

Dataansvarlig eller databehandler – med særligt fokus på advokater

Controller or processor - especially regarding lawyers

af BENT BRO MILTERSEN

I specialet behandles spørgsmålet om, hvornår en organisation er henholdsvis dataansvarlig og databehandler. De to begreber er defineret i persondatalovgivningen, men virkeligheden er ofte for kompliceret til, at man kan presse faktum ind under disse definitioner. Dette fører til, at der i praksis kan opstå tvivl om organisationens rolle, til skade for både organisationen og den registrerede.

Afklaringen af spørgsmålet er især vigtigt i forhold til de mange virksomheder, der er i gang med implementeringen af den nye persondataforordning. I specialet er der derfor foretaget en nærmere undersøgelse af baggrunden for de to begreber, og hvordan man kan anvende dem i den praktiske verden.

I anden del af specialet bliver det behandlet, hvilken rolle advokater og advokatkontorer har i en række forskellige tilfælde.

Indholdsfortegnelse

Indholdsfortegnelse	1
English summary	2
Controller or processor - especially regarding lawyers	2
Forkortelser:	3
1. Indledning	3
1.1. Præsentation af emnet	3
1.2. Problemformuleringen	5
1.3. Afgrænsning	6
2. Metode og kilder	6
2.1. Metode	6
2.2. Kilder	6
3. Den abstrakte fortolkning af de to begreber	7
3.1. Karakteren af de to begreber	7
3.1.1. Konklusion:	9
3.2. Rækkevidden af EU-konform fortolkning	9
3.2.1. Konklusion	10
3.3. Begrebernes kontekst og formål	11
3.3.1. Konklusion	12
3.4. Hvem bestemmer formålet og hjælpemidlerne?	12
3.4.1. Konklusion	16
3.5. Nærmere om formålet med behandlingen	17
3.5.1. Konklusion	18
3.6. Nærmere om kontrol	18

3.7.Hvad er man dataansvarlig for?	20
3.7.1.Konklusion	22
3.8.Kan den registrerede være dataansvarlig?.....	22
3.8.1.Konklusion	23
3.9.Hvilke personer er dataansvarlige og databehandlere?	23
3.9.1.Konklusion	24
3.10.Særligt om dataansvar i koncerner og joint ventures	24
3.10.1.Konklusion	27
3.11.Undtagelsen om privat/familiemæssig brug og en generel bagatelgrænse for dataansvaret	27
3.11.1.Konklusion	28
3.12.Samlet konklusion af den abstrakte fortolkning af de to begreber.....	29
4.Advokaters dataansvar	29
4.1.Præsentation af problemstillingen vedr. advokater	29
4.2.Advokater i rådgiverrollen	30
4.2.1.Konklusion	33
4.3.Behandlingen er lovpligtig	33
4.4.Behandling af oplysninger om klienten selv og dennes familie.....	34
4.4.1.Konklusion	35
4.5.Behandling af personoplysninger som procesførende advokat.....	35
4.5.1.Konklusion	36
4.6.Ansvarsfordeling mellem advokaten som fysisk person og advokatselskabet	36
4.6.1.Konklusion	37
4.7.Samlet konklusion af advokaters dataansvar	37
5.Samlet konklusion af specialet.....	37
5.1.Konklusion	37
6.Perspektivering.....	38
6.1.Perspektivering.....	38
Litteraturliste.....	38
Bilag 1 – Mail fra Datatilsynet d. 11. maj 2017.....	42

English summary

Controller or processor - especially regarding lawyers

Directive 95/46/EC contains two main “actors”, namely the controller and the processor. Whether a person is one or the other can have a significant impact on the person’s compliance with data protection law. It is, however, an exceedingly difficult task to distinguish between the two, especially considering the ever-growing complexity of data processing and business practice.

In this dissertation, the author, first of all, sets out to identify the elements of the abstract interpretation of the two concepts and lay out some principals for their application in practice. Hereafter, the author considers how the two concepts apply to lawyers.

The author concludes that the concept of controller should be subject to a widened interpretation, limiting the scope of the concept of the processor. In regards to lawyers, they will be viewed as controllers in most cases.

Forkortelser:

ICO	Information Commissioner's Office (britisk datatilsyn)
KPDL	Den kommenterede persondatalov
ORL	Lov om offentlige myndigheders registre
PDD	Persondatadirektivet
PDL	Persondataloven
PDF	Persondataforordningen
PRL	Lov om private registre mv.
SL	Selskabsloven
STRFL	Straffeloven
WP	Working paper (vejledning udstedt af Artikel 29-gruppen)

1. Indledning

1.1. Præsentation af emnet

Persondataretten er i dag reguleret af PDL, der er baseret på PDD. Den 25. maj 2018 træder den nye PDF i kraft. Forordningen viderefører i stort omfang reglerne fra det nu gældende persondatadirektiv, men der indføres også nye regler. Fx indfører forordningen et meget højere bødeniveau. Dette har gjort stort indtryk på både erhvervsdrivende og det offentlige, og der bliver gjort store bestræbelser for at implementere forordningen i alle typer organisationer. I det praktiske liv er der således et stort behov for den størst mulige afklaring af de persondataretlige regler.

Et stort problem under de nuværende regler er sondringen mellem persondatarettens to pligtsubjekter: den dataansvarlige og databehandleren. Den dataansvarlige er som udgangspunkt den, der har kontrol over en behandling af personoplysninger og dermed også ansvaret for behandlingens lovlighed, såvel strafferetligt som erstatningsretligt. Databehandleren er en person, der udfører en behandling af personoplysninger på vegne af den dataansvarlige efter dennes instrukser uden at have selvstændig kontrol over behandlingen. Databehandleren har som følge heraf ikke ansvaret for lovligheden. Formålet med sondringen er dermed at fordele ansvaret for overholdelsen af de persondataretlige regler og forhindre omgåelse af dataansvaret ved, at dataansvarlige kan lade andre udføre behandlinger på sine vegne efter instrukser uden at have noget ansvar. Grundlæggende går ordningen ud på, at med kontrollen over en behandling følger også et ansvar for behandlingens lovlighed. I sidste ende er formålet at sikre en effektiv og fuldstændig beskyttelse af den registrede, hvilket fremgår af C-131/12, Google Spain.¹

I praksis kan det dog være enormt svært at vurdere, hvor grænsen skal drages mellem den dataansvarlige og databehandleren, da der findes et utal af forskellige samarbejds- og handelsformer med varierende grader af kontrol. De to begreber er defineret næsten fuldstændig enslydende i både

¹ Dommens præmis 34

PDD, PDL og PDF,² og PDF viderefører dermed direktivets definitioner, uden de bliver nærmere præciseret. Dette medfører en fortsat stor usikkerhed i retsstillingen. Under direktivet har medlemsstaterne desuden udviklet forskellige opfattelser af spørgsmålet.³ Disse forskelle blandt medlemsstaterne kan give anledning til store problemer for erhvervsdrivende med grænseoverskridende aktiviteter. Skelnen mellem den dataansvarlige og databehandleren har grundlæggende betydning for flere forskellige forhold:⁴

