan ifalde dataansvar. Ved først at afvise nødvendigheden af en formel ansvarsplacering og herefter fastslå at det er den, der aktivt og faktisk afgør formål og hjælpemidler, der bærer dataansvar, må det konkluderes, at dataansvaret placeres ud fra de faktiske omstændigheder.

3.2.2. Kompetencen til at afgøre

Den dataansvarlige er den, der træffer afgørelse om, til hvilke formål og med hvilke hjælpemidler behandling af personoplysninger må foretages. Som det blev konkluderet ovenfor i sag C-25/17 Jehovan, må det anses som et krav for at blive pålagt dataansvaret, at et subjekt faktisk har indflydelse på eller udøver en kompetence til at træffe afgørelsen.

Med henblik på at gøre den faktuelle vurdering simplere og derved mere forudsigelig har Artikel 29-gruppen anført, at den kontrol man faktisk skal besidde for at kunne træffe afgørelse om formål og hjælpemidler, kan oprinde fra tre forskellige kilder.[52] De tre kilder kan opstilles således:

1. Kontrollen kan være fastsat direkte eller indirekte i lovgivningen. Kontrollen kan være fastsat i lovgivningen, f.eks. når kompetencen til at definere dataansvaret i EU- eller national lov jf. DBF art. 4, nr. 7, 2. led anvendes. Hyppigere findes der dog lovgivning,

[48] Ibid. pr. 51.
[49] C-210/16 Wirtschaftsakademie, pr. 30.
[50] C-25/17 Jehovan, pr. 65.
[51] Ibid. pr. 66.
[52] WP 169, s. 9 f.

hvoraf kompetencen til at træffe afgørelse indirekte fremgår. Som eksempler herpå kan nævnes hvidvaskloven og bogføringsloven. Begge disse love definerer en part, som er forpligtet til at opbevare specifikke typer af dokumenter mv.

2. Kontrollen kan stamme fra det, Artikel 29-gruppen betegner som implicit kompetence. Med implicit kompetence menes der forhold, hvor kompetencen kan udledes af en konstruktion, der er nedfæstet i lov eller fast praksis. Som eksempler herpå nævnes ansættelsesforhold, hvor arbejdsgiver naturligt vil være at anse som dataansvarlig for dennes arbejdstageres personoplysninger.
3. For det tredje kan kontrollen over afgørelsen stamme fra faktisk omstændigheder. Denne kontrol vil kunne ses i f.eks. aftale- og kontaktforholdsregulerede samarbejder. Her kan en retvisende kontrakt ofte antyde, om en og i givet fald hvilken part, der har kompetencen til at træffe afgørelse om formål og hjælpemidler. Vurderingen af kontrollen vil imidlertid altid blive foretaget ud fra de faktiske omstændigheder og ikke på baggrund af f.eks. en kontrakt. Denne kontrol omfatter også de tilfælde, hvor behandling bliver foretaget ulovligt, fordi den alene ser på hvem, der har kontrollen ud fra de faktiske omstændigheder.

På baggrund af ovenstående må det fastslås, at der ikke kan pålægges et dataansvar, såfremt en part ikke har kontrol over afgørelsen om formål og hjælpemidler. Det udelukker imidlertid ikke mange situationer, da den tredje kilde fungerer som en opsamlingskilde. Opdelingen er dog praktisk anvendelig og giver et peg mod de steder, kontrollen kan findes.

3.2.3. Definitionen af formål og hjælpemidler

Udøvelse af kontrollen over eller faktisk indflydelse på afgørelsen er det første element i vurderingen af, hvordan dataansvaret placeres, og kan ikke stå alene. Afgørelsen skal ifølge definitionens ordlyd omhandle formålene med og hjælpemidlerne, der må anvendes ved behandlingen af personoplysninger. Det er derfor nødvendigt at fastlægge, hvad der ligger i begreberne formål og hjælpemiddel.

Artikel 29-gruppen henviste i deres udtalelse om dataansvarlige og databehandlere til definitionen af formål som *"et forventet resultat, der er tilsigtet eller guider dine planlagte handlinger."*[53] Ud fra definitionen er begrebet en meget løs og omfangsrig størrelse. Artikel 29-gruppen sidestillede behandlingens formål, med "hvorfor" der behandles personoplysninger.

Når man skal finde formålet med en behandling, skal man se på det faktiske formål og ikke det lovlige formål.[54] Dataansvaret skal for at sikre effektiv beskyttelse kunne pålægges folk, der handler ulovligt. Dataansvar skal som ovenfor under afsnit 3.2.1 anført vurderes på baggrund af de faktiske omstændigheder. Det medfører, at undersøgelsen af formålet, som er en del af definitionen af dataansvarlig, ligeledes må vurderes ud fra de faktiske omstændigheder. Når man ser på formålet, må det altså være i dets rene forstand. Enhver vurdering af lovlighed må foretages selvstændigt. Formålet med en behandling skal altså forstås ud fra deres legaldefinition for at harmonere med kravet om en faktisk vurdering af dataansvaret.

[53] WP 169, s. 13.
[54] Ibid. s. 9.

Formål som begreb er imidlertid en relativ størrelse, der medfører, at man kan have et hovedformål f.eks. personaleadministration og heri subformål såsom administration af ferie, sygedage, løn mv.[55] Da der nedlægges en faktisk vurdering af dataansvaret, vil en domstol kunne finde et formål af den størrelse, den finder passende for den i en sag relevante behandling, så længe det er indeholdt i sagens omstændigheder.

Definitionen af hjælpemidler er ifølge Artikel 29-gruppens henvisning *"måden hvorved et resultat er opnået eller et mål er nået"*.[56] Dette sidestilles med, "hvordan" personoplysninger behandles. Begrebet hjælpemiddel er, ligesom begrebet formål, en ekstremt løs størrelse, som kan dække utroligt bredt.

I det oprindelige forslag til PDD indebar definitionen af den registeransvarlige, at denne var:

> *"beføjet til at afgøre, hvad et register måtte bruges til, hvilke typer personoplysninger der måtte registreres i det, hvilke operationer de måtte underkastes og hvilke tredjemænd der må få adgang hertil."*[57]

Definitionen blev ændret inden vedtagelsen af det endelige lovforslag, således at den registeransvarlige ville være den der afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. Elementerne i definitionen af den dataansvarlige, som fremført i forslaget til PDD, kan fortolkes indeholdt i DBF definition af begrebet.[58] Formuleringen i forslaget til PDD, der lyder, *"hvad et register må bruges til"* må kunne sidestilles med, hvorfor der behandles personoplysninger, og altså hvilke formål der forfølges.[59] Spørgsmålet er herefter, om de tre øvrige kriterier kan subsumeres under betegnelserne formål eller hjælpemidler.

Artikel 29-gruppen anførte uden yderligere begrundelse, at den endelige definition af dataansvarlig alene skal forstås som en forkortelse af den oprindelige.[60] Derfor antages det, at afgørelsen af hvilke typer af personoplysninger der må registreres, hvilke aktiviteter de måtte underkastes og hvilke tredjemænd der må få adgang hertil, skal ses som en afgørelse af hjælpemidler. Med denne fortolkning indebærer hjælpemidler ikke alene tekniske spørgsmål, såsom hvilke it-programmer skal behandlingen udføres med, men også organisatoriske elementer.

Synspunktet giver dog mening, hvis man kigger på de enkelte elementer, og holder dem op overfor definitionen af et hjælpemiddel. Valget af hvilke personoplysninger, der må behandles, hvilke aktiviteter eller behandlinger personoplysninger må underkastes og hvilke ansatte, der må have adgang til personoplysninger, må anses som organisatoriske spørgsmål. Alle disse kan ordlydsmæssigt anses som værende elementer, der udgør *"måden hvormed et resultat opnås"* og derfor indeholdt i definitionen af et hjælpemiddel.

Yderligere må kravet om, at begrebet dataansvarlig skal fortolkes bredt, for at sikre borgernes beskyttelse, tale for, at afgørelsen af disse elementer kan medføre dataansvar, særligt henset til

[55] Bet. 1565/2016, s. 452.
[56] WP 169, s. 13.
[57] KOM (90) endelig udg. — SYN 287.
[58] Fortolkningen af PDD legaldefinitioner kan anvendes ved fortolkningen af DBF jf. afsnit 3.1.1, da dataansvarligdefinitionen i det endelige PDD er indholdsmæssigt identisk med definitionen i DBF.
[59] WP 169, s. 14.
[60] Ibid. s. 14.

disses essentielle betydning. Imidlertid synes det ikke praktisk hvis en part, der alene pga. dennes tekniske specialisering skal ifalde dataansvar ved at vælge hvilken software, der er egnet til at gennemføre en given behandling. Særligt henset til den dataansvarliges byrdefulde forpligtelser. Der lader da også til at være bred konsensus om, at der kan ske en vis uddelegering af kompetencen til at træffe afgørelse om hjælpemidlerne til en databehandler, uden at denne ifalder dataansvar.[61] Grænserne herfor vil blive undersøgt nærmere nedenfor i afsnit 3.2.6.

Af interesse er det, at Europarådet ikke synes at være enige i, at de tre ovenfor behandlede organisatoriske hjælpemidler kan indeholdes i begreberne formål og hjælpemidler. Konvention 108 gennemgik ændringer, som blev vedtaget den 18.05.2018. Disse ændringer er blevet udfærdiget sideløbende med og i kontekst af bl.a. DBF.[62] Begge retssystemer har været yderst omhyggelige med at sikre sammenhæng og kompatibilitet mellem de to lovsystemer.[63] I forbindelse med moderniseringen af Konvention 108 er definitionen dataansvarlig blevet indført som erstatning til filansvarlig.

Definitionen af dataansvarlig i DBF hhv. den moderniserede Konvention 108 er ordlydsmæssigt varierende. Efter DBF er kompetencen til at afgøre formål og hjælpemidler afgørende for dataansvaret, hvorimod den moderniserede Konvention 108 tillægger *beslutningskompetence* den afgørende betydning. I den forklarende rapport til ændringen bliver det nævnt, at der i vurderingen af hvem der er dataansvarlig, særligt må ses på hvem, der bestemmer begrundelsen for behandling eller med andre ord hvem, der træffer afgørelse om behandlingens formål og hjælpemidler. Af væsentlig interesse er imidlertid den følgende passus i den begrundende rapport, som siger at yderligere relevante faktorer for vurderingen af hvem, der har dataansvaret er, om subjektet har kontrol over behandlingsmetoderne, over hvilke personoplysninger der behandles, og hvem der har adgang til personoplysningerne.[64] Ordlyden varierer en smule, men indholdsmæssigt er de tre faktorer identiske med de, der fremgår af det oprindelige forslag til PDD. Med anvendelsen af formuleringen *"yderligere relevante faktorer"* indikeres det, at de øvrige faktorer skal ses som selvstændige momenter, der ligger udenfor begreberne formål og hjælpemidler.

Definitionen i den moderniserede Konventionen 108 kan imidlertid ikke siges at have en så tungtvejende retskildeværdi, at dennes fortolkning skal lægges til grund frem for teori og konsensus vedr. PDD og DBF. Dette begrundes med, at definitionen af den dataansvarlige i den moderniserede Konvention 108 og DBF indholdsmæssigt er ens, såfremt man accepterer forskellen i fortolkningen af kriterierne formål og hjælpemidler. En modsat fortolkning vil medføre, at begreberne ikke kunne anvendes ens, således at et selskab f.eks. kunne være dataansvarlig efter DBF, men ikke den moderniserede Konvention 108. Dette kan ikke være en tilsigtet retstilstand.

Det kan konkluderes, at der i vurderingen af hvor dataansvaret skal placeres, skal foretages en vurdering af, hvem der afgør formålet med behandlingen. I denne sammenhæng skal formålet fortolkes ud fra legaldefinitionen, for at sikre, at et ansvar kan placeres, i situationer, hvor en part behandler personoplysninger ulovligt til eget formål. Begrebet hjælpemidler må omfatte

[61] Handbook on European data protection law s. 108; WP 169, s. 14; Dt's Vejledning om dataansvarlige og databehandlere, s. 9; ICO Data controllers and data processors, s. 7.
[62] Explanatory Report to CETS No. [223], s. 1.
[63] Handbook on European data protection law s. 12 og 26.
[64] Explanatory Report to CETS No. [223], s. 4 f.

både tekniske og organisatoriske hjælpemidler og forstås bredt i overensstemmelse med konsensus herom. Det må yderligere konkluderes, at den moderniserede Konvention 108 har anlagt en anden definition af formål og hjælpemidler end den, der findes i PDD og DBF, på trods af at moderniseringen af Konvention 108 og DBF er gennemført med henblik på at sikre sammenhæng og kompatibilitet mellem hinanden. Dette kan imidlertid ikke tillægges afgørende betydning.