- **Hvem der er ansvarlig for overholdelsen af reglerne.** Det er som udgangspunkt den dataansvarlige, der er ansvarlig for overholdelsen af reglerne. Det er den dataansvarlige, der får en bøde eller ifalder et erstatningsansvar, hvis reglerne bliver overtrådt. Det er den dataansvarlige, der skal sørge for de nødvendige foranstaltninger, inden en behandling af personoplysninger påbegyndes, og det er den dataansvarlige, der skal sørge for den registreredes rettigheder og sikkerhed. Databehandleren er blot en forlængelse af den dataansvarlige og er ansvarsfri så længe den dataansvarliges ordrer og instrukser bliver fulgt.⁵
- **Hvordan den registrerede kan udøve deres rettigheder.** Den registrerede har en række rettigheder i PDL, som de udøver over for den dataansvarlige. Den registrerede kan fx kræve indsigt i oplysninger om vedkommende over for den dataansvarlige, jf. PDL § 33, stk. 1. Den registreredes rettigheder bliver udvidet, når forordningen træder i kraft.⁶ Hvis den registrerede skal kunne udøve disse rettigheder effektivt, må der være en klarhed omkring, hvem der er dataansvarlig.
- **Lovvalg.** Ifølge PDL § 4, stk. 1, gælder loven for behandlinger, hvor den dataansvarlige er etableret i Danmark. Det er således afgørende for lovvalget, hvem der er dataansvarlig. Lovvalg vil stadig have betydning internt i EU, når forordningen træder i kraft, da forordningen giver medlemsstaterne mulighed for at udstede særskilte nationale forskrifter.⁷
- **Forholdet mellem kontraktparter.** Den dataansvarlige skal føre tilsyn med databehandleren og give databehandleren instrukser og retningslinjer, jf. PDL §§ 41, stk. 1, og 42, stk. 1. Dette kan medføre gnidninger parterne imellem i deres daglige forretningsførelse, og tilsynspligten må betegnes som byrdefuld for den dataansvarlige.
- **Hvad man må gøre med personoplysningerne.** Den dataansvarlige må behandle personoplysninger, så længe han overholder de persondataretlige regler. Den dataansvarlige har under visse betingelser mulighed for at bruge indsamlede oplysninger til andre formål end de oprindelige. Databehandleren må derimod kun behandle personoplysninger efter den dataansvarliges instrukser og kan ikke bruge dem til eget formål. Efter PDF art. 28, stk. 3, litra g, skal databehandleren slette eller tilbagegive alle oplysninger, når hans opgave er færdiggjort.

² PDL § 3, nr. 4 og 5, direktivets art. 2, litra d og e, samt forordningens art. 4, nr. 7 og 8. I direktivet er begreberne dog benævnt "den registeransvarlige" og "registerføreren", hvilket dog ikke har nogen retlig betydning, jf. Betænkning nr. 1342/1997, s. 210. I retslitteraturen er den dataansvarlige visse steder benævnt "dataforvalter".

³ WP 169, s. 2.

⁴ WP 169, s. 1 og 4-6 og "Data Protection" s. 266

⁵ Se PDL §§ 41-42. Når forordningen træder i kraft, får databehandleren dog også få selvstændige pligter, fx pligten til at anmelde sikkerhedsbrud til den dataansvarlige, jf. PDF art. 33, stk. 2. Desuden kan databehandlere blive dataansvarlige, hvis de overskrider aftalen med den dataansvarlige og selv fastlægger formålet med behandlingen og de anvendte hjælpemidler, hvilket nu fremgår eksplicit af PDF art. 28, stk. 10. Selv hvis databehandleren overskrider den dataansvarliges instrukser, bliver den dataansvarlige kun ansvarsfri, hvis han kan påvise, han har ført tilstrækkelig tilsyn med databehandleren.

⁶ Fx retten til begrænsning, jf. PDF art. 18.

⁷ PDF kapitel IX.

- **Om visse formelle betingelser skal være opfyldt.** Antager en dataansvarlig en databehandler, skal der indgås en skriftlig databehandleraftale, jf. PDL § 42, stk. 2. Når forordningen træder i kraft, skal den dataansvarlige desuden kunne dokumentere overholdelsen af forordningen, herunder dokumentere tilsynet med databehandleren, jf. forordningens art. 5, stk. 2.
- **Opfyldelsen af oplysningspligten.** Efter PDL §§ 28-29 skal den registrerede have forskellige oplysninger udleveret, når oplysninger om vedkommende indsamles. Bl.a. skal den registrerede have oplyst identiteten på den dataansvarlige, jf. PDL § 28, stk. 1, nr. 1, og § 29, stk. 1, nr. 1. Denne pligt videreføres i PDF art. 13-14.

Det er derfor strengt nødvendigt at fastlægge indholdet af de to begreber. Dels skal de erhvervsdrivende let kunne gennemskue deres retsstilling når de indgår i et samarbejde med en forretningspartner, dels skal begreberne anvendes ens i medlemsstaterne for at udvikle og fastholde den grænsoverskridende økonomiske aktivitet, både inden for og uden for EU. Særligt henset til forordningens og direktivets mål om at sikre den fri udveksling af personoplysninger inden for unionen, må det være vigtigt, at der ikke er tvivl om skelnen mellem de to begreber.⁸ Dette mål kan næppe sikres, hvis medlemsstaterne har forskellige opfattelser af problemstillingen. Desuden vil tvivl om begrebernes fortolkning bringe den registreredes rettigheder i fare. Den registrerede kan ikke udøve sine rettigheder over for den dataansvarlige, når det ikke er gennemskueligt, hvem dataansvaret påhviler. Når forordningen træder i kraft, vil bødeniveauet nå nye højder, hvilket også understreger vigtigheden af en afklaring af problemet, da erhvervsdrivende risikerer bødeansvar for at forsømme et dataansvar, de ikke vidste, de havde.

Konkret opstår problemstillingen, når en person antager en anden person til at udføre en opgave, der indebærer behandling af personoplysninger. Afhængig af graden af kontrol og selvstændighed kan parterne være dataansvarlige, fælles dataansvarlige eller databehandlere. Generelt kan det siges, at jo mere kontrol en part har, jo tættere er han på at være dataansvarlig. Har parten ingen kontrol over behandlingen, er han databehandler. Det har imidlertid i litteraturen og i det praktiske liv ikke været muligt at nå en konsensus om, hvor grænsen skal drages mellem den dataansvarlige og databehandleren. Hvor meget kontrol skal man udøve for at være dataansvarlig? Hvad skal man udøve kontrol over? Hvad er man i det hele taget dataansvarlig for? I denne afhandling skal det derfor forsøges at fastlægge en abstrakt fortolkning af de to begreber ved at formulere nogle generelle principper for vurderingen.