3.2.4. Dataansvarets indtræden

Af ordlyden fremgår det, at den dataansvaret pålægges, er den, der afgør til hvilke formål og med hvilke hjælpemidler, personoplysninger skal behandles. Dataansvaret må således ud fra en ordlydsfortolkning kunne pålægges, når der træffes en afgørelse om formål og hjælpemidler, og altså inden der bliver foretaget en behandling. Artikel 29-gruppen har også indikeret, at udøvelsen af indflydelse på formål og hjælpemidler er tilstrækkeligt til at ifalde dataansvar.[65] I sag C-25/17 Jehovan blev en part pålagt dataansvar, da denne til eget formål udøvede indflydelse på behandlingen af personoplysninger, og derved deltog i fastlæggelsen af formål og hjælpemidler.[66]

Domstolene har imidlertid endnu ikke taget klar stilling til, hvornår dataansvaret specifikt indtræder, og derfor må det være udgangspunktet, at dataansvar ifaldes, når der bliver truffet afgørelse eller udøvet indflydelse.[67] Et væsentligt spørgsmål er, om indflydelse skal udøves aktivt, og i bekræftende fald i hvilket omfang, eller om en part kan forholde sig passivt og derved undgå at ifalde dataansvar. En dom vedr. dette spørgsmål vil forhåbentlig afveje de potentielle spekulationsmuligheder overfor rimeligheden i at pålægge f.eks. en virksomhed dataansvar uden at denne har foretaget en aktiv handling. Dog må det forventes, at omgåelsesbetragtninger ville kunne blive aktuelle og derved sikre effektiv beskyttelse.

3.2.5. Dataansvarets omfang

Det følger af DBF art. 4, nr. 7 ordlyd, at dataansvar lægger ved den, der træffer afgørelse om formål og hjælpemidler for behandling af personoplysninger. Dataansvaret pålægges altså for en behandling. DBF art. 4, nr. 2 definerer behandling 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 dække over en enkelt eller en række af aktiviteter. En aktivitet kan bl.a. være indsamling, ændring, sletning, videregivelse, brug. Om en behandling dækker over en enkelt eller flere aktiviteter, må afhænge af, om der er en sammenhæng mellem de aktiviteter, der udføres.[68] Ved kvalificeringen af dataansvarlig bør man se på, om de enkelte aktiviteter bliver til en række af sammenhængende aktiviteter, når man vurderer dette på et makroniveau.[69] Ved et par eksempler indikerer Artikel 29-gruppen, at man på et mikroniveau kan se enkelte aktiviteter som forfølgende selvstændige formål, men på makroniveau kan de forfølge

[65] WP 169, s. 9.
[66] C-25/17 Jehovan, pr. 68.
[67] Se hertil Motzfeldt, s. 77.
[68] WP 169, s. 20.
[69] Ibid.

det samme formål eller anvende fælles definerede hjælpemidler.[70] Det indikeres herved, at formålet eller hjælpemidlerne eksempelvis kan anvendes som den faktor, der logisk binder aktiviteter sammen, således at disse må ses som en sammenhængende række af aktiviteter.

Anvendelsen af formålet som styrende for, hvornår der er tale om sammenhængende række af aktiviteter, er logisk, henset til at formålet med DBF er at beskytte medlemsstaternes borgere ens og derved ophæve hindringer for det indre marked. Anvendelsen af formålet vil sikre gennemsigtighed, da enhver dataansvarlig er nødt til at kunne definere formål for deres behandlingsaktiviteter, jf. bl.a. oplysningspligten i art. 13 og 14, fortegnelseskravet i art. 30 og kravet om behandlingssikkerhed i art. 32. Da størrelsen er håndterbar, vil anvendelsen af denne være med til at ophæve hindringen for det indre marked, som en vurdering af dataansvar for hver enkelt aktivitet ville medføre. Vurderingen ville med andre ord blive langt mere praktisk, og derved iagttage det effektivitetsformål DBF forfølger. Ligeledes vil medlemsstaternes borgere og nationale tilsynsmyndigheder lettere kunne finde frem til den dataansvarlige, hvilket vil sikre muligheden for effektiv opretholdende af DBF forpligtelser og rettigheder.

Motzfeldt er nået samme konklusion, bl.a. med henvisning til at en berettiget indsigelse fra en registreret som udgangspunkt medfører, at der ikke kan ske fremtidige behandlinger og derved rammer enhver behandling, der forfølger et specifikt formål.[71]

Det konkluderes, at man er dataansvarlig for behandling af personoplysninger på makroniveau. Dette medfører, at man vil være ansvarlig for de behandlingsaktiviteter, der foretages i forfølgelsen af et formål.

3.2.6. Afgrænsningen af dataansvarlig over for databehandler

Indledningsvist er det formålstjenstligt at se på definitionen af, hvad en databehandler er. Databehandler er defineret i DBF art. 4, nr. 8 som:

> *"en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne"*

For at man kan være databehandler, skal man behandle personoplysninger på vegne af en dataansvarlig. En databehandler kan således kun eksistere, såfremt en dataansvarlig har delegeret behandlingsopgaver til denne. De to begreber er tæt knyttede, og der eksisterer et afhængighedsforhold mellem disse. Som gennemgået ovenfor i afsnit 3.1.2 blev det i bl.a. sag C-210/16 Wirtschaftsakademie fastslået, at begrebet dataansvarlig skal fortolkes bredt. Da de to begreber grænser op af hinanden, må dette ske på bekostning af databehandlerbegrebets anvendelsesområde.

Dette giver anledning til en række undersøgelser:

For det første skal det undersøges, om den uddelegerede opgave skal have primær fokus på behandling af personoplysninger, eller om det faktum at personoplysninger indgår i arbejdet i begrænset omfang er tilstrækkeligt til, at man kan anses som databehandler.

For det andet skal det undersøges, om en databehandler i noget som helst omfang kan træffe afgørelse om hhv. formål eller hjælpemidler uden at ifalde dataansvar.

[70] Ibid. eksempel 9 og 10.
[71] Se Motzfeldt, s. 47.

For det tredje skal det undersøges, om lovforpligtelser kan begrænse muligheden for at være databehandler.

For det fjerde skal det undersøges, om den registreredes opfattelse kan påvirke en databehandlerkonstruktion.

For det femte skal det undersøges, om den dataansvarliges tilsyn med databehandlere har betydning for vurderingen.

Endeligt skal det undersøges, hvem der kan være databehandler. Da persongruppen er identisk med dem, der kan ifalde dataansvar, vil dette spørgsmål blive besvaret i afsnit 3.3.

3.2.6.1. Skal databehandlerens opgave primært angå behandling af personoplysninger

Definitionen af databehandler synes ikke at betinge, at behandlingen af personoplysninger skal være en central del af den opgave, der er uddelegeret fra en dataansvarlig.

Motzfeldt har beskrevet, at der har været en linje i Dt's praksis, der har antaget, og en vis konsensus blandt nordiske persondataretsforfattere om, at databehandlerbegrebet ikke bør fortolkes udvidende.[72] Praksis fra Dt vedr. afgrænsningen af begrebet har været domineret af afgørelser, hvor behandlingen af personoplysninger har været i centrum for opgaven, databehandleren skulle varetage. Som eksempler herpå kan nævnes opbygning, drift og vedligehold af journal- eller betalingssystemer,[73] bortskaffelse af computerudstyr med lagrede personoplysninger[74] og administration af en whistleblower-ordning.[75] Dog henleder Motzfeldt opmærksomheden på eksempler i Dt's praksis, hvor den modsatte fortolkning muligvis kan udledes.[76] Et eksempel herpå er en sag, som omhandlede tv-overvågning af hæveautomater.[77] Her blev det selskab, der varetog drift og vedligeholdelse af hæveautomaterne betegnet som databehandler. Drift og vedligeholdelse af automater må generelt antages at omfatte en lang række af opgaver, som ikke omhandler behandling af personoplysninger. Vurderingen af om behandlingen af personoplysninger lægger tilstrækkeligt i centrum af aftalen, må imidlertid bero på de konkrete omstændigheder, som sagen ikke oplyser yderligere om. Dt vurderede dog, at denne opgave i sin helhed kunne rummes inden for databehandlerbegrebet.

Artikel 29-gruppen har indikeret, at opgaver, som ikke har fokus på behandling af personoplysninger, ikke kan lede til en databehandlerkonstruktion. Dette illustreres i et eksempel, hvor en advokat skal repræsentere sin klient i retten.[78] Her fastslås det, at det juridiske grundlag for behandling af de nødvendige informationer er klintens mandat. Dette mandat er imidlertid ikke med fokus på behandling af personoplysninger, men i stedet på repræsentation i retten, hvilket advokater har selvstændig juridisk basis for. Derfor er advokaten selvstændig dataansvarlig.

Dt har i en vejledning om dataansvarlige og databehandlere gjort op med den tidligere debat og den til dels misvisende praksis herom. Det følger af vejledningen, at en aftale skal gå ud på, at en part skal behandle personoplysninger på vegne af en anden. Såfremt den primære ydelse, der skal leveres, ikke omhandler behandling af personoplysninger, så kan der ikke eksistere en

[72] Se Motzfeldt, s. 95 f.f.
[73] "Klage over sikkerheden i praktiserende læges journalsystem" Publiceret 27.10.2003.
[74] Dt's nyhedsbrev af 08.08.2001.
[75] Dt's j.nr. 2006-42-1061.
[76] Motzfeldt s. 98; Forfatteren fremkommer med alternative fortolkninger, som kan være begrundelse for Dt's resultater.
[77] Dt's j.nr. 2007-213-0022.
[78] WP 169, s. 28, eksempel 21.

databehandlerkonstruktion.[79] Et eksempel herpå er en håndværkerydelse. Håndværkerens primære ydelse er at udøve sit håndværk. For at kunne levere denne ydelse, har håndværkeren brug for en adresse, hvor ydelsen skal leveres og et navn på modtageren af fakturaen.

At fortolke begrebet databehandler indskrænket, således at begrebet alene dækker over de tilfælde, hvor behandling af personoplysninger er centrale for den opgave, der varetages på vegne af den dataansvarlige, stemmer godt overens med, at begrebet dataansvarlig skal fortolkes bredt for at forfølge dets formål.

Det kan på baggrund af ovenstående konkluderes, at det er en betingelse for at kunne være databehandler, at den opgave, der uddelegeres af den dataansvarlige, skal vedrøre behandling af personoplysninger med en vis klarhed. Der er endnu ikke praksis, som fastslår den klare grænsedragning, men afgørelsen om overvågning af hæveautomater indikerer, at databehandlerbegrebet dog må anses for at dække relativt bredt. Det kan dog konkluderes, at visse ydelser såsom håndværkerydelser ikke kan give liv til en databehandlerkonstruktion, da behandlingen af personoplysninger er et uvæsentligt element i leveringen af sådanne ydelser.

3.2.6.2. Kan en databehandler træffe afgørelse om formål eller hjælpemidler

For at man kan anses for at være databehandler, skal behandling ske på vegne af den dataansvarlige. For at man kan siges at handle på vegne af nogle, må man have et mandat. Dette sker som den klare hovedregel igennem en instruks fra den dataansvarlige.[80] I tilfælde hvor mandatet ikke er afgrænset tilstrækkeligt, og databehandleren selv træffer afgørelse om formål og hjælpemidler, ifalder databehandleren et selvstændigt dataansvar, jf. DBF art. 28, stk. 10. Men som det blev nævnt i afsnit 3.2.3, eksisterer der en bred konsensus om, at kompetencen til at træffe afgørelse om hjælpemidlerne kan uddelegeres til en databehandler, uden at denne ifalder dataansvar. For at finde frem til grænsen for hvem der er dataansvarlig, må man finde frem til om, og i bekræftende fald hvor meget af, kompetencen til at træffe afgørelse, der kan uddelegeres til en databehandler, uden at denne ifalder dataansvar.

Artikel 29-gruppen foreslår, at man kan opdele hjælpemidlerne i uessentielle og essentielle.[81] For at sondre imellem disse to kategorier må man finde en måde at kvalificere de enkelte hjælpemidler på. Dette kan gøres ved at se på, om afgørelsen har afgørende betydning for lovligheden af behandlingen.[82] I bekræftende fald må der være tale om et essentielt hjælpemiddel. Denne test skal undersøges i det følgende.

Indledningsvist bør det undersøges, om en databehandler kan træffe afgørelse om formålet. De hjælpemidler, der måtte være relevante for en behandling, vil afhænge af hvilket formål, der forfølges. Dette ligger i definitionernes natur, i og med at formålet er det ønskede resultat, og hjælpemidlerne er måden, hvorved dette resultat opnås. Formålet må altså ses som det styrende element for både essentielle og uessentielle hjælpemidler. Anvender man testen på formålet, så følger det af princippet om formålsbegrænsning i DBF art. 5, stk. 1, litra b, at formålet skal være specifikt, udtrykkeligt og legitimt for at være lovligt. Formålet er derfor konsekvent et

[79] Dt's Vejledning om dataansvarlige og databehandlere, s. 7 f.
[80] For at konstruktionen er lovlig, skal der udfærdiges en databehandleraftale. Det medfører, at instruksen skal være skriftlig jf. DBF art. 28, stk. 3.
[81] WP 169, s. 14.
[82] Ibid. s. 15.

essentielt element og afgørelsen af hvilket formål, der skal forfølges, må medføre et dataansvar. Dette er der også konsensus om.[83]

Spørgsmålet er herefter, hvilke hjælpemidler en databehandler kan træffe afgørelse om uden at ifalde dataansvar.