Datatilsynet i Danmark og den danske retslitteratur har den anskuelse, at advokater i de fleste forhold er databehandlere, mens Artikel 29-gruppen og tilsynsmyndigheder i andre medlemsstater har en anden opfattelse. Advokater er således i stor fare for at overtræde persondataretten ud fra en vildfarelse om deres dataansvar. I denne afhandling vil advokaternes retsstilling derfor blive undersøgt nærmere.

1.2. Problemformuleringen

Spørgsmålet er, hvornår man er dataansvarlig og databehandler, særligt vedrørende advokater.

⁸ Se PDF art. 1, stk. 3, og PDD art. 1, stk. 2.

1.3. Afgrænsning

I denne afhandling vil der blive fastlagt en abstrakt fortolkning af de to begreber dataansvarlig og databehandler. Den abstrakte fortolkning skal fastlægge de generelle principper for den retlige subsumtion. Herefter vil principperne blive anvendt på advokater.

Af hensyn til kravene til afhandlingens længde vil andre situationer, hvor problemstillingen kan opstå, ikke blive behandlet. Andre gruppers dataansvar såsom udbydere af cloud-ydelser vil derfor ikke blive behandlet. Der vil heller ikke blive foretaget en nærmere fortolkning af begreberne fælles dataansvarlig eller underdatabehandler. Fokus vil desuden være på dataansvaret i den private sektor. For så vidt angår behandlingen af problemstillingen i forhold til advokater, vil kun det direkte dataansvar og identifikation mellem advokat og selskab blive behandlet, men ikke andre advokaters eller advokatselskabets evt. hæftelse på andet grundlag eller et evt. arbejdsgiveransvar efter DL 3-19-2.

2. Metode og kilder

2.1. Metode

Afhandlingen vil et give et svar på problemformuleringen ud fra en retsdogmatisk tilgang, hvor de traditionelle retskilder⁹ inddrages i en systematisk analyse, diskussion og vurdering af problemet. De forskellige retskilders styrker og svagheder vil løbende blive vurderet, og deres fortolkningsbidrag vil blive sammenlignet med hinanden. Desuden vil andre kilder blive inddraget i det omfang, de bidrager til belysningen af problemet, bl.a. ud fra en vurdering af kvaliteten af kildens argumentation. Her tænkes der særligt på retslitteraturen og vejledninger fra Artikel 29-gruppen. Den komparative metode vil også blive anvendt ved at sammenligne de danske kilder med udenlandske kilder for at belyse problemstillingen yderligere.

2.2. Kilder

Historisk har området været reguleret på forskellig vis. I Danmark startede den persondatarelige regulering i 1978 med vedtagelsen af de to registerlove.¹⁰ I 1981 blev Europarådets konvention 108/1981¹¹ vedtaget. Konventionen fastsatte visse minimumskrav for nationalstaternes persondatubeskyttelse. Konventionen blev ratificeret af Danmark i 1989. I 1995 blev PDD vedtaget og implementeret for Danmarks vedkommende i 2000 med PDL. I 2016 blev PDF vedtaget, og den træder i kraft d. 25. maj 2018. Sideløbende er der afsagt domme og afgørelser. Henset til udviklingen i persondataretten vil der derfor i et vist omfang blive draget linjer tilbage i tiden. Afhandlingen vil også have et fremtidigt perspektiv ved løbende at inddrage PDF.

⁹ De traditionelle retskilder anføres ofte som lovgivning, bekendtgørelser, forarbejder, retspraksis, administrativ praksis, retssædvaner, retsgrundsætninger og forholdets natur. Der er i øvrigt ikke enighed om retskildebegrebet. Fx betragter nogle retsvidenskabsmænd retslitteraturen som en retskilde, og andre vil udelade retspraksis og administrativ praksis som (formelle) retskilder. Det er ikke meningen med denne afhandling at behandle dette problem nærmere.

¹⁰ Lov nr. 293 af 08/06/1978 om private registre m.v. (PRL) og lov nr. 294 af 08/06/1978 om offentlige myndigheders registre (ORL).

¹¹ Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.

Ud over de formelle kilder nævnt ovenfor, vil både dansk og udenlandsk retslitteratur blive inddraget, herunder også Artikel 29-gruppens og ICO's vejledninger.

3. Den abstrakte fortolkning af de to begreber

3.1. Karakteren af de to begreber

Allerede i lov om private registre mv.¹² fra 1978 skelnedes der mellem registeransvarlige og edb-servicebureauer. Mens den registeransvarlige var hovedpligtssubjektet, var man allerede dengang opmærksom på, at den registeransvarlige kunne lade andre udføre databehandling på sine vegne, hvilket kunne give nogle problemer i forhold til reglerne om ansvar. I lovenes kapitel 5 var der derfor en regulering af *edb-servicebureauer*. Disse blev i lovens § 20 omtalt som:

”Virksomheder, der **for tredjemand**, herunder for en offentlig myndighed, **udfører elektronisk databehandling** af oplysninger som nævnt i § 1...”

Databehandlere er i PDL § 3, nr. 5, defineret som:

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

Umiddelbart forekommer ligheden mellem de to begreber slående. Ligeledes er i det hele taget ideen om en sondring mellem en ansvarlig og personer, der handler på vegne af den ansvarlige, noget der findes i både registerlovgivningen, PDD og PDL. I Betænkning nr. 1342/1997¹³ udtalte udvalget derfor om databehandleren:¹⁴

”Bestemmelsen [§ 3, nr. 5] fastsætter, hvad der skal forstås ved begrebet databehandleren. I den gældende registerlovgivning findes ikke nogen legal definition af dette begreb. **Bestemmelsens definition af begrebet databehandleren må dog antages at svare til, hvad der efter den gældende registerlovgivning anses for at være en databehandler.** Der henvises herved til § 20, stk. 1, i lov om private registre, der fastsætter hvad der skal forstås ved et edb-servicebureau (databehandler)”.

Om den dataansvarlige, skriver udvalget:¹⁵

”Bestemmelsen [§ 3, nr. 4] fastsætter, hvad der skal forstås ved begrebet den dataansvarlige. Begrebet den dataansvarlige er ikke defineret i gældende dansk registerlovgivning. **Den givne definition i bestemmelsen må dog antages at svare til, hvad der i dag antages at gælde på ulovbestemt grundlag. Bestemmelsen kan således ikke antages at medføre nogen ændringer i gældende ret. Registertilsynets praksis**

¹² I lov om offentlige registre nævnes den ”registeransvarlige myndighed”. Et tilsvarende udtryk bruges ikke i loven om private registre, men ordet blev brugt i praksis af Registertilsynet om private virksomheder. Se fx Registertilsynets årsberetning fra 1997, hvor tilsynet skriver: ”Også i den private sektor er det virksomheden selv, der som *registeransvarlig* i det daglige må tage stilling til...”. Dette bekræftes i Betænkning nr. 1342/1997, s. 433, til nr. 4: ”Den givne definition [om dataansvarlig/registeransvarlig] i bestemmelsen må dog antages at svare til, hvad der i dag antages at gælde på ulovbestemt grundlag.

¹³ ”Behandling af personoplysninger”, betænkning afgivet af udvalget om registerlovgivningen.

¹⁴ Betænkning nr. 1342/1997, s. 434

¹⁵ Betænkning nr. 1342/1997, s. 433

vedrørende udpegningen af den dataansvarlige vil dermed fortsat kunne tillægges betydning”.

Udvalget lagde dermed linjen til forståelsen af den dataansvarlige og databehandleren: Begreberne skulle forstås på samme måde, som man forstod begreberne den registeransvarlige og edb-servicebureau under registerlovgivningen.

Dette synspunkt har også slået igennem i den danske retslitteratur. I KPDL læner forfatterne sig op ad Registertilsynets praksis. Således skriver forfatterne generelt om de to begreber:¹⁶

”Definitionen [af den dataansvarlige]... **må dog i vidt omfang antages at svare til, hvad der tidligere på ulovbestemt grundlag blev anset for den registeransvarlige.** Registertilsynets praksis vedrørende udpegningen af den dataansvarlige (registeransvarlige) vil dermed fortsat kunne tillægges betydning....

Registertilsynets praksis vil derfor fortsat have betydning ved fastlæggelsen af begrebet databehandler.”

Det ovenstående synspunkt om den tidligere skelnen mellem registeransvarlige og edb-servicebureauer er dog stærkt kritisabel, da der ikke tages hensyn til PDL's baggrund i PDD. Det generelle spørgsmål om fortolkning af begreber fra direktiver blev behandlet i C-149/15 Wathelet, der omhandlede fortolkningen af begrebet ”sælger” i direktiv 1999/44 (direktivet om visse aspekter af forbruger køb og garantier i forbindelse hermed):¹⁷

”[...] i henhold til Domstolens faste praksis følger af kravet om en ensartet anvendelse af EU-retten, at **såfremt en bestemmelse i EU-retten ikke indeholder nogen udtrykkelig henvisning til medlemsstaternes ret hvad angår et særligt begreb, skal denne sidstnævnte undergives en selvstændig og ensartet fortolkning i hele Den Europæiske Union, som skal søges under hensyntagen til bestemmelsens kontekst og formålet med den pågældende ordning**

Henset til, at artikel 1, stk. 2, litra c), i direktiv 1999/44 definerer begrebet »sælger« uden nogen henvisning til national ret for så vidt angår betydningen af dette begreb, skal bestemmelsen dermed **anses for at indeholde et selvstændigt EU-retligt begreb, som ved anvendelsen af dette direktiv skal fortolkes ens på EU's område”.**

Ifølge dommen skal et begreb fra et direktiv altså anses som et selvstændigt EU-retligt begreb, der skal underkastes en ensartet fortolkning i hele EU, medmindre direktivet konkret henviser til national ret. Fortolkningen af begrebet skal hvile på bestemmelsens kontekst og formålet med direktivets ordning.

Dermed kan det slutes, at begreberne dataansvarlig og databehandler må være selvstændige, EU-retlige begreber i det omfang, direktivet ikke henviser til national ret.¹⁸ PDD henviser imidlertid til national ret ved definitionen af dataansvarlig (registeransvarlig) i art. 2, litra d:

¹⁶ Se KPDL s. 162-164

¹⁷ Dommens præmis 28-29.

¹⁸ Dette resultat nås også i WP 169, s. 8.

”; er formålet med og hjælpemidlerne ved behandlingen fastlagt ved nationale love eller forskrifter eller på fællesskabsplan, kan den registeransvarlige, eller de specifikke kriterier for udpegelse af denne, angives i den pågældende nationale ret eller i fællesskabsretten”.

Dette er dog en snæver henvisning til national ret, der forudsætter, at den nationale ret fastlægger formålet eller hjælpemidlerne med en behandling, hvorefter man i den nationale ret kan fastlægge en anden definition eller direkte udpege den dataansvarlige ved lov.¹⁹ I alle andre tilfælde, må de to begreber derfor være selvstændige EU-retlige begreber. Som følge heraf, er fortolkningsbidrag tilbage fra de danske registerlove fra 1978 uden betydning, da national ret ikke kan influere på fortolkningen af selvstændige EU-retlige begreber.

Denne opfattelse bekræftes i C-131/12, Google Spain, der bl.a. omhandler fortolkningen af begrebet dataansvarlig. EU-domstolen tager i fortolkningen kun udgangspunkt i ordlyden af direktivets definition og formål, og der henvises ikke til medlemsstatens (Spaniens) nationale ret.²⁰

3.1.1. Konklusion:

De to begreber har karakter af selvstændige EU-retlige begreber, der skal fortolkes ud fra bestemmelsernes kontekst og ordning. Fortolkningsbidrag fra den danske registerlovgivning kan ikke bruges ved fastlæggelsen af de to begreber.

3.2. Rækkevidden af EU-konform fortolkning²¹

Konklusionen fra forrige afsnit bygger på, at retsanvenderen er forpligtet til at fortolke EU-konformt. Man må kunne fastholde synspunktet fra forarbejderne til PDL i det omfang, man ikke er forpligtet til at fortolke EU-konformt. Det næste relevante spørgsmål må herefter være, om der er en pligt til at fortolke EU-konformt, og hvilken rækkevidde, denne pligt har.

EU-domstolen har tidligere fastslået, at selvom en fællesskabsretlig regel ikke finder direkte anvendelse, har medlemsstaterne stadig pligt til at foretage en EU-konform fortolkning ved deres anvendelse af national ret. Denne pligt blev første gang slået fast i sag 14/83 von Colson.²²

”Heraf følger at ved anvendelsen af national ret [...] er den nationale domstol forpligtet til at fortolke intern ret i lyset af direktivets ordlyd og formål og at fremkalde det resultat, der tilstræbes ved traktatens artikel 189, stk. 3.”

Hermed blev det slået fast, at medlemsstaten, er forpligtet til at fortolke en implementeringslov i lyset af det direktiv, den implementerer. I bilag 16 til Registerlovgivningsudvalgets betænkning, anerkendes det da også, at national lovgivning skal fortolkes direktivkonformt.²³

¹⁹ Det har ikke været muligt at finde en sådan bestemmelse i dansk ret, der udnytter denne mulighed. Et eksempel fra udlandet er Storbritanniens Data Protection Act of 1998, section 1 (4), der bestemmer, at når en behandling er pålagt ved lov, er den forpligtet altid dataansvarlig. Dette vil dog alligevel være tilfældet i de fleste, hvis ikke alle tilfælde, hvorfor bestemmelsen må karakteriseres som overflødig.

²⁰ Se dommens præmis 32-41.

²¹ Se ”Europæiseringen af dansk ret”, s. 303, 310 og 318ff.

²² Sag 14/83 von Colson, præmis 39

²³ Betænkning nr. 1342/1997, bilag 16: ”Justitsministeriets notits af 10. september 1996 om udformningen af lovbestemmelser i tilknytning til gennemførelse af direktiver i danske ret”, betænkningens anden del, s. 191.