Ifølge Artikel 29-gruppen dækker de uessentielle hjælpemidler over bl.a. software- og hardwarevalg. Disse kan overlades til en databehandler, uden at denne ifalder dataansvar, da et sådant valg ikke har afgørende betydning for behandlingens lovlighed. Overfor disse hjælpemidler står de essentielle. Disse omfatter bl.a. valg af hvilke personoplysninger, der skal behandles, hvordan disse skal behandles, hvem der må have adgang til disse, og hvornår disse skal slettes.

Både ICO og Dt har tilkendegivet, at en databehandler kan træffe afgørelse om sikkerhedsforanstaltningerne ved denne selv, uden at denne ifalder dataansvar.[84] Den dataansvarlige er ansvarlig for, at behandling af personoplysninger sker under anvendelse af passende tekniske eller organisatoriske foranstaltninger, jf. DBF art. 5, stk. 1, litra f, jf. stk. 2. Afgørelsen af tekniske og organisatoriske sikkerhedsforanstaltninger kan derfor ved første øjekast anses for at have afgørende betydning for behandlings lovlighed. Artikel 29-gruppen har da også anført, at der ved implementeringen af PDD var nogle lovsystemer, der tillage sikkerhedsforanstaltningerne afgørende betydning for lovligheden af behandling, fordi disse foranstaltninger skulle defineres af den dataansvarlige.

Ved en nærmere undersøgelse stemmer ICO og Dt's tilkendegivelser dog overens med artikel 29-gruppen sondring mellem essentielle og uessentielle hjælpemidler. Efter PDD art. 17 var det op til medlemsstaterne at fastsætte regler, som sikrede, at dataansvarlige gennemførte sikkerhedsforanstaltninger. Der skulle ligeledes vedtages regler, som fastsatte, at den dataansvarlige kun måtte anvende databehandlere, der gav den fornødne garanti for sikkerhedsforanstaltninger, jf. PDD art. 17, stk. 2. PDD er imidlertid et minimumsdirektiv, hvorfor visse medlemsstater kunne have fastsæt, at den dataansvarlige skulle fastsætte sikkerhedsforanstaltningerne, og ikke alene sikre at databehandlere stillede garanti herfor.

Den dataansvarlige er ansvarlig for, at behandling af personoplysninger sker under anvendelse af passende tekniske eller organisatoriske foranstaltninger, jf. DBF art. 5, stk. 1, litra f, jf. stk. 2. Men den dataansvarlige er ikke forpligtet til at træffe afgørelse om hvilke specifikke sikkerhedsforanstaltninger, der implementeres ved en databehandler. Dette er databehandlere selvstændigt pålagt, jf. DBF art. 32, stk. 1. Den dataansvarlige er alene forpligtet til at sikre, at der stilles garanti for, at der er truffet tilstrækkelige sikkerhedsforanstaltninger jf. DBF art. 28, stk. 1, og stk. 3, litra c. Det er derfor af afgørende betydning for lovligheden af behandling ved en databehandler, at der stilles garanti for, at der er truffet det fornødne niveau af sikkerhedsforanstaltninger. Det er imidlertid ikke af afgørende betydning for lovligheden af behandling ved en databehandler, at den dataansvarlige selv træffer afgørelse om de specifikke sikkerhedsforanstaltninger.

[83] Ibid. s. 14; Dt's vejledning om dataansvarlige og databehandlere, s. 9; ICO Data controllers and data processors, s. 7.
[84] ICO Data controllers and data processors, s. 7; Dt's Vejledning om dataansvarlige og databehandlere, s. 9.

I sag C-210/16 Wirtschaftsakademie lagde EU-domstolen ved placeringen af dataansvar vægt på kompetencen til at afgøre, hvem der skal behandles personoplysninger om, og hvilke personoplysninger der skal behandles om disse.[85] Sagen omhandlede et selskab, som havde en fanside på Facebook. Ved at have en fanside kan enhver finde selskabet på Facebook. Når en person besøger selskabets fanside på Facebook, placerer Facebook cookies på den besøgendes computer, mobil eller andet medium. Disse cookies kan indsamle personoplysninger om den besøgende. Selskaber, der har en fanside, får stillet et værktøj til rådighed igennem Facebook. Værktøjet kan danne statistikker over de besøgende på selskabernes sider, således at selskaber kan finde frem til deres aktuelle målgrupper. Selskaber kan i denne sammenhæng angive hvilke kategorier af personer, der skal indsamles personoplysninger om samt hvilke personoplysninger om disse personer, der skal indsamles.[86] EU-domstolen fandt på baggrund af disse valg, at selskabet bidrog til at afgøre formål og hjælpemidler.[87]

Afgørelsen af hvem der behandles personoplysninger om og hvilke personoplysninger om disse, der behandles, er også af afgørende betydning for lovligheden af behandlingen, jf. DBF art. 5, stk. 1, litra c, hvoraf det bl.a. fremgår, at personoplysninger skal begrænses til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

ICO oplistede en række afgørelser i en vejledning fra 2004, som ville medføre dataansvar, og en række afgørelser som en databehandler kunne træffe.[88] De forskellige afgørelser stemmer overens med det ovenfor gennemgåede og Artikel 29-gruppens test.

Af ICO's liste fremgår det, at dataansvarlige kan træffe afgørelse om:

> formålet med eller formålene som personoplysningerne skal anvendes til,
>
> at indsamle personoplysningerne i første omgang og retsgrundlaget for at gøre det,
>
> hvilke personoplysninger, der skal indsamles, dvs. indholdet af dataene,
>
> hvilke personer, der skal indsamles personoplysninger om,
>
> om oplysningerne skal offentliggøres, og i bekræftende fald for hvem,
>
> om retten til indsigt og andre rettigheder finder anvendelse, dvs. anvendelse af undtagelser[89] og
>
> hvor længe personoplysningerne skal opbevares, eller om der skal foretages ikke-rutinemæssige ændringer af dataene.

Databehandleren kan træffe afgørelse om:

> detaljerne vedr. sikkerheden omkring personoplysningerne,

[85] Sagen vedrører ikke afgrænsningen mellem dataansvarlig og databehandler, men momenterne der tillægges vægt er relevante for kvalificeringen af dataansvar, hvorfor momenterne har samme relevans i en afgrænsning mellem en dataansvarlig og en databehandler.
[86] C-210/16 Wirtschaftsakademie, pr. 36 f.
[87] Ibid, pr. 39.
[88] ICO Data controllers and data processors, s. 6 f.
[89] Dette skal fortolkes således, at afgørelse af om eller hvornår rettighederne finder anvendelse tilkommer den dataansvarlige, men måden hvormed den administrative håndtering sker kan udføres af en databehandler. Se hertil også Den nye persondatarets aktører, s. 63 og 68.

hvilke it-systemer eller metoder, der skal bruges til indsamling af personoplysninger,

de hjælpemidler, der bruges til at indsamle personoplysninger om bestemte personer,

de hjælpemidler, der bruges til at overføre de personoplysninger fra en organisation til en anden,

hvordan man lagrer personoplysningerne,

de hjælpemidler, der bruges til at slette eller bortskaffe dataene og

fremgangsmåden til sikring af at en opbevaringsplan/sletningsrutine overholdes.

Listen er ikke udtømmende, men den taler yderligere for, at Artikel 29-gruppens test er et brugbart værktøj i vurderingen af, hvilke afgørelser en databehandler kan træffe uden at ifalde dataansvar.

Dt har i dets vejledning også udtalt:

> *"Det afgørende, for om der foreligger en instruks, og dermed en databehandlerkonstruktion, er, om en behandling af personoplysninger foretages af en anden part, mens du som dataansvarlig fortsat bestemmer over formålet og over de væsentligste behandlingsskridt, herunder indsamling, sletning, videregivelse og brug af eventuelle underdatabehandlere."*[90]

Det fremgår klart, at Dt har tilsluttet sig synspunktet om, at databehandleren kan træffe afgørelse om uvæsentlige behandlingsskrid, om end mindre detaljeret.

Det må på baggrund af ovenstående fastslås, at Artikel 29-gruppens test, om end ikke direkte nævnt i praksis eller vejledninger, repræsenterer den accepterede sondring mellem hvilke hjælpemidler en databehandler kan træffe afgørelse om uden at ifalde dataansvar og hvilke afgørelser, der medfører et dataansvar. Det kan konkluderes, at afgørelsen af formål og med hvilke essentielle hjælpemidler, der må foretages behandling af personoplysninger med, alene tilkommer den dataansvarlige. Det medfører, at man ifalder dataansvar, såfremt man træffer afgørelse om enten formål eller essentielle hjælpemidler.

3.2.6.3. Gennembrydende formål

Det kan være besværligt at fastlægge hvilket formål, man forfølger med en given behandling, når man varetager en lang række af behandlingsaktiviteter. En situation kan opstå, hvor en databehandler behandler personoplysninger til eget formål. Her vil databehandleren ifalde dataansvar, jf. DBF art. 28, stk. 10. Denne selvstændige behandling kan ske som en ulovlig handling, men den kan ligeså vel ske med henblik på at iagttage lovforpligtelser eller legitime interesser. Sidstnævnte er eksemplificeret af Artikel 29-gruppen og ICO. De fastslår, at en in house revisor, der dog ikke er at anse som en almindelig ansat, kan være dataansvarlig for arbejdet, som udføres under klar instruks.[91] Dette kan ske såfremt revisoren opdager tegn på f.eks. økonomisk kriminalitet, og derefter vil være forpligtet til at rapportere dette, jf. revisorens professionelle forpligtelser.[92]

[90] Dt's Vejledning om dataansvarlige og databehandlere, s. 9.
[91] WP 169, s. 29, eksempel 23; ICO Data controllers and data processors, s. 13.
[92] Se hertil Revisorloven § 22.

En retsførende advokat vil, på samme måde som en revisor, være underlagt en række professionelle forpligtelser i sit hverv. En advokat vil også selv indsamle nødvendige oplysninger for at kunne levere sin ydelse. Med andre ord vil advokater på et niveau selv træffe afgørelse om både formål og essentielle hjælpemidler. ICO anfører derfor, at advokater er selvstændige dataansvarlige i denne sammenhæng. ICO konkluderer herefter:

> *"Hvor specialiserede tjenesteudbydere behandler personoplysninger i overensstemmelse med deres egne professionelle forpligtelser, vil de altid agere som dataansvarlige og kan ikke aftale at overdrage eller dele den dataansvarliges forpligtelser med klienten i denne sammenhæng."*[93]

Kernen i denne vurdering af hvem der skal bære dataansvar ligger i, om det overhovedet er muligt for en advokat eller revisor mv. at følge en klar instruks, eller om disse er bundet af selvstændige forpligtelser.

Ved vurderingen af dataansvar skal man altså have for øje, om en antaget databehandlers eget formål kan gennembryde den dataansvarliges, således at der etableres et selvstændigt dataansvar.

3.2.6.4. Den registreredes opfattelse

Både Artikel 29-gruppen og Dt har anført, at der i vurderingen af om en part er dataansvarlig eller databehandler, vil kunne tillægges den registreredes opfattelse heraf betydning.[94] Da DBF har til formål at beskytte de registrerede, giver det god mening, at disses opfattelse kan tillægges betydning i tilfælde, hvor de har indrettet sig herefter. Dog bør dette moment ikke tillægges afgørende betydning, da resultatet heraf ville være en åbenbar spekulationsmulighed. Ved at vildlede en registreret ville en virksomhed kunne vælge, hvorvidt denne ønskede at agere dataansvarlig eller databehandler. Den faktiske vurdering af hvem, der træffer afgørelse om formål eller essentielle hjælpemidler, må være afgørende. Den registreredes opfattelse heraf, kan dog ud fra en formålsbetragtning tillægges vægt.

3.2.6.5. Tilsyn

Dt har anført, at det er en pligt for den dataansvarlige at føre tilsyn med dennes databehandlere.[95] Om der gennemføres tilsyn, kan imidlertid også få betydning for vurderingen af, om en part er databehandler. Artikel 29-gruppen anfører hertil, at en dataansvarligs konstante og omhyggelige tilsyn med henblik på at sikre databehandlerens grundige overholdelse af instruks og kontraktbetingelser giver en indikation af, at den dataansvarlige fortsat har fuld og selvstændig kontrol over behandlingsaktivisterne.[96] Betragtningen lægger sig op ad den faktuelle vurdering, der foretages af dataansvarets placering. Aktive tilsyn skaber en formodning for kontrol, og indholdet i dokumentationen for tilsyn må ligeledes kunne illustrere, om databehandleren holder sig indenfor instruksen. Manglende tilsyn kan være begrundet i, at man ikke ønsker at anvende ressourcer på tilsyn. Dette kan lede til sanktioner i sig selv, men er ikke af essentiel betydning for vurderingen af, om der er etableret en databehandlerkonstruktion. Såfremt der ikke føres tilsyn, må vurderingen falde tilbage på de øvrige omstændigheder.

---

[93] ICO Data controllers and data processors, s. 13.
[94] WP 169, s. 28; Dt's Vejledning om dataansvarlige og databehandlere, s. 12.
[95] Dt's Vejledende tekst om tilsyn med databehandlere og underdatabehandlere, s. 2.
[96] WP 169, s. 28.