På baggrund af dommen må det også stå klart, at fortolkningspligten påhviler medlemsstaten, herunder alle offentlige myndigheder og domstolene. Danmarks domstole og Datatilsynet er dermed som udgangspunkt generelt forpligtet til at fortolke PDL EU-konformt i lyset af PDD.

Det blev imidlertid slået fast i C-212/04 Adeneler, at man ikke er forpligtet til at fortolke *imod national ret (contra legem)*. Dette kan tænkes at være problematisk i forhold til det nærværende problem, da de danske forarbejder instruerer retsnavenderen i at foretage en helt bestemt fortolkning, der afviger fra direktivet. Er en fortolkning således *contra legem*, hvis ordlyden af den nationale lov kan rumme det EU-konforme resultat, men de nationale forarbejder klart forbyder dette resultat? Dette spørgsmål blev behandlet i C-371/02 Björnekulla, præmis 13:²⁴

”Når en national ret skal fortolke nationale retsfor skrifter, hvad enten de er ældre eller yngre end et direktiv, er den forpligtet til, **i videst muligt omfang** at fortolke dem i lyset af direktivets ordlyd og formål og at fremkalde det med direktivet tilsigtede resultat [...], **uanset at der i forarbejderne til den nationale bestemmelse findes elementer, der kunne føre til en anden fortolkning**”.

Pligten til at fortolke EU-konformt gælder dermed også, uanset den EU-konforme fortolkning er i strid med forarbejderne. Ved fortolkningen af de to begreber dataansvarlig og databehandler, er man således ikke bundet af forarbejderne til PDL, hvis de er i strid med den EU-konforme fortolkning.

Fortolkningspligten må også gælde, selvom EU-retten ikke er klar. Hvis EU-retten ikke har en klar løsning (fx hvis der ikke foreligger nogen EU-dom) må retsnavenderen selv fortolke EU-retten. Domstolene vil efter omstændighederne have en ret (og en pligt) til at stille præjudicielle spørgsmål om fortolkningen af EU-retten til EU-domstolen, jf. TEUF art. 267, hvilket gør den EU-konforme fortolkning betydeligt nemmere. Den samme mulighed har Datatilsynet og andre europæiske datatilsyn ikke, da de ikke kan anses som en ”ret” efter TEUF art. 267. Dette åbner op for, at alle de forskellige datatilsyn kan have hver deres EU-retlige fortolkning af begreberne den dataansvarlige og databehandleren, men man må holde fast i, at fortolkning af begreberne skal hvile på en analyse af de EU-retlige kilder.

Dernæst vil det få en betydning for fortolkningen af de to begreber, når området fra maj 2018 ikke længere reguleres af PDD, men i stedet af PDF. Når først PDF træder i kraft, må det betyde, at begreberne umuligt kan fortolkes efter synspunkterne i forarbejderne til PDL, da forordningen er en selvstændig retsakt, der naturligvis ikke fortolkes i lyset af national ret.

3.2.1. Konklusion

Både de danske domstole og Datatilsynet er forpligtet til at fortolke EU-konformt *ex officio*. En sådan pligt foreligger dog ikke, hvis den EU-konforme fortolkning er i strid med national ret (*contra legem*). En fortolkning i strid med forarbejderne til PDL kan dog ikke anses for at være *contra legem*. Man er således forpligtet til at fortolke EU-konformt, så længe fortolkningen kan rummes inden for ordlyden af bestemmelsen. Pligten gælder uanset om EU-retten er klar eller uklar, om end dette åbner op for, at retsnavendere, der ikke kan forelægge præjudicielle spørgsmål,

²⁴ Se Europæiseringen af dansk ret”, s. 321-322.

som fx Datatilsynet, kan have forskellige EU-retlige fortolkninger af de to begreber. Når forordningen træder i kraft i maj 2018, vil det være helt umuligt at fortolke de to begreber i lyset af national ret.

3.3. Begrebernes kontekst og formål

De to begreber dataansvarlig og databehandler må anses som selvstændige EU-retlige begreber, se afsnit 3.1. Det følger af den i afsnit 3.1. nævnte dom, C-149/15 Wathelet, at selvstændige EU-retlige begreber skal fortolkes i lyset af deres bestemmelses kontekst og ordningens formål. Hvad er da de to begrebers kontekst og formål? Dette spørgsmål blev behandlet i C-131/12, Google Spain, for så vidt angår den dataansvarlige:²⁵

[...] men også med dens formål – **som består i at sikre en effektiv og fuldstændig beskyttelse af de berørte personer ved at fastsætte en bred definition af begrebet ”ansvarlig”** [...]”.

Ved fortolkningen af begrebet dataansvarlig, skal man altså tage hensyn til formålet, der består i at sikre en effektiv og fuldstændig beskyttelse af den registrerede. Dette følger også af, at persondatabeskyttelse er blevet optaget som en selvstændig, grundlæggende menneskerettighed i Den Europæiske Unions Charter om grundlæggende rettigheder art. 8. Dette formål opnås i videst muligt omfang ved at have en så bred definition som muligt af begrebet. Man vil hermed dæmme op for, at en person planlægger en behandling og instruerer en anden i at udføre behandlingen, uden selv at være dataansvarlig. Omvendt lempes ansvaret for personen, der blot udfører den dataansvarliges ordrer.

Dette er dog ikke det eneste formål, man kan pege på. Selvom det ikke står eksplicit i PDD, er det utvivlsomt, at et andet afgørende formål må være kravet om gennemsigtighed, både af hensyn til den registrerede, så han nemt kan udøve sine rettigheder, men ligeledes af hensyn til erhvervslivet, der skal kunne tilrettelægge deres forretning og forudsige deres retsstilling. Princippet om gennemsigtighed følger dog implicit af direktivets art. 10-12, der pålægger den dataansvarlige en oplysningspligt og giver den registrerede en indsichtsret. Princippet om gennemsigtighed fremgår da nu også eksplicit af PDF, jf. forordningens art. 5, stk. 1, litra a, og betragtning nr. 13. Ved fortolkningen skal man altså tilstræbe at udvikle nogle simple principper, der gør vurderingen nemmest for både den registrerede og erhvervslivet.

EU-domstolen nævner ikke direkte begrebernes kontekst i Google Spain-dommen. Ud fra en umiddelbar sproglig forståelse af ”kontekst”, må det siges, at man kan inddrage flere momenter i denne sammenhæng. Man må i hvert fald kunne inddrage, hvilken kontekst, begreberne umiddelbart optræder i i direktivets tekst. Til dette kan man påpege, at de to begreber optræder som en del af en liste over legaldefinitioner. Nærmere bestemt optræder de to begreber sammen som definitioner af de to pligtsubjekter i direktivet, og de må derfor have en sammenhæng med hinanden og skal forstås sammen og ikke hver for sig. Yderligere bør man kunne inddrage konteksten mellem to personer i en konkret sag, hvor man analyserer de to personers roller, fx graden af parternes professionalisme. Man vil formentlig også kunne inddrage den historiske kontekst, hvor man ser på udviklingstendenser af begreberne.