3.2.7. Delkonklusion

Dataansvaret placeres ud fra en vurdering af de faktiske omstændigheder. Vurderingen angår hvem, der har indflydelse på afgørelsen af til hvilke formål eller med hvilke essentielle hjælpemidler, der må foretages behandling af personoplysninger, da en del af afgørelseskompetencen kan udøves af databehandlere, uden at disse ifalder dataansvar. Dataansvaret ifaldes fra det øjeblik, afgørelsen træffes eller indflydelsen herpå udøves, og omfatter behandlingsaktiviteter, der forfølger det samme formål. Databehandlerbegrebet, som begrænser anvendelsesområdet af begrebet dataansvarlig, finder alene anvendelse, når en part varetager en opgave, hvor behandling af personoplysninger på vegne af en dataansvarlig er den primære del af opgaven. Er dette tilfældet, må det undersøges, om databehandleren er overladt et råderum til selvstændige afgørelser. Træffer databehandleren afgørelse om formål eller essentielle hjælpemidler, ifalder denne dataansvar. En sådan afgørelse kan ske ulovligt såvel som på baggrund af en lovforpligtelse, der påhviler databehandleren. Ved at handle på baggrund af en sådan lovforpligtelse vil databehandleren også ifalde dataansvar. Når man ønsker at anvende en databehandler, skal man derfor overveje, om denne kan handle i overensstemmelse med ens instruks. Endeligt må man i vurderingen se på den registreredes opfattelse af, hvorvidt der er tale om en databehandlerkonstruktion eller et samarbejde mellem dataansvarlige.

3.3. Fysisk person, offentlig myndighed, institution og andre organer

Det skal undersøges hvilke subjekter, der kan ifalde dataansvar og agere som databehandler. Definitionerne af de to begreber fastslår, at den dataansvarlige eller databehandleren kan være:

> *"en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ"*

Denne gruppe dækker utrolig bredt, hvilket stemmer godt overens med, at DBF har til formål at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder.

Det er imidlertid ikke helt klart, hvor bredt denne gruppe af potentielle subjekter rækker. I spansk og norsk lovgivning har det ikke været anerkendt, at visse foreningstyper kunne være dataansvarlige.[97] Både den irske nationale tilsynsmyndighed og ICO har anført, den modsatte fortolkning.[98] En forudsætning for at ifalde dataansvar er, at subjektet har partsevne,[99] da det er en forudsætning for at kunne anlægge sag ved domstolene om erstatning efter DBF art. 82, at både sagsøger og sagsøgte har partsevne.[100] I litteraturen er det imidlertid anført, at enhver kan anses som dataansvarlig.[101] Problematikken har endnu ikke givet anledning til et præjudicielt spørgsmål. Henset til at begrebet dataansvarlig skal fortolkes bredt, synes det logisk, at begrebet skal omfatte flest mulige subjekter, så længe dette assisterer til at sikre de registreredes rettigheder.

Der kan dog opstilles visse undtagelser til dette udgangspunkt. I det følgende skal det først undersøges, hvornår DBF finder anvendelse, og herefter hvornår der sker identifikation mellem subjekter.

---

[97] Identity management and data protection law, s. 420, fn. 90. Her anvendes betegnelsen unincorporated associations.
[98] A Guide for Data Controllers; ICO Information Governance in Dental Practices, s. 3.
[99] Motzfeldt, s. 70.
[100] Den civile retspleje, s. 44 f.f.
[101] Den nye persondataret, s. 60.

3.3.1. Anvendelsesområde

3.3.1.1. Behandling under udøvelse af aktiviteter, der falder uden for EU-retten

Det er en forudsætning for at fysiske eller juridiske personer, offentlige myndigheder, institutioner eller andre organer kan være dataansvarlige og databehandlere, at DBF finder anvendelse. Det materielle anvendelsesområde er defineret i DBF art 2. Af bestemmelsens stk. 1 følger det, at:

> *"forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, [102] og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register."*

I DBF art. 2, stk. 2, litra a-d er undtagelserne til anvendelsesområdet oplistet. Ifølge litra a er behandling under udøvelse af aktiviteter, der falder uden for EU-retten undtaget. Efter litra b er behandling, som foretages af medlemsstaterne, når de udfører aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i TEU ikke omfattet. Dette omfatter aktiviteter i forbindelse med Unionens fælles udenrigs- og sikkerhedspolitik. Litra c undtager behandling, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter. Endeligt er behandling, som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed undtaget, jf. litra d. Disse undtagelser er indholdsmæssigt overvejende ens, med dem som findes i PDD art. 3, stk. 2.[103] Ændringen mellem DBF og PDD består i, at det strafferetlige område nu er undtaget fra DBFs anvendelsesområde,[104] og at litra a, b og d nu er opdelt i tre selvstændige punkter, modsat i PDD. I denne afhandling vil litra b og d ikke blive behandlet yderligere grundet opgavens afgrænsning.

Når det materielle anvendelsesområde skal afgrænses i forhold til undtagelsen i litra a, kan der med fordel ses på sagerne C-101/01 Lindqvist samt C-465/00 Österreichischer Rundfunk m.fl. Sagerne blev afgjort på baggrund af PDD. DBF præambelbetragtning nr. 9 fastslår dog, at målsætningerne og principperne i PDD stadig er gyldige. I de efterfølgende præambelbetragtninger beskrives det, at DBF skal fungere som en videreførelse, men præcisering af direktivets regler med henblik på at komme de den manglende harmoniserede af nationale lovgivninger til livs.[105] På denne baggrund vil praksis, som fastslår målsætninger og principper fortsat have præjudikatsværdi for fortolkningen af DBF.[106]

Sag C-465/00 Österreichischer Rundfunk m.fl. omhandlede, hvorvidt der var en pligt for offentlige institutioner, som var underlagt den østrigske rigsrevision, til at meddele og stille oplysninger til rådighed for offentligheden om ansattes indkomster og pensioner med angivelse af de ansattes navne og stillinger. Et tema i sagen var, om man skulle vurdere hver sags tilknytning til EU-retten for at vurdere, om undtagelsen fandt anvendelse. EU-domstolen bemærkede, at PDD blev vedtaget i medfør af Traktaten om Den Europæiske Unions funktionsmådes art.

[102] Begrebet automatisk behandling er sammenfaldende med EDB eller elektronisk behandling jf. bet. 1565/2016, s. 31.
[103] Se også bet. 1565/2016, s. 36.
[104] Området reguleres af retshåndhævelsesdirektivet.
[105] DBF præambelbetragtning nr. 9-13.
[106] Dette synspunkt støttes i bet. 1565/2016, s. 29.

100 A.[107] [108] Artiklen kan anvendes som hjemmel til at vedtage foranstaltninger med henblik på en indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser, der vedrører det indre markeds oprettelse og funktion. Den omstændighed, at traktatens art. 100 A er anvendt som retsgrundlag for en retsakt, forudsætter imidlertid ikke, at der rent faktisk i enhver af de situationer, der er omfattet af den pågældende retsakt, skal foreligge en tilknytning til den frie bevægelighed mellem medlemsstater.[109] Det der er afgørende for, om det er berettiget at anvende traktatens art. 100 A som hjemmel for en retsakt, er om den pågældende retsakt faktisk har til formål at skabe bedre vilkår for det indre markeds oprettelse og funktion.[110] Ved at fortolke undtagelsen i PDD i lyset af dets hjemmelsgrundlag kom EU-domstolen frem til, at anvendelsen af PDD ikke afhænger af, om en konkret situation, har en tilstrækkelig tilknytning til udøvelsen af de grundlæggende friheder - såsom den frie bevægelighed for personer, tjenesteydelser og kapital - der er garanteret i Traktaten om oprettelse af Det Europæiske Fællesskab.[111] EU-domstolen begrundede dette med, at en modsat fortolkning ville kunne medføre, at grænserne for direktivets anvendelsesområde ville blive særdeles usikre og uberegnelige, hvilket ville være uforeneligt med de grundlæggende formål i PDD, der er at foretage en indbyrdes tilnærmelse af medlemsstaternes nationale love og administrative bestemmelser for at fjerne de hindringer for det indre markeds funktion, der netop hidrører fra forskellene i de nationale lovgivninger.[112] EU-domstolen begrundede yderligere sin fortolkning med, at art. 3, stk. 1's ordlyd indeholder en meget bred definition af anvendelsesområdet for PDD, som ikke sigter til at skulle kunne begrænses på baggrund af enhver situations individuelle tilknytning til den frie bevægelighed mellem medlemsstaterne.[113] EU-domstolen støttede denne fortolkning bl.a. på, at undtagelserne i PDD art. 3 stk. 2 ikke ville være affattet således, at de netop tog sigte på specifikke situationer, der falder udenfor den grundlæggende ret til fri bevægelighed.[114] Her kan med fordel nævnes, at PDD ikke finder anvendelse, når behandling foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.

Den yderligere begrundelse blev uddybet i sagen C-101/01 Lindqvist. Her fastslog EU-domstolen med henvisning til sag C-465/00 Österreichischer Rundfunk m.fl., at det ikke ville give mening at undtagelsen i PDD art. 3, stk. 2, som omfatter aktiviteter, der ikke er omfattet af fællesskabsretten, skulle kræve en vurdering af, om en given sags aktivitet er direkte berørt af retten til fri bevægelighed.[115] Med andre ord ville det ikke give mening at indføre undtagelser om sådanne behandlinger, såfremt de i forvejen faldt uden for lovens anvendelsesområde. EU-domstolen kom herefter frem til, at undtagelserne definerer rækkevidden for anvendelsesområdet. Herefter vil kun aktiviteter, som direkte fremgår af oplistningen, eller som kan henføres til samme kategori, være undtaget for lovens anvendelsesområde.

Det er ikke et krav, at der er en direkte forbindelse til EU-retten i en given sag, for at PDD finder anvendelse. Det er kun situationer, som specifikt er oplistet i undtagelsesbestemmel-

[107] Nu findes bestemmelsen som art. 114 i TEUF.
[108] C-465/00 Österreichischer Rundfunk m.fl., pr. 39.
[109] Ibid. pr. 41.
[110] C-465/00 Österreichischer Rundfunk m.fl., pr. 41.
[111] nu i TEUF.
[112] C-465/00 Österreichischer Rundfunk m.fl., pr. 42.
[113] Ibid. pr. 43.
[114] Ibid.
[115] C-101/01 Lindqvist, pr. 42.

serne, der er undtaget fra lovens anvendelsesområde. Undtagelserne skal med andre ord fortolkes indskrænkende. Disse grundlæggende principper i forståelsen af det materielle anvendelsesområde er ligeledes gældende for DBF, da forordningen netop søger at videreføre og præcisere direktivets formål, jf. forordningens præambelbetragtning nr. 9.[116] En anden fortolkning af forordningens materielle anvendelsesområde ville kunne medføre større uklarhed, hvilket ville gå direkte imod formålet med DBF.

3.3.1.2. Behandling af personoplysninger til privat og familiemæssig brug

Undtagelsen af behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter er særligt relevant, i vurderingen af hvem der kan være dataansvarlig eller databehandler. Undtagelsen vedrører alene privatpersoner. Af DBFs præambelbetragtning nr. 18 følger det, at erhvervsmæssige eller kommercielle aktiviteter falder udenfor anvendelsesområdet. Yderligere fremgår det, at:

> *"Personlige eller familiemæssige aktiviteter kan omfatte korrespondance og føring af en adressefortegnelse eller sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter."*

En privatpersons aktiviteter på Facebook vil således kunne være af ren privat karakter. Men hvis aktiviteterne får erhvervsmæssig karakter, vil undtagelsen ikke længere finde anvendelse. Yderligere blev det i sag C-101/01 Lindqvist slået fast, at offentliggørelse af personoplysninger til et ubestemt antal personer falder udenfor undtagelsens anvendelsesområde.[117]

I sag C-25/17 Jehovan, som er behandlet ovenfor i afsnit 3.2.1, uddybede EU-domstolen indholdet af bestemmelsen. EU-domstolen understregede, at undtagelsen skal fortolkes indskrænket, *og derfor omhandler den behandlingen af oplysninger med henblik på udøvelse af »rent« personlige eller familiemæssige aktiviteter*.[118] EU-domstolen fandt, at dør til dør forkyndelse overskred det enkelte trossamfundsmedlems privatsfære.[119] Der blev her særligt lagt vægt på, at formålet med forkyndelsen var at udbrede trossamfundet Jehovas Vidners tro blandt personer, der ikke tilhører de forkyndende medlemmers husstand. Denne aktivitet er således rettet uden for de forkyndende medlemmers privatsfære.[120]

Generaladvokat N. Jääskinen anførte i sit forslag til sag C-131/12 Google Spain, at den brede fortolkning af begreberne personoplysninger, behandling af personoplysninger og dataansvarlig, på grund af den teknologiske udvikling sandsynligvis vil dække en hidtil uset bred vifte af nye faktiske situationer. Dette begrundede Generaladvokaten med, at de fleste websites og filer, som kan tilgås på internettet, indeholder personoplysninger som f.eks. navne på nulevende fysiske personer. Generaladvokaten konkluderede, at:

---

[116] Hertil skal det nævnes, at DBF er vedtaget med hjemmel i TEUF art. 16 og ikke TEUF art. 114 (tidligere art. 100 A). Da fortolkningsprincipperne er knyttet til ordlyden og opbygningen af samt formålet med PDD art. 3, er det ikke af yderligere relevans, at DBF er vedtaget med hjemmel i TEUF art. 16, der blev indført ved Lissabontraktaten.
[117] C-101/01 Lindqvist, pr. 47.
[118] Ibid. pr. 40.
[119] Ibid. pr. 50.
[120] Ibid. pr. 44 jf. pr. 50.