²⁵ Dommens præmis 34

3.3.1. Konklusion

Ved fortolkning af de to begreber skal man inddrage formålet med begreberne og konteksten, de indgår i. Formålet med begrebet dataansvarlig er at sikre en effektiv og fuldstændig beskyttelse af de registrerede. Begrebet skal derfor fortolkes udvidende. De to begreber optræder sammen i den samme kontekst og skal derfor fortolkes sammen. Da dataansvarlig skal fortolkes udvidende, må dette ske på bekostning af databehandlerbegrebet, der indskrænkes. I øvrigt må man kunne inddrage konteksten i den konkrete sag, man vurderer.

3.4. Hvem bestemmer formålet og hjælpemidlerne?

Efter at have fastlagt karakteren af de to begreber og afvist synspunktet fra forarbejderne om sondringen mellem registeransvarlige og edb-servicebureauer, kan afhandlingen nu koncentrere sig om, hvilke momenter, man skal lægge vægt på ved fortolkningen af de to begreber, og hvordan momenterne skal vægtes og anvendes.

Direktivets art. 2, litra d, definerer den dataansvarlige (den registeransvarlige) 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 personoplysninger [...]”

Direktivets art. 2, litra e, definerer databehandleren (registerføreren) som:

”den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, **der behandler personoplysninger på den registeransvarliges vegne**”

Disse to begreber hænger derfor nøje sammen, dels da de to definitioner udelukker hinanden, og dels da eksistensen af en databehandler afhænger af eksistensen af en dataansvarlig (”på vegne af den [dataansvarlige]”). I det omfang, man kan definere en person som den dataansvarlige, kan man dermed samtidigt udelukke, at personen er databehandler.²⁶ Dette følger primært af formålet med begreberne og den kontekst, de indgår i, se afsnit 3.3.

Efter ordlyden skal man ved definitionen af den dataansvarlige lægge vægt på, om personen fastlægger formålet med behandlingen og bestemmer hvilke hjælpemidler, der skal bruges. Men hvad menes der med formål og hjælpemidler?

Om definitionen af den dataansvarlige skriver forfatterne i KPDL, at den dataansvarlige er den der ”har det *umiddelbare ansvar for behandlingen*, og som i det daglige har *dispositionsretten* over de oplysninger, der indgår i behandlingen”²⁷. Forfatterne lægger altså vægt på ansvaret for behandlingen og dispositionsretten. Dette uddybes ved kommentaren til begrebet databehandler, således at ”det er den dataansvarlige og ikke databehandlere, der **er direkte ansvarlig over for den registrerede**, jf. herved bl.a. reglen om **erstatningsansvar i § 69**”²⁸. Databehandleren, der ”modtager

²⁶ Man kan dog være dataansvarlig i ét forhold, og databehandler i et andet, men ordlyden af de to definitioner må udelukke, man er begge dele for den nøjagtig samme behandling.

²⁷ Se KPDL s. 163

²⁸ Se KPDL s. 165

oplysningerne... [kan ikke selv] **disponere over oplysningerne til egne formål eller i øvrigt uden den dataansvarliges accept**²⁹.

Med ”ansvar for behandlingen” skal der altså forstås bl.a. det direkte erstatningsansvar over for den registrerede. Med ”dispositionsretten” skal der forstås, hvem der fastlægger formålet med behandlingen og i øvrigt bestemmer over behandlingen, og at databehandleren ikke kan fastlægge et andet formål uden den dataansvarliges accept.

For så vidt angår betragtningen om det umiddelbare ansvar for behandlingen, giver dette intet nyt bidrag til fortolkningen af begreberne. Erstatningsansvar over den registrerede i PDL § 69 er en følge af dataansvaret, men dette hjælper ikke med at skille de dataansvarlige fra databehandlerne. Skal man således vurdere erstatningsansvaret efter § 69, må det kræve, at man først fastlægger, om den omhandlede person er dataansvarlig eller databehandler. Når det er sagt, skal det selvfølgelig anerkendes, at erstatningsansvaret efter § 69 er et aspekt af dataansvaret.

Betragtningen om dispositionsretten er uden tvivl rigtig, men er på den anden side blot en omformulering af ordlydens bestemmelse om, at det er den dataansvarlige, der bestemmer formålet og hjælpemidlerne, og bidrager dermed ikke nævneværdigt til fortolkningen.

Datatilsynet har en kortfattet guide på deres hjemmeside for vurderingen:³⁰

”Af definitionen følger det, at den dataansvarlige er den, der afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. Det afgørende er således, hvem der juridisk og/eller faktisk afgør, hvordan personoplysninger skal behandles (hvem har ”ejerskabet” til oplysningerne)”.

Derefter giver Datatilsynet et eksempel med en offentlig myndighed, der foretager en lovbestemt behandling, og et andet eksempel med en privat arbejdsgiver, der behandler oplysninger om sine ansatte. I begge tilfælde bestemmer personen formålet med behandlingen, og hvilke hjælpemidler, der skal anvendes og er således dataansvarlige. Dette er dog også et meget sparsomt bidrag til forståelsen.

Mere dækkende er Artikel 29-gruppens vejledning³¹ om emnet. Artikel 29-gruppen er alene rådgivende, jf. PDD art. 29, stk. 1, og deres udtalelse er derfor ikke retligt bindende. I kraft af den autoritet gruppen har fået efter direktivets art. 29 som rådgivende, er det dog rimeligt at inddrage deres vejledning i fortolkningen. Desuden er gruppen sammensat af repræsentanter fra alle datatilsynene i de forskellige medlemsstater, repræsentanter fra EU’s persondataretlige organer samt en repræsentant fra Kommissionen, hvorfor gruppens holdning naturligvis kan tillægges stor betydning ved fortolkningen.

Artikel 29-gruppens vejledning opdeler fortolkningen af den dataansvarlige. I forhold til, hvem der afgør formålet med behandlingen, og hvilke hjælpemidler, der skal bruges, deler vejledningen fortolkningen op i en fortolkning af ”afgør” og en fortolkning af ”formål og hjælpemidler”.³²

²⁹ Se KPDL s. 165

³⁰ <https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/>

³¹ Udtalelse 1/2010 om begreberne ”registeransvarlig” og ”registerfører”, vedtaget den 16. februar 2010 af Artikel 29-gruppen vedrørende databeskyttelse, benævnt WP 169.

³² WP 169, s. 7-8.