> *"Dette forpligter Domstolen til at anvende et rimelighedsprincip, med andre ord proportionalitetsprincippet, ved fortolkningen af direktivets anvendelsesområde for at undgå urimelige og for omfattende retlige konsekvenser."*[121]

Praksis har imidlertid endnu ikke vist, at dette synspunkt har vundet tilslutning ved domstolene. Retspraksis, som set ovenfor, synes derimod at pege i retning af, at der fortsat foretages en indskrænket fortolkning af undtagelsen.

Der må ved vurderingen af, om undtagelsen finder anvendelse, ses på om personen, der foretager behandling af personoplysninger, udøver behandlingsaktiviteter, som alene forfølger formål af privat eller familiemæssig karakter.

3.3.2. Identifikation

3.3.2.1. Ansatte

For at beskytte borgerne og samtidig sikre effektivitet er det essentielt, at man ved hvilket subjekt, der kan og skal bære dataansvaret i alle situationer. Der er således et behov for forudsigelighed. Artikel 29-gruppen har anført, at det med henblik på at sikre denne forudsigelighed bør foretrækkes, at ansvaret placeres ved en juridisk person eller et organ frem for en fysisk person i disse.[122] Dette synes logisk, da man ofte vil have lettere ved at identificere f.eks. et selskab frem for den enkelte ansatte, der rent faktisk har udført en behandling.

Hvis udgangspunktet er, at juridiske personer skal bære ansvaret frem for de ansatte, kunne man foranlediges til at tro, at de ansatte er databehandlere for disse. Dette er imidlertid ikke en korrekt slutning. Kommissionens skrev i dets andet forslag til PDD, at den dataansvarlige kan lade dennes ansatte eller en ekstern databehandler, som er en separat person, behandle personoplysninger på dennes vegne.[123] Ansatte anses derfor ikke som databehandlere. Ansatte er heller ikke tredjemænd. Tredjemænd er defineret som:

> ***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 dataansvarliges eller databehandlerens direkte myndighed****, der er beføjet til at behandle personoplysninger.*[124]

Det fremgår således, at ansatte bliver identificeret med deres arbejdsgiver. Dette er da også den logiske konklusion på baggrund af ovenstående.

At ansvaret skal placeres ved f.eks. det selskab en ansat arbejder i, er alene et udgangspunkt, da det ikke ville være rimeligt at lade et selskab hæfte for enhver handling, som en ansat kan foretage. En sådan hæftelse ville have karakter af et objektivt ansvar, hvilket enten må have et klart holdepunkt i lov eller indføres igennem retspraksis. Hverken DBF eller retspraksis har indført et sådant ansvar på det persondataretlige område. Spørgsmålet bliver altså, hvornår identifikationen mellem ansat og selskab brydes.

Spørgsmålet her er, hvornår en del af f.eks. et dataansvarligt selskab (den ansatte) handler så selvstændigt og i strid med selskabets instrukser, at denne udskilles til at ifalde et selvstændigt

[121] Forslag til sag C-131/12 Google Spain, pr. 30.
[122] WP 169, s. 15.
[123] COM (92) 422, s. 10.
[124] DBF art. 4, nr. 10.

dataansvar. DBF tager ikke ud over definitionsbestemmelserne stilling til denne ansvarsudskillelsesproblematik. Artikel 29-gruppen har anført, at vurderingen vil være sammenkoblet med den vurdering, der tages i national civil, administrativ eller strafferetlig lovgivning, når ansvar og sanktioner skal fordeles mellem fysiske og juridiske personer.[125] Civilretligt vil arbejdsgiveransvaret som udgangspunkt reguleres efter DL 3-19-2. Bestemmelsen medfører, at en arbejdsgiver hæfter for det erstatningsansvar, som hans arbejdstager måtte pådrage sig for uforsvarlige skadegørende handlinger, der er foretaget i forbindelse med hvervets udførelse.[126] Arbejdsgiveren er imidlertid ikke ansvarlig for abnorme handlinger. Rækkevidden af dette ansvar varierer alt efter, om et krav vedrører erstatning i eller uden for kontraktforhold. I strafferetlig regi er udgangspunktet, at et selskab er ansvarssubjekt frem for de ansatte, men visse handlinger af ansatte medfører, at disse må anses som ansvarssubjekt.[127] Denne fortolkning har Rigsadvokaten også tiltrådt.[128]

Udgangspunktet er, at der sker identifikation mellem arbejdstager og arbejdsgiver. Eftersom DBF ikke tager stilling til spørgsmålet om ansvarsfordeling mellem selskaber og ansatte, må det være naturligt, at man ved vurderingen af grænsen for identifikationen følger national lovgivning vedr. erstatning og sanktionering, som Artikel 29-gruppen har foreslået.

3.3.2.2. Koncerner

Det følger af DBF art. 4, nr. 10, at tredjemænd ikke omfatter bl.a. juridiske personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle personoplysninger. I forarbejderne til PDD gives der eksempler på, hvem der kan, og ikke kan, anses for at være under den dataansvarliges direkte myndighed. Heraf fremgår det, at ansatte i andre organisationer, selv hvis de tilhører den samme koncern eller det samme holdingselskab som udgangspunkt vil være tredjemænd.[129] Da de ansatte bliver identificeret med deres arbejdsgivende selskab, må selskaberne imellem som udgangspunkt anses som tredjemænd og derfor selvstændige dataansvarssubjekter.

Den Irske Data Protection Commission har også tilsluttet sig dette synspunkt, idet de har anført, at *det skal understreges, at hvert selskab, om det er moderselsksab eller underordnet, er en selvstændig juridisk person med dets egne sæt af lov- og databeskyttelsesforpligtelser.*[130]

Både forarbejderne til PDD og den Irske Data Protection Commission pointerer, at dette kun er et udgangspunkt. Undtagelse er ifølge den Irske Data Protection Commission de sjældne tilfælde, hvor to eller flere selskaber rent faktisk kan udøve lovhjemlet eller de facto kontrol og ansvar for et givent sæt af personoplysninger. I sådanne tilfælde vil selskaberne kunne anses som fælles dataansvarlige.

---

[125] WP 169, s. 16.
[126] Erstatningsret, s.147 f.f.
[127] Ansvaret, s. 249-250, hvor der yderligere sondre mellem selskabets ledelse og underordnede ansatte. Sidstnævnte skal i almindelighed ikke drages til ansvar, selvom de har handlet forsætligt eller groft uagtsomt. Personlig tiltale mod en underordnet ansat kan dog komme på tale f.eks., hvor en ansat har kørt spirituskørsel i forbindelse med dennes arbejde.
[128] Rigsadvokatmeddelelsen om strafansvar for juridiske personer, pkt. 3.1.3. jf. Rigsadvokatmeddelelsen, Sager om overtrædelse af databeskyttelsesreglerne pkt. 4.5.
[129] COM (92) 422, s. 11.
[130] Are you a "data controller"?.

En anden undtagelse er dog blevet foreslået.[131] DBF præambelbetragtning nr. 150 anfører, at begrebet "virksomhed" skal fortolkes i overensstemmelse med TEUF art. 101 og 102 ved udstedelsen af administrative sanktioner. I retspraksis vedr. disse bestemmelser er begrebet blevet fortolket således, at et moder- og datterselskab kan betragtes som en "virksomhed", såfremt datterselskabet ikke frit bestemmer sin adfærd på markedet, men i stedet følger instruktioner fra moderselskabet.[132] Denne fortolkning kunne medføre, at et moderselskab kan pålægges sanktioner, selvom det ikke kan konstateres, at dette er dataansvarlig. Ordlyden af DBF art. 83, stk. 3 anfører imidlertid, at bøder skal påføres dataansvarlige eller databehandlere, hvorfor betragtningerne kan være tiltænkt situationer, hvor moder- og datterselskaber er fælles dataansvarlige.[133]

Det kan konkluderes, at der som det klare udgangspunkt ikke sker identifikation mellem moder- og datterselskaber. I stedet kan fælles dataansvar komme på tale. Det er endnu ikke afklaret, om der kan ske identifikation mellem selskaber i en koncern, ved udstedelse af administrative sanktioner.

3.4. Alene eller sammen med andre

Den sidste del, der skal behandles i definitionen af dataansvarlig er "alene eller sammen med andre". Dette blev indført i PDD på baggrund af et ændringsforslag fra Kommissionen og tilsigter at lade dataansvaret blive båret af flere parter.[134] Leddet er direkte videreført til DBF, dog således at det er blevet suppleret af en yderligere bestemmelse, som findes i DBF art. 26. Det følger af bestemmelsens stk. 1, 1. pkt., at:

> *"Hvis to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling, er de fælles dataansvarlige."*

Det er iøjnefaldende, at art. 26 anvender begreberne "i fællesskab" og "fastlægger", mens art. 4, nr. 7 anvender "sammen" og "afgør". Den engelske sprogversion af bestemmelserne anvender imidlertid begreberne "jointly" og "determines" konsekvent. Den franske sprogversion anvender "conjointement" samt "détermine" og "déterminent" som alene er grammatiske bøjninger af hinanden. Det kan derfor ikke antages, at anvendelsen af andre begreber i art. 26 ændrer på vurderingen af det fælles dataansvar.

Det kan af bestemmelsen udledes, at det fælles dataansvar pålægges ud fra samme kriterier som et individuelt, nemlig ved at vurdere hvem der afgør formål og hjælpemidler. Der er altså ikke tale om en udvidelse eller ændring af definitionen i DBF art. 4, nr. 7, og art. 26 tilføjer intet nyt til afgrænsningen af fælles dataansvar. Art. 26 har derimod til formål at sikre gennemsigtighed for registrerede og iagttagelse af disses rettigheder ved at stille krav om, at de fælles dataansvarlige fastsætter en ordning, der sikrer dette. Dataansvaret placeres ud fra de normale kriterier.[135] Om ansvaret er fælles vurderes på baggrund af, om formål og essentielle hjælpemidler er afgjort i fællesskab.

Dt har imidlertid indfortolket en yderligere betingelse, hvorefter alle parter skal have ret til at bruge oplysningerne til egne formål.[136] Det uddybes ikke yderligere hvad der menes hermed.

---

[131] Dataansvarlig eller databehandler, s. 24 f.f.
[132] C-508/11 P – Eni, pr. 46.
[133] Dataansvarlig eller databehandler, s. 26
[134] COM (95) 375 final, s. 3.
[135] Dette synspunkt støttes også i WP 169, s. 18.
[136] Dt's Vejledning om dataansvarlige og databehandlere, s. 15.

At have ret til at bruge personoplysningerne kan forstås som en henvisning til kravet om behandlingsgrundlag i DBF art. 6 og 9, stk. 2 samt DBL afsnit II. Denne fortolkning harmonerer imidlertid ikke med, at Dt efterfølgende fastslår, at man som fælles dataansvarlige er fælles ansvarlige for at overholde reglerne i DBF. En mere korrekt fortolkning ville være, at kravet om at man "i fællesskab skal fastlægge formålene med og hjælpemidlerne til behandling" medfører, at man de facto må have kompetence til at afgøre formålet eller essentielle hjælpemidlerne som gennemgået ovenfor under afsnit 3.2.1 og 3.2.2. Med andre ord udelukkes fælles dataansvar i tilfælde, hvor en part foretager behandling til sine egne formål, og andre parter ikke kan afgøre formål eller essentielle hjælpemidler sammen med denne. I situationer hvor kun en part kan afgøre formål og essentielle hjælpemidler, vil der pr definitionen ikke kunne være tale om fælles dataansvar. Dt nævner dog ikke de essentielle hjælpemidler i deres kriterie. Dette kan være et udslag af vejledningens pædagogiske opbygning. Vejledningen foretager ikke sondringen mellem essentielle og uessentielle hjælpemidler, men anerkender alene, at visse kompetencer skal forblive ved den dataansvarlige herunder kompetencen til at afgøre væsentlige behandlingsskridt. Det må altså lægges til grund, at Dt's betingelse er indeholdt i den normale vurdering af dataansvar.

Samarbejder mellem dataansvarlige kan fremkomme på et utal af måder, og det må stå klart, at ethvert samarbejde mellem dataansvarlige ikke medfører, at de er fælles dataansvarlige. Det fælles dataansvar kan, henset til de mange mulige samarbejdskonstruktioner, dække både delvist såvel som komplet og må vurderes på baggrund af de relevante omstændigheder.[137]

De forskellige grader af samarbejde kan opdeles i fire grupper.[138]

Den første gruppe er hvor den selvstændig dataansvarlige optræder alene. Dette kan være tilfældet, hvor en virksomhed ønsker at sende markedsføringsmateriale ud til dets kunder, og derfor behandler kundernes personoplysninger til dette formål.

Den anden gruppe omfatter tilfælde, hvor flere selvstændig dataansvarlige samarbejder uden, at de i fællesskab træffer afgørelse om formål eller essentielle hjælpemidler. Dette kunne eksempelvis være en virksomhed, der overlader personoplysninger til SKAT, for at SKAT kan behandle disse til egne formål på den måde, SKAT finder egnet.