Vejledningen sidestiller ”afgør” med ”faktisk kontrol”³³ eller ”faktisk indflydelse” over formål og hjælpemidler.³⁴ Vejledningen opstiller tre kategorier af situationer, hvor en person har en sådan kontrol:³⁵

1. **Kontrol, der er baseret på eksplicit juridisk kompetence.** Man har en sådan kontrol, hvis man er forpligtet til at foretage en behandling ved lov. Man kan fx være forpligtet til at behandle personoplysninger efter hvidvaskningsloven. Kontrollen kan også følge af, at man er direkte udpeget til at være dataansvarlig ved lov³⁶.
2. **Kontrol, der er baseret på implicit kompetence.** Man kan således have en implicit kontrol, der hviler på bredere betragtning fra et retsområde. Det bedste eksempel er ledelsesretten, der implicit giver arbejdsgiveren kontrol over behandlingerne af de ansattes personoplysninger.
3. **Kontrol, der er baseret på faktisk indflydelse.** Man kan efter de faktiske omstændigheder have kontrollen over formålet og hjælpemidlerne. Ofte vil man kunne se i kontrakten, hvem af to parter har kontrollen (eller om der eventuelt er fælles kontrol). Det afgørende er dog ikke kontraktens ordlyd, men hvem der faktisk i det daglige udøver kontrollen. Dette betyder også, at en person kan anses for dataansvarlig, hvis han bryder kontrakten og faktisk udøver en kontrol, der er i strid med kontraktens bestemmelser (eller endog i strid med gældende ret).

Mens kategori 1 og 2 er nemme at håndtere, kan det ofte være svært at vurdere, om der foreligger en kontrol efter kategori 3, da dette beror på en nærfortolkning af de præcise faktiske omstændigheder. Har ingen af parterne selvstændig kontrol, men derimod fælles kontrol, er parterne fælles dataansvarlige for behandlingen.

Formål og hjælpemidler sidestiller vejledningen med behandlingens ”hvorfor” og ”hvordan”.³⁷ Vejledningen medgiver, at databehandleren altid i et eller andet omfang kan have en indflydelse på ”hvordan”. Det er således normalt for en part at bestemme nogle helt grundlæggende hjælpemidler for behandlingen: Hvilken computer skal behandlingen ske på, på hvilken server skal oplysningerne gemmes, hvor hyppigt skal der tages backup, hvor skal backuppen være osv. Vejledningen skelner derfor mellem de *væsentlige* hjælpemidler og de *uvæsentlige* hjælpemidler. Mens eksempler på uvæsentlige hjælpemidler er nævnt ovenfor, kan væsentlige hjælpemidler være: Hvilke oplysninger skal behandles, hvilke tredjemænd skal have adgang til oplysningerne, hvornår skal oplysninger slettes osv.³⁸ Grænsen mellem væsentlige og uvæsentlige hjælpemidler må anses for at være flydende. Vejledningen peger dog på *lovligheden* som det afgørende moment for grænsedragningen:³⁹

”Væsentlige spørgsmål, som er afgørende for lovligheden af en behandling, er forbeholdt for den [dataansvarlige].”

³³ På engelsk hedder den dataansvarlige da også ”controller”.

³⁴ WP 169, s. 8-9.

³⁵ WP 169, s. 10-11.

³⁶ Se også sidste del af afsnit 3.1., om begreberne som selvstændige EU-retlige begreber.

³⁷ WP 169, s. 13.

³⁸ WP 169 s. 14.

³⁹ WP 169, s. 15.

Spørgsmål som fx hvilken konkret computer på arbejdspladsen, der skal bruges til behandlingen, har ikke indflydelse på lovligheden af behandlingen,⁴⁰ hvorfor dette ikke er et spørgsmål om et væsentligt hjælpemiddel, der skal afgøres af den dataansvarlige.

I vejledningen skriver Artikel 29-gruppen om formål og hjælpemidler:

”På den baggrund er fastlæggelsen af hjælpemidlerne kun et tegn på kontrol, når fastlæggelsen vedrører de væsentlige elementer ved hjælpemidlerne, mens fastlæggelsen af formålet med behandlingen under alle omstændigheder udløser kvalificeringen som en registeransvarlig”.

Hermed synes vejledningen at lægge op til, at man er dataansvarlig når man fastlægger formålet **eller** de væsentlige hjælpemidler. Efter ordlyden skal den dataansvarlige dog fastlægge formålet **og** hjælpemidlerne. Synspunktet er behandlet af Brendan Van Alsenoy i en artikel fra 2012.⁴¹ Forfatteren mener, det er uklart, hvad Artikel 29-gruppen overhovedet mener.⁴² Fx påpeger vejledningen, at man altid i et eller andet omfang afgør hjælpemidlerne, når man indleder et samarbejde med en anden person om behandling af personoplysninger. Selv hvis samarbejdspartneren har en fast og kendt måde, han behandler oplysninger på, og han ikke vil ændre denne, har man alene ved *antagelsen* af samarbejdspartneren valgt, hvilke hjælpemidler, der skal anvendes.⁴³ Dette gør dog ikke vejledningens synspunkt uklart i forhold til ovenstående citat, da vejledningen blot gør opmærksom på, at den udfarende part, der antager en samarbejdspartner med standardiserede og kendte vilkår for behandlingen, fastlægger behandlingens hjælpemidler. Dette betyder ikke, at vejledningen mener, at det lige pludselig altid er *påkrævet*, at man skal fastlægge både formålet og hjælpemidlerne for at blive anset som dataansvarlig.⁴⁴

Dernæst påpeger forfatteren, at Artikel 29-gruppen i tidligere udtalelser har gjort det modsatte synspunkt gældende, fx i udtalelsen om SWIFT⁴⁵ og om sociale netværk⁴⁶. Med hensyn til SWIFT-sagen gentager Artikel 29-gruppen kun bestemmelsens ordlyd⁴⁷ og konstaterer, at SWIFT afgør både formål og hjælpemidler. Artikel 29-gruppen havde derfor ikke anledning til at overveje, om SWIFT også ville være dataansvarlig, hvis SWIFT kun havde kontrol over enten formål eller hjælpemidler. Med hensyn til udtalelsen om sociale netværk skriver Artikel 29-gruppen kun yderst kort, at sociale netværk (så som Facebook eller Twitter) er dataansvarlige, da de fastlægger formål og hjælpemidler,⁴⁸ men igen ikke har anledning til at behandle spørgsmålet, om mindre kontrol også vil kunne medføre dataansvar. Forfatterens synspunkter må derfor afvises, og det må fasthol-

⁴⁰ Brug af forældet teknologi kan dog udøge en sikkerhedsfare, hvorfor det alligevel kan have betydning for lovligheden, hvis man vælger gammelt og usikkert udstyr til behandlingen. En sådan beslutning må være en beslutning om et væsentligt hjælpemiddel.

⁴¹ "Allocating responsibility among controllers, processors, and everything in between - the definition of actors and roles in directive 95-46 EC", "Computer Law and Security review", 2012, s. 25-43, af Brendan Van Alsenoy

⁴² "Allocating responsibility among controllers, processors, and everything in between - the definition of actors and roles in directive 95-46 EC", s. 31.

⁴³ WP 169, s. 26, note 18.