Den tredje gruppe omfatter tilfælde, hvor flere dataansvarlige træffer afgørelse om formålet og hjælpemidlerne vedr. behandlingsaktiviteter i fællesskab, mens andre behandlingsaktiviteter udføres separat af de enkelte dataansvarlige. Et eksempel herpå er Facebook og administratorerne af fansider på platformen som gennemgået ovenfor i afsnit 3.2.1. Administratoren træffer afgørelse om hvilke kategorier af personoplysninger, der skal indsamles, og hvilke registrerede der skal indsamles personoplysninger om. Facebook anvender imidlertid personoplysningerne til egne yderligere formål.

Den fjerde gruppe omfatter tilfælde, hvor flere dataansvarlige i fællesskab afgør samtlige behandlingers formål og hjælpemidler. Et eksempel herpå kunne tænkes at være, hvor to selskaber går sammen om et forskningsprojekt og tilrettelægger hele projektet i fællesskab.

[137] WP 169, s. 19; C-210/16 Wirtschaftsakademie pr. 43.
[138] Identity management and data protection law, s. 419.

3.4.1. Behandling af de samme personoplysninger

Selvom både PDD og DBF anerkender, at formål og hjælpemidler kan bestemmes af mere end en part, formulerer de ikke nogen kriterier, som kan anvendes til at afgøre, hvornår parter kan anses for at træffe afgørelse om formål og hjælpemidler i fællesskab.

I den engelske Data Protection Act 1998 var en dataansvarlig defineret som en person der *"enten alene eller sammen eller til fælles med andre personer"*[139] afgør formål og hjælpemidler. At træffe afgørelse om formål og hjælpemidler til fælles dækker ifølge ICO tilfælde, hvor flere parter deler en samling af personoplysninger, som de behandler uafhængigt af hinanden til individuelle formål.[140] Denne definition af dataansvarlig dækker over en konstruktion af selvstændige dataansvarlige.[141] Definitionen viser dog, at den fælles afgørelse er essentiel i vurderingen af, hvornår dataansvarlige sammen træffer afgørelse. Fælles dataansvar dækker altså ikke situationen, hvor parter alene anvender de samme personoplysninger. Det er en betingelse, at afgørelsen om formål eller essentielle hjælpemidler bliver truffet i fællesskab.

Et eksempel herpå findes i Artikel 29-gruppens udtalelse om SWIFT (The Society for Worldwide Interbank Financial Telecommunication).

SWIFT er udbyder af finansielle kommunikationsservices, som faciliterer internationale pengeoverførsler.[142] Alt efter hvilken kommunikation der udføres, vil en sådan indeholde personoplysninger såsom navne på både modtagere og kunder, der ønsker en transaktion gennemført, referencenumre mv.[143] SWIFT havde ikke adgang til at læse indholdet, men opbevarede transaktionsoplysningerne i 124 dage ved to driftscentre i hhv. EU og USA, for at sikre imod datatab og sikre informationer i tilfælde af tvister. Efter terrorangrebet 09.11.2001 udstedte US Department of Treasury løbende en række påkrav, såkaldte subpoenas, om at SWIFT skulle give adgang til opbevarede transaktionsoplysninger. SWIFT efterkom anmodningerne, dog med enkelte begrænsninger efter forhandlinger herom var gennemført.

Artikel 29-gruppen fastslog, at SWIFT handlede som dataansvarlig både for den normale behandling af personoplysninger såvel som for overførslen til US Department of Treasury.[144] Begrundelsen for dataansvaret placering var:

> at SWIFT ikke alene handlede på dets kunders vegne, men i stedet havde påtaget sig forpligtelser, som pr deres natur og omfang, gik videre end de normale instruktioner og forpligtelser der påhviler en databehandler,
>
> at administrationen af SWIFT skete igennem et formelt samarbejdsnetværk, som afgjorde formålet med og hjælpemidlerne til SWIFTs kommunikationsservice,
>
> at samarbejdsnetværket afgjorde, hvilke personoplysninger der skulle behandles via servicen, og hvilke informationer der skulle videregives til finansielle institutter,

[139] DPA 1998, del 1, § 1.
[140] ICO Key definitions (arkiveret).
[141] Joint Data Controllers under the GDPR, s. 2.
[142] WP 128, s. 2.
[143] Ibid. s. 8.
[144] Ibid. s. 11.

at samarbejdsnetværket afgjorde formål og hjælpemidler ved at udvikle, markedsføre og ændre eksisterende og nye ydelser. Dette skete bl.a. ved at ændre i eksisterende ydelsers behandlingsmåder uden at dette krævede samtykke fra kunderne,

at SWIFT tilbød added value ydelser til behandlingen, f.eks. sikker opbevaring og validering af personoplysninger,

at samarbejdsnetværket havde ret til at træffe kritiske afgørelser vedr. behandlingen, såsom den sikkerhedsstandard der skulle etableres og hvor behandling måtte foretages,

at samarbejdsnetværket forhandlede og opsagde serviceaftaler med fuld autonomi og ændrede i forskellige kontraktdokumenter og politikker.

Det manøvrerum vedr. valg af praktiske og lovlige (uessentielle og essentielle) hjælpemidler som SWIFT var overladt medførte, at SWIFT ikke længere kunne anses for at være databehandler.

Artikel 29-gruppen fastslog også, at de finansielle institutter var dataansvarlige for behandlingen foretaget i SWIFT herunder overførslen til US Department of Treasury - dog i en mindre grad. Dette blev begrundet med, at de finansielle institutter selvstændigt traf afgørelser, og ikke var bundet af deres kunders instrukser.[145] De finansielle institutter var f.eks. ikke pålagt at anvende SWIFT, men kunne frit vælge andre services eller serviceudbydere og derved selv træffe afgørelse om sikkerhedsniveauet. De finansielle institutter handlede som selvstændige dataansvarlige overfor deres kunder, da de traf afgørelser, der alene tilkommer dataansvarlige, og havde en de facto kompetence hertil. Det fælles dataansvar synes at være pålagt på baggrund af, at det var forudsat, at de finansielle institutter have en bestemmende indflydelse i SWIFT, potentielt havde kendskab til SWIFTs efterkommen af subpoenas og en undersøgelsespligt i forhold hertil. Indflydelsen stammede fra at visse finansielle institutter, der anvendte SWIFT, var repræsenteret i bestyrelsen, og at administrationsstrukturen i SWIFT oprindeligt var organiseret på en sådan måde, at den skulle sikre, at banker og andre finansielle institutter bevarede beslutningskompetence i forbindelse med SWIFTs beslutningsproces. Det faktum at SWIFT med tiden var blevet mere uafhængig, betød ikke, at de finansielle institutter ikke fortsat handlede som dataansvarlige for behandlingerne fortaget af SWIFT.

Begrundelsen for det fælles dataansvar for hhv. de generelle behandlinger foretaget af SWIFT og specifikt vedr. overførslen til US Department of Treasury blev behandlet som et. Det kan dog udledes, at Artikel 29-gruppen tillægger det betydning, at de finansielle institutter havde eller burde have haft kendskab til overførslerne på baggrund af subpoenasene. Viden om en behandling synes at være en logisk forudsætning for det fælles dataansvar, da man ikke kan afgøre formål eller essentielle hjælpemidler i fællesskab, såfremt man ikke har viden om disse. At burde viden er tilstrækkeligt, sikrer at en dataansvarlig ikke kan påberåbe sig ikke at have læst en aftale eller lignende. Dette må tolkes som en omgåelsesbetragtning som nævnt i afsnit 3.2.4. Herudover satte Artikel 29-gruppen ikke høje krav til betingelsen om fællesskab i afgørelsen om formål og essentielle hjælpemidler. I SWIFT havde de finansielle institutter kompetence til at afgøre formål og essentielle hjælpemidler, da nogle af disse var repræsenteret i bestyrelsen, og da de finansielle institutter havde indflydelse igennem administrationsstrukturen. Udtalelsen uddyber desværre ikke hvilken indflydelse administrationsstrukturen gav de

[145] WP 128, s. 12 f.

finansielle institutter, og der kan derfor ikke klart siges, om en indirekte afgørelse af formål og essentielle hjælpemidler er tilstrækkeligt til at etablere et fælles dataansvar. Indflydelsen var imidlertid faldet som følge af SWIFTs stigende selvstændighed. Der kan på denne baggrund være en formodning for, at en indirekte indflydelse på en afgørelse er tilstrækkeligt til at statuere fællesskab. Det må dog overvejes om samtlige finansielle institutter udøvede indflydelse på formål eller essentielle hjælpemidler. Dette er tvivlsomt. Artikel 29-gruppen fremstår herved villige til at strække begrebet "fælles dataansvar" meget langt. Dette kan være begrundet i, at SWIFT ikke kunne opfylde forpligtelserne som dataansvarlig selvstændigt, idet de bl.a. ikke havde kendskab til de finansielle institutioners kunder eller meddelelsernes indhold. Denne vide fortolkning er dog ikke nødvendigvis usaglig. I afsnit 3.1.2. blev det nævnt, at DBFs formål opnås ved at pålægge pligtsubjekterne forpligtelser. Som nævnt i afsnit 1.1. er det væsentligt forskellige forpligtelser, der påhviler dataansvarlige hhv. databehandlere. Sondringen mellem de to definitioner er derfor vigtig, for at beskytte de registreredes rettigheder effektivt. Effektiv beskyttelse opnås i praksis igennem forudsigelighed, da dette tillader subjekter at indrette sig efter definitionerne og deres respektive forpligtelser. Behovene for beskyttelse og forudsigelighed er dog ikke de samme i vurderingen af fælles dataansvar. De dataansvarliges forpligtelser overfor de registrerede ændrer sig ikke væsentligt ved, at de er fælles dataansvarlige. De skal alene fordele forpligtelserne mellem sig og oplyse herom. Det er derfor ikke utænkeligt, at EU-domstolen også vil foretage en mere formåls- og kontekstbaseret fortolkning ved placeringen af fælles dataansvar end ved vurderingen af, om en part er databehandler. EU-domstolen må dog være varsom med, hvilke situationer de placerer under begreberne, såfremt en vis forudsigelighed skal opretholdes.

3.4.2. Behandling via samme it-systemer

I sager om såkaldte e-government portaler og andre it-systemer fremgår det, at det ikke er tilstrækkeligt til at statuere fælles dataansvar, at man anvender og driver et fælles it-system til behandling af personoplysninger.

I sagerne er formålene for systembrugerne f.eks. at udføre en opgave, som er pålagt ved lov. Anvendelsen af hjælpemidlet kan ligeledes være pålagt ved lov. En part, der træffer afgørelse om at leve op til sine forpligtelser i medfør af loven, afgør derved formål og hjælpemidler. Hver part, der er underlagt denne forpligtelse, er derfor selvstændig dataansvarlig, da de ikke har nogen indflydelse på hinandens afgørelse af formål eller hjælpemidler. Den part, som administrerer et system kan imidlertid være dataansvarlig eller databehandler. Viser det sig, at administratoren er dataansvarlig, opstår spørgsmålet, om denne er fælles dataansvarlig med nogle af brugerne. Ser man på kompetencekilderne i afsnit 3.2.2 virker det oplagt, at et selskab eller en myndighed mv., der har kompetence til at oprette og nedsætte bindende retningslinjer for anvendelsen af et system, kan anses som fælles dataansvarlig med de enkelte brugere.

Et eksempel herpå er the internal market information system (IMI). IMI-systemet fungerer som et redskab, medlemsstaterne imellem kan anvende til at udveksle informationer. En myndighed kan f.eks. få bekræftet, at et diplom mv. er ægte af en udenlandsk myndighed, der har udstedt diplomet, f.eks. i tilfældet hvor en læge flytter til en anden stat, og ønsker at praktisere der.

Artikel 29-gruppen anså her Kommissionen som fælles dataansvarlig med brugerne af systemet, da Kommissionen sammen med brugerne traf afgørelse, om hvor længe personoplysningerne skulle opbevares.[146] [147] Kommissionen bestemte mere præcist at:

> *"Alle personoplysninger vedrørende de registrerede i forbindelse med informationsudvekslinger, som finder sted mellem de kompetente myndigheder og underkastes behandling i IMI, slettes seks måneder efter, at informationsudvekslingen formelt er afsluttet, medmindre en kompetent myndighed udtrykkeligt anmoder Kommissionen om slettelse inden udløbet af denne periode."*[148]

Kommissionen træffer således afgørelse om, at sletning sker efter 6 måneder, men brugerne har adgang til at påvirke afgørelsen.[149] Begge parter har altså kompetence til at træffe afgørelse om det samme essentielle hjælpemiddel.

Som kontrast kan man se på Dt's afgørelse vedr. Beskæftigelsesministeriets Elektronisk Sags- og Dokumenthåndtering-system (ESDH).[150] Systemet havde flere funktioner herunder en til håndteringen af borgerbreve, § 20-spørgsmål og spørgsmål fra folketingsudvalg. Den myndighed, der modtog et sådant brev eller spørgsmål, skulle oprette en sag og administrere hvem, der havde adgang til sagen. I forbindelse med denne funktion blev hver myndighed anset som selvstændig dataansvarlig for de personoplysninger, de behandlede i sagerne. Valgte en myndighed i denne sammenhæng at videregive personoplysningerne til anden relevant myndighed, uanset dette er på baggrund af en pligt,[151] ville dette være et udslag af dets egen kompetence til at afgøre formål og hjælpemidler. Anvendelsen af ESDH-systemet medførte således ikke i sig selv fælles dataansvar, da myndighederne ikke havde kompetence til sammen at afgøre formål eller essentielle hjælpemidler.

At en dataansvarlig vælger et system eller en ydelse medfører altså ikke i sig selv fælles dataansvar mellem bruger og administrator. Heller ikke såfremt administratoren træffer afgørelse om at behandle personoplysningerne til egne formål, da en sådan afgørelse ikke ville være fælles.

3.4.3. Serviceudbyders fastsættelse af vilkår

SWIFT og IMI-systemet illustrerer tilfælde, hvor bruger og administrator træffer afgørelse i fællesskab. Det behandlede af afgørelsen om ESDH-systemet illustrerer tilfælde, hvor administratoren ikke træffer afgørelse. En situation, der mangler at blive undersøgt, er, om en bruger, der ikke efterlades et forhandlingsrum vedr. f.eks. essentielle hjælpemidler, kan siges at træffe afgørelse i fællesskab.

I visse tilfælde er det ikke den dataansvarlige køber af en ydelse, der dikterer betingelser og vilkår for en serviceudbyder. Teknologisk specialisering har medført, at flere serviceudbydere udfærdiger standardkontrakter, der udbydes som "take it or leave it" tilbud. Her ville man kunne foranlediges til at tro, at serviceudbyderen havde afgjort formål og/eller de essentielle hjælpemidler. Denne konklusion er imidlertid ikke korrekt. Artikel 29-gruppen har anført, at

[146] WP 140, s. 4 f.
[147] IMI er nu reguleret af IMI-forordningen.
[148] 2008/49/EF, art. 4.
[149] Kommissionen traf yderligere afgørelse om andre essentielle hjælpemidler og formål. Dette blev ikke tillagt fokus af Artikel 29-gruppen.
[150] Dt's j.nr. 2007-321-0027.
[151] Et eksempel er Forvaltningslovens § 7 om pligten til vejledning og videresendelse.

en dataansvarlig har mulighed for at sætte sig ind i tilbuddet.[152] Den dataansvarlige træffer herefter afgørelsen om, hvorvidt behandlingen skal ske i overensstemmelse med serviceudbyderens standardkontrakt. Den dataansvarlige påtager sig således det fulde ansvar for kontraktens indhold. Derved får det faktum, at kontrakten er udfærdiget af databehandleren ikke betydning for dataansvarets placering, da de essentielle aspekter af behandlingen fortsat afgøres af den dataansvarlige. Den dataansvarliges valg om at anvende en serviceudbyder er et valg, som falder indenfor den dataansvarliges kompetence til at afgøre. Er kontrakten en instruks, som fastsætter formål og essentielle hjælpemidler, kan serviceudbyderen være databehandler. Er kontrakten ikke specificeret i en sådan grad, medfører dette ikke automatisk fælles dataansvar. Alene såfremt der er et faktisk element af fællesskab i afgørelsen af formål eller essentielle hjælpemidler, er fælles dataansvar relevant.

Denne forståelse tillader også en part at komme med forslag til løsninger af problemer og valg af essentielle hjælpemidler. Har parten imidlertid indflydelse på afgørelsen, følger det dog af definitionen af den dataansvarlige, at denne ifalder dataansvar. Når to parter finder en løsning, er grænsen mellem et forslag til løsning og indflydelse på f.eks. essentielle hjælpemidler ikke nem at navigere, særligt ikke når vurdering foretages ud fra de faktiske omstændigheder. Dog må vurderingen mellem databehandler og dataansvarlig følge det i afsnit 3.2-3.3 gennemgåede. Viser det sig, at der faktisk er udøvet indflydelse på formål eller essentielle hjælpemidler, må det vurderes, om dataansvaret er fælles. Dette vil oftest være tilfældet, da parternes indflydelse på afgørelsen bliver udøvet igennem forhandling og derved i fællesskab.

3.4.4. Delkonklusion

Det konkluderes, at fælles dataansvar indtræder, når to eller flere dataansvarlige de facto træffer afgørelse om formål eller essentielle hjælpemidler i fællesskab. Det er ikke tilstrækkeligt, at parterne anvender de samme it-systemer eller personoplysninger. Der skal være et yderligere element af fællesskab forbundet med afgørelsen. Dette kan opstå i et utal af situationer f.eks. igennem fælles forhandlinger, anvendelse af fælles beføjelser, men også igennem en formentlig meget indirekte indflydelse som anført af Artikel 29-gruppen i SWIFT-udtalelsen. Mulighederne er kun begrænset af de samarbejdsstrukturer, ansvarssubjekter kan indgå i. Muligheden for at anvende begreberne på mange forskellige situationer er en naturlig selvfølge af, at begreberne er generelt formuleret.[153]

4. Konklusion

Denne afhandling har til formål at klarlægge, hvor dataansvaret skal placeres, og hvordan dette gøres.

Første spørgsmål i vurderingen af hvor dataansvar skal placeres er, om DBF finder anvendelse for den behandling, dataansvaret vurderes på baggrund af. Dernæst er spørgsmålet, om det subjekt, som vurderingen foretages af, har partsevne. Er dette tilfældet, skal det undersøges, om der sker identifikation mellem denne og et andet subjekt.

Indgår parten et samarbejde med andre, må det vurderes, om dette udgør enten en databehandlerkonstruktion eller et samarbejde mellem dataansvarlige. Denne vurdering skal foretages på baggrund af de faktiske omstændigheder. En kontrakt eller serviceaftale kan dog udgøre et udgangspunkt i vurderingen, hvorfor en sådan bør formuleres klart og specifikt. Dette sikrer

[152] WP 169, s. 26.
[153] C-101/01 Lindqvist, pr. 83.

også, at de involverede parter er oplyst om deres respektive forpligtelser. Det afgørende for dataansvarets placering er, om et subjekt afgør hvilke formål, der skal forfølges med en behandling eller hvilke essentielle hjælpemidler, der skal anvendes med henblik herpå. Problematikken, der er forbundet med at anvende en faktisk vurdering, er, at den i praksis er besværlig at anvende. SWIFT er et fremragende eksempel herpå. Det er derfor en god ide for enhver, der har intentioner om at behandle personoplysninger, at have rollefordeling med i sine betragtninger f.eks. i forbindelse med strukturering af samarbejder eller virksomheder i koncerner. I den sammenhæng er det væsentligt at holde for øje, at dataansvaret omfatter behandlingsaktiviteter, der følger samme formål, hvorfor man kan være dataansvarlig for visse behandlinger og databehandler for andre.

Databehandlerkonstruktionen kan kun eksistere, såfremt en part har fået til primær opgave at behandle personoplysninger på vegne af en dataansvarlig. Herudover er det en betingelse, at databehandleren ikke træffer afgørelse om formål eller essentielle hjælpemidler. I denne sammenhæng er definitionen af den dataansvarlige misvisende, idet den anvender begreberne formål *og* hjælpemidler. En databehandlers afgørelse af hvilke uessentielle hjælpemidler der skal anvendes, medfører ikke, at en databehandler ifalder dataansvar. Hvordan samarbejdet fremstår udadtil, kan få betydning i vurderingen, da formålet med DBF er at sikre de registreredes rettigheder. Yderligere er det ikke en betingelse, at den dataansvarlige selv udfærdiger instruksen, som databehandleren skal handle efter. Dette medfører, at parterne i en vis grad kan vælge hvilken konstruktion, de ønsker at anvende. Vurderingen af hvor dataansvaret skal placeres, skal dog foretages løbende på grundlag af hver behandling og ikke alene ved en aftales indgåelse.

Er der et samarbejde mellem to eller flere dataansvarlige, må der foretages en vurdering af, om de har truffet afgørelse i fællesskab, eller om de alene deler personoplysninger eller it-systemer. Det kan ud fra SWIFT-udtalelsen ikke antages, at artikel 29 gruppen vil stille høje krav, til hvordan indflydelsen på en afgørelse af formål eller essentielle hjælpemidler skal udøves, for at den kan anses som værende sket i fællesskab. I mangel på andre begreber end dataansvarlig, fælles dataansvar og databehandler virker denne afgørelse praktisk, men ikke formålstjenstlig for forudsigeligheden af begreberne. En klarlæggelse af om forudsigelighed eller fleksibilitet er mest ønskværdigt i vurderingen mellem selvstændigt eller fælles dataansvar mangler dog. Ligeledes vil en afgørelse, som tager klar stilling til, hvornår dataansvaret indtræder, eller mere specifikt hvornår indflydelse på en afgørelse kan anses for udøvet i en sådan grad, at man ifalder dataansvar, være af væsentlig betydning for klarlæggelsen af definitionerne. Det er muligt, at en sådan klarlægning kommer indenfor den nærmeste fremtid. Sag C-40/17 Fashion ID er endnu ikke afgjort, men et præjudicielt spørgsmål i sagen går på, om en hjemmesideadministrator er dataansvarlig for de personoplysninger, der sendes til Facebook, når en brugers browser loader en hjemmeside, hvor der er en Facebook ”like” knap, i de tilfælde hvor hjemmesideadministratoren ikke kan udøve indflydelse på behandlingsaktiviteterne. Sagens nærmere omstændigheder bliver essentielle for, om der bliver givet en afklaring, men spørgsmålets formulering er af væsentlig interesse i nærværende sammenhæng.

5. Litteraturliste

Bøger:

Ansvaret; Strafferet- Ansvaret af Gorm Toftegaard Nielsen, Jurist- og Økonomforbundet, 2013,4. udgave, 1. oplag, 978-87-574-2947-3.

Den civile retspleje; Den civile retspleje af Ulrik Rammeskow Bang-Pedersen, Lasse Højlund Christensen og Clement Salung Petersen, Hans Reitzels, 2015, 3. udgave.

Den nye persondataret; Den nye persondataret : forordning 2016/679 om persondatabeskyttelse : med en omtale af direktiv 2016/680 (politipersondataret) af Peter Blume, Jurist- og Økonomforbundet, 2016, 978-87-574-3392-0.

Den nye persondatarets aktører; Den nye persondatarets aktører af Peter Blume, Jurist- og Økonomforbundet, 2018, 1. udgave, 9788757440263.

Erstatningsret; Lærebog i erstatningsret af Bo von Eyben & Helle Isager, Jurist- og Økonomforbundet, 2011, 7. udgave, 978-87-574-2453-9.

Evald og Schaumburg-Müller; Retsfilosofi, retsvidenskab og retskildelære af Jens Evald og Sten Schaumburg-Müller, Jurist- og Økonomforbundets Forlag, 2004, 1. udgave.

Handbook on European data protection law; Handbook on European data protection law af Den Europæiske Menneskerettighedsdomstol, Den Europæiske Tilsynsførende for Databeskyttelse, Den Europæiske Unions Agentur for Grundlæggende Rettigheder (EU-organ og EU-agentur), Europarådet, Luxembourg: Publications Office of the European Union, 2018 2018, PDF 978-92-9491-901-4, Papir 978-92-9491-903-8.
http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

Kuner; European Data Protection Law – Corporate Compliance and Regulation af Christopher Kuner, Oxford University Press, New York, 2007, 2. udgave.

Motzfeldt; God databehandlingsskik – udvalgte problemstillinger ved forvaltningsmyndigheders videregivelse af personoplysninger af Hanne Marie Motzfeldt, Jurist- og Økonomforbundets Forlag, 2009, 1. udgave, 978-87-574-2127-9.

Artikler, vejledninger og øvrig litteratur:

A Guide for Data Controllers; A Guide for Data Controllers, Data Protection Commission.
https://www.dataprotection.ie/docs/A-Guide-for-Data-Contollers/y/696.htm

Are you a "data controller"?; Are you a "data controller"?, Data Protection Commission.
https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm

Dataansvarlig eller databehandler; Dataansvarlig eller databehandler – med særligt fokus på advokater af Bent Bro Miltersen, Rettid, 2017.
http://law.au.dk/fileadmin/Jura/dokumenter/forskning/rettid/Afh_2017/afh28-2017.pdf

Datatilsynet (Norge) vejledning om databehandleraftaler; Veileder Databehandleravtale, 18.06.2018.
https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/databehandleravtale/?print=true

Dt's Vejledende tekst om tilsyn med databehandlere og underdatabehandlere; Datatilsynets Vejledende tekst om tilsyn med databehandlere og underdatabehandlere, maj 2018.
https://www.datatilsynet.dk/media/6865/vejledende-tekst-om-tilsyn-med-databehandlere-og-underdatabehandlere.pdf

Dt's Vejledning om dataansvarlige og databehandlere; Vejledning om dataansvarlige og databehandlere, November 2017.
https://www.datatilsynet.dk/media/6560/dataansvarlige-og-databehandlere.pdf

ICO Data controllers and data processors; Data controllers and data processors: what the difference is and what the governance implications are, 2014.05.06, Information Commissioner's Office.
https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

ICO Information Governance in Dental Practices; Information Governance in Dental Practices, Summary of findings from ICO reviews, Information Commissioner's Office, September 2015.
https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/1432834/information-governance-in-dental-practices.pdf

ICO Key definitions (arkiveret); Key definitions of the Data Protection Act, Information Commissioner's Office.
http://webarchive.nationalarchives.gov.uk/20180524151709/https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Identity management and data protection law; Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II af Thomas Olsen og Tobias Mahler, Computer Law & Security Review Volume 23, Issue 5, 2007, Pages 415-426.
https://www.sciencedirect.com/science/article/pii/S0267364907000672

Joint Data Controllers under the GDPR; Joint Data Controllers under the GDPR af The Information Technology Panel, maj 2018.
http://www.barcouncilethics.co.uk/wp-content/uploads/2018/05/Joint-data-controllers-under-the-GDPR-pdf.pdf

WP 128; Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Article 29 data protection working party, 22 November 2006.
http://www.dataprotection.ro/servlet/ViewDocument?id=234

WP 140; Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI), Article 29 data protection working party, 20 September 2007.
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp140_en.pdf

WP 169; Opinion 1/2010 on the concepts of "controller" and "processor", Article 29 data protection working party, 16 February 2010.
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

WP 203; Opinion 03/2013 on purpose limitation, Article 29 data protection working party, 2 April 2013.
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Traktater:

Den moderniserede Konvention 108; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. [223], Strasbourg, 10.X.2018.
https://rm.coe.int/16808ade9d

Explanatory Report to CETS No. [223]; Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 10.X.2018.
https://rm.coe.int/16808ac91a

Explanatory Report to the Convention 108; Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981.
https://rm.coe.int/16800ca434

Konvention 108; Konvention nr. 108 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, Strasbourg, 28.I.1981.
https://rm.coe.int/1680078b37

Lissabontraktaten; Lissabontraktaten om ændring af traktaten om Den Europæiske Union og traktaten om oprettelse af Det Europæiske Fællesskab, Lissabon, 13.12.2007.
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12007L/TXT&from=DA

Ratificeret: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

EU Lovgivning:

DBF, Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=EN

TEUF; Konsoliderede udgaver af traktaten om Den Europæiske Union og traktaten om Den Europæiske Unions funktionsmåde, 2012/C 326/01.
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12012E/TXT&from=DA

IMI-forordningen; Europa-Parlamentets og Rådets forordning (EU) Nr. 1024/2012 af 25. oktober 2012 om administrativt samarbejde via informationssystemet for det indre marked og

om ophævelse af Kommissionens beslutning 2008/49/EF (»IMI-forordningen«).
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32012R1024&from=DA

PDD, Europa-Parlamentets og Rådets Direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=en

Retshåndhævelsesdirektivet; Europa-Parlamentets og Rådets Direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA.
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016L0680&from=EL

National lovgivning:

Bogføringsloven; Bekendtgørelse af bogføringslov, lovbekendtgørelse nr 648 af 15/06/2006.
https://www.retsinformation.dk/Forms/R0710.aspx?id=27298

DBL; Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, lov nr 502 af 23/05/2018.
https://www.retsinformation.dk/Forms/R0710.aspx?id=201319

Forvaltningsloven; Bekendtgørelse af forvaltningsloven, lovbekendtgørelse nr 433 af 22/04/2014.
https://www.retsinformation.dk/Forms/R0710.aspx?id=161411

Hvidvaskloven; Lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven), nr 651 af 08/06/2017.
https://www.retsinformation.dk/Forms/R0710.aspx?id=191822

Lov om offentlige myndigheders registre; Lov om offentlige myndigheders registre, lov nr. 294 af 8 juni 1978.
https://digitalimik.gl//~/media/Digitaliseringsstyrelsen/Files/Lovgivning/1978-06-08%20Lov%20om%20Offentlige%20Myndigheders%20Registre%20nr%20294%208%20juni%201978.pdf

Lov om private registre; Lov om private registre, lov nr. 293 af 8 juni 1978.
https://digitalimik.gl//~/media/Digitaliseringsstyrelsen/Files/Lovgivning/1978-06-08%20Lov%20om%20Private%20Registre%20nr%20293%208%20juni%201978.pdf

PDL; Lov om behandling af personoplysninger, lov nr 429 af 31/05/2000.
https://www.retsinformation.dk/Forms/R0710.aspx?id=828

Revisorloven; Lovbekendtgørelse om godkendte revisorer og revisionsvirksomheder, lovbekendtgørelse nr. 1167 af 09/09/2016.
https://www.retsinformation.dk/Forms/R0710.aspx?id=183855

Anbefalinger og beslutninger:

2008/49/EF; Kommissionens beslutning af 12. december 2007 om gennemførelse af informationssystemet for det indre marked (IMI) hvad angår beskyttelse af personoplysninger, 2008/49/EF.
https://eur-lex.europa.eu/legal-content/DA/TXaT/PDF/?uri=CELEX:32008D0049&from=EN

Recommendation 509; Recommendation 509 (1968) vedr. Human rights and modern scientific and technological developments.
http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en

Resolution 73/22; Council of Europe Committee of Ministers, Resolution (73) 22, on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies).
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

Resolution 74/29; Council of Europe Committee of Ministers, Resolution (74) 29, on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51

EU forarbejder:

COM (90) 314 final; COM (90) 314 final - SYN 287 og 288, Bruxelles, den 24. september 1990. Forslag til Rådets direktiv om beskyttelse af personer i forbindelse med behandling af personoplysninger, SYN 287 og Forslag til Rådets direktiv om beskyttelse af personoplysninger og kommunnikationshemmeligheden i forbindelse med offentlige digitale telenet, herunder tjenesteintegrerede digitalenet (ISDN) og offentlige digitale mobilnet, SYN 288, De europæsike Fælleskaber, Rådet, 20.september 1990. ISBN engelsk udg. 92-77-64093-6.
http://aei.pitt.edu/3768/1/3768.pdf

COM (92) 442; Amended proposal for a COUNCIL DIRECTIVE on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final - SYN 287, Brussels, 15 October 1992.
http://aei.pitt.edu/10375/1/10375.pdf

COM (95) 375 final; OPINION OF THE COMMISSION pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 18.07.1995, COM(95) 375 final-COD287.
http://aei.pitt.edu/13101/1/13101.pdf

KOM (90) endelig udg. — SYN 287; Forslag til Rådets direktiv om beskyttelse af personer i forbindelse med behandling af personoplysninger, KOM(90) endelig udg. -SYN 287 (Forelagt af Kommissionen den 27. juli 1990) (90/C 277/03).
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:51990PC0314(01)&from=EN

Betænkninger:

Bet. 1342/1997; Behandling af personoplysninger, Betænkning afgivet af udvalget om registerlovgivningen, Betænkning nr. 1345, 1997, Statens Information, ISBN 87-601-3133-0.
https://www.foxylex.dk/media/betaenkninger/Behandling_af_personoplysninger_betaenkning_afgivet_af_udvalget_om_registerlovgivningen_Del_1.pdf

Bet. 1565/2016; Databeskyttelsesforordningen og de retlige rammer for dansk lovgivning, betænkning nr. 1565, 2016.
http://jm.schultzboghandel.dk/upload/microsites/jm/ebooks/bet1565/index.html

EU Retspraksis:

C-101/01 Lindqvist; Sag C-101/01, Göta hovrätt (Sverige) mod Bodil Lindqvist, 06.11.2003.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=643579

C-201/13 Deckmyn og Vrijheidsfonds; Sag C-201/13, Deckmyn og Vrijheidsfonds, 03.09.2014.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=157281&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649434

C-210/16 Wirtschaftsakademie; Sag C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein mod Wirtschaftsakademie Schleswig-Holstein GmbH, 05.06.2018.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649461

C-25/17 Jehovan; Sag C-25/17, Tietosuojavaltuutettu mod Jehovan todistajat – uskonnollinen yhdyskunta, 10.07.2018.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649483

C-283/81 CILFIT; Sag C-283/81 - CILFIT v Ministero della Sanità, 06.10.1982.
http://curia.europa.eu/juris/showPdf.jsf?text=&docid=91672&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649533

C-327/82 Ekro; Sag C-327/82, Ekro, 18.01.1984.
http://curia.europa.eu/juris/showPdf.jsf?text=&docid=92294&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649603

C-34/10 Brüstle; Sag C-34/10, Brüstle, 18.10.2011.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=111402&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649651

C-40/17 Fashion ID; Sag C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany), 26.01.2017.
https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.112.01.0022.01.ENG

C-465/00 Österreichischer Rundfunk m.fl.; Sag C-465/00, C-138/01 og C-139/01, Rechnungshof mod Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG og Christa Neukomm, Joseph Lauermann mod Österreichischer Rundfunk, 20.05.2003.
http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48330&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649709

C-508/11 P – Eni; Sag C-508/11 P - Eni mod Kommissionen, 08.05.2013.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=137303&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649754

C-544/13 og C-545/13 Abcur; Sag C-544/13 og C-545/13, Abcur, 16.07.2015.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=165910&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649898

Forslag til sag C-131/12 Google Spain; Sag C-131/12 Forslag til afgørelse fra generaladvokat: N. Jääskinen, 25.06.2013, Google Spain SL, Google Inc. mod Agencia Española de Protección de Datos (AEPD), Mario Costeja González.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649943

Forslag til sag C-210/16 Wirtschaftsakademie; Sag C-210/16 forslag til afgørelse fra generaladvokat Y. Bot, 24.10.2017, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein mod Wirtschaftsakademie Schleswig-Holstein GmbH.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=195902&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=649995

Forslag til sag C-25/17 Jehovan; Sag C-25/17 Forslag til afgørelse fra generaladvokat P. Mengozzi, 01.02.2018, Tietosuojavaltuutettu mod Jehovan todistajat – uskonnollinen yhdyskunta.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=198949&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=650034

Afgørelser, udtalelser mv. fra nationale tilstynsmyndigheder:

"Klage over sikkerheden i praktiserende læges journalsystem" Publiceret 27.10.2003; "Klage over sikkerheden i praktiserende læges journalsystem", Datatilsynet, publiceret 27-10-2003.

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2003/okt/klage-over-sikkerheden-i-praktiserende-laeges-journalsystem/

Datainspektionen j.nr. 111-2014; Datainspektionen, j.nr. 111-2014, Svar på Skatteverkets förfrågan om personuppgiftsansvar i Mina Meddelanden.
https://www.datainspektionen.se/globalassets/dokument/gammalt/forfragan-personuppgiftsansvar-i-mina-meddelanden.pdf

Datatilsynet (Norge) vejledning om databehandleraftaler; Datatilsynet (Norge), Veileder Databehandleravtale.
https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/databehandleravtale/?id=7371

Dt's j.nr. 2006-42-1061; Spørgsmål om behandling af personoplysninger i forbindelse med whistleblowing, Datatilsynets journalnummer 2006-42-1061, publiceret 05-12-2006.
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2006/dec/spoergsmaal-om-behandling-af-personoplysninger-i-forbindelse-med-whistleblowing/

Dt's j.nr. 2007-213-0022; Spørgsmål om synkronisering af ure ved tv-overvågning, Datatilsynets journalnummer 2007-213-0022, Publiceret 08-10-2007.
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2007/okt/spoergsmaal-om-synkronisering-af-ure-ved-tv-overvaagning/

Dt's j.nr. 2007-321-0027; Vedrørende høring over Beskæftigelsesministeriets ESDH-projekt, Datatilsynets Journalnummer: 2007-321-0027, Publiceret 20-08-2007.
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2007/aug/vedroerende-hoering-over-beskaeftigelsesministeriets-esdh-projekt/

Dt's nyhedsbrev af 08.08.2001; Afslutning af harddisksagen, Datatilsynets nyhedsbrev, 08.08.2001.

Københavner-erklæring; Nordic data protection authorities working together, København, 08.05.2018.
https://www.datatilsynet.dk/media/6816/copenhagen-declaration.pdf

Hjemmesider:

Chart of signatures and ratifications of Treaty 108
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=kLhh6tYc (Link sidst tilgået den 31.08.2018)

Nonprofitorganisationen noyb.eu (None of your buisness)
https://www.noyb.eu (Link sidst tilgået den 31.08.2018)

Øvrigt:

De advokatetiske regler; De advokatetiske regler, Advokatsamfundet, 1. november 2016.
http://www.advokatsamfundet.dk/Advokatregulering/ReglerOgVedtaegter/Alle%20regler.aspx

DPA 1998; Data Protection Act, 1998, Reprinted Incorporating Corrections 2005. https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

EU-domstolens pressemeddelelse nr. 36/18; Den Europæiske Unions Domstol Pressemeddelelse nr. 36/18 Luxembourg den 23. marts 2018. https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-03/cp180036da.pdf

Rigsadvokatmeddelelsen om strafansvar for juridiske personer; Rigsadvokatmeddelelsen, Juridiske personer - Strafansvar for juridiske personer 17.4.2015. https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/0624de33-d1a2-4910-a8f4-7801b4c142bb

Rigsadvokatmeddelelsen, Sager om overtrædelse af databeskyttelsesreglerne; Rigsadvokatmeddelelsen, Sager om overtrædelse af databeskyttelsesreglerne, 25.05.2018. https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/c9b2bc89-c740-4303-9e47-f0dbea47d99c