⁴⁴ Dette synspunkt fra vejledningen vil blive uddybet under afsnit 3.6.

⁴⁵ Udtalelse 10/2006 om behandling af personoplysninger i Society for Worldwide Interbank Financial Telecommunication (SWIFT), vedtaget den 22. november 2006, benævnt WP 128.

⁴⁶ Udtalelse nr. 5/2009 om internetbaserede sociale netværksaktiviteter, vedtaget den 12. juni 2009 af Artikel 29-gruppen, benævnt WP 163.

⁴⁷ Se WP 128, s. 10.

⁴⁸ WP 163, s. 5.

des, at kontrol over formål **eller** de væsentlige hjælpemidler er nok til at gøre en person dataansvarlig. Dette synspunkt er også bedst i tråd med EU-domstolens udtalelse i C-131/12 Google Spain, hvorefter begrebet dataansvarlig skal fortolkes udvidende for at sikre en effektiv og fuldstændig beskyttelse af de registrerede.⁴⁹ Synspunkt fremgår også (indirekte) af ICO's vejledning:⁵⁰

“A car hire company contracts a vehicle-tracking company to install devices in its cars and monitor them so that cars can be recovered if they go missing. They specify that the tracking company should track all the company's cars and send back the location data to the hire company six hours after the end of the hire period, if the car has not been returned.

However, despite these instructions, the vehicle-tracking company is a data controller in its own right. This is because it has sufficient freedom to use its expertise to decide which information to collect about cars (and their drivers) and how to analyse this. It is entirely in control of its own data collection – the operation of the vehicle-tracking software is a trade secret and the hire company does not even know what information is collected. **Although the hire company determines the overall purpose of the tracking (the recovery of its cars), the fact that the tracking company has such a degree of freedom to decide which information to collect and how, means it is a data controller in its own right.**”

Det er dog vigtigt ikke at stirre sig fuldstændig blind på behandlingens formål og hjælpemidler. Formålet med ordningen er, at databehandleren skal have mindre ansvar, fordi han ikke kan agere selvstændigt, mens den dataansvarlige skal være ansvarlig for databehandlerens handlinger, hvis han instruerer databehandleren. Behandlingens formål og hjælpemidler er gode pejlemærker for denne vurdering, men hvis modellen ikke giver mening i den konkrete situation, bør man falde tilbage på formålet med ordningen om ansvarsfordeling. Det afgørende for vurderingen må være vedkommendes selvstændighed og handlefrihed med udførelsen af opgaven. Har han selvstændighed, er han dataansvarlig. Er han underlagt kontrol, er han databehandler.

3.4.1. Konklusion

Efter ordlyden er en person dataansvarlig, når personen afgør formålet med en behandling, og afgør hvilke hjælpemidler, der skal anvendes. Hverken Datatilsynet eller dansk retslitteratur hjælper med at uddybe dette synspunkt.

I en vejledning har Artikel 29-gruppen behandlet, hvad der skal forstås ved ”afgør” og ”formål og hjælpemidler”. ”Afgør” kan sidestilles med indflydelse eller kontrol, der kan opstå i tre typetilfælde:

- 1. Kontrol, der er baseret på eksplicit juridisk kompetence**
- 2. Kontrol, der er baseret på implicit kompetence**
- 3. Kontrol, der er baseret på faktisk indflydelse**

Formål skal forstås som behandlingens hvorfor, og hjælpemidler skal forstås som behandlingens hvordan. Hjælpemidler kan deles op i væsentlige og uvæsentlige hjælpemidler.

⁴⁹ Forfatteren er dog lovligt undskyldt for ikke at inddrage C-131/12 Google Spain, da dommen blev afsagt efter forfatterens artikel blev bragt.

⁵⁰ Vejledningens s. 14.

”Formål og hjælpemidler” skal forstås som ”formål **eller** (væsentlige) hjælpemidler”, således at man kan anses som dataansvarlig, hvis man har kontrol over bare én af delene. Brendan Van Alsenoy konkluderer i en artikel, at det i de fleste tilfælde stadig vil være en analyse af, hvem der bestemmer formål **og** hjælpemidler, der er afgørende for dataansvaret. Dette bygges på, at Artikel 29-gruppen har antaget dette, dels et sted i selve vejledningen, dels i nogle ældre udtalelser. Dette synspunkt må dog anses for at være forkert. Modellen med kontrol over formål og hjælpemidler kan dog tænkes at passe dårligt på flere situationer i det praktiske liv; her kan man anlægge en formålsfortolkning, baseret på partens selvstændighed og handlefrihed med udførelsen af opgaven.

3.5. Nærmere om formålet med behandlingen

Som det blev redegjort for ovenfor, sidestiller Artikel 29-gruppen formålet med behandlingens ”hvorfor”. Artikel 29-gruppens vejledning om problemstillingen uddyber ikke (eksplicit) dette synspunkt nærmere. Vejledningen henviser dog til en ordbogsdefinition af ordet:⁵¹

”Et forventet resultat, der er tilsigtet, eller som er styrende for planlagte handlinger”.

Umiddelbart forekommer det måske enkelt. Hvis man giver personoplysninger til en advokat, er formålet, at advokaten skal fastslå, om man har et retskrav. Giver man personoplysninger til en læge, kan formålet være, at lægen skal fastslå, om man lider af en bestemt sygdom. I dette tilfælde er det klienten og patienten, der har bestemt formålet, det tilsigtede resultat, eller det mål som er styrende for lægens og advokatens behandling af oplysninger. Spørgsmålet er dog, om dette synspunkt kan nuanceres.⁵² Det må dog fastslås som det første, at formål ikke skal forstås som ”i hvis interesse behandlingen sker”. Denne forståelse er i strid med den sproglige forståelse af ordet ”formål” og en sådan fortolkning vil indskrænke ordlyden, der ellers skal fortolkes udvidende på baggrund af C-131/12, Google Spain.

Om advokater udtaler ICO:⁵³

”The solicitors process this personal data for the **broad purpose of providing legal service in accordance with their professional obligations**”.

Her ser ICO formålet ud fra advokatens synsvinkel: Advokaten behandler generelt personoplysninger ud fra sit eget formål om at udbyde juridisk rådgivning i overensstemmelse med sine professionelle pligter.

Man kan derfor overveje, om man skal anlægge *en differentieret formålsbetragtning*. De forskellige parter kan have forskellige formål med deres behandlinger. Klienten, der videregiver oplysninger til advokaten, kan have det formål med en videregivelse, at advokaten skal fastslå, om han har et retskrav mod en handelspartner. Advokatens behandlinger af oplysningerne – den juridiske vurdering – har derimod det formål at fungere som led i advokatens udbud af juridisk rådgivning i overensstemmelse med sine juridiske og etiske forpligtelser.

Dette synspunkt bygger formentlig på, at advokaten har en vis selvstændighed i forhold til opgavens udførelse, der hviler på advokatens ekspertise og de særlige etiske og juridiske krav til den

⁵¹ WP 169, s. 13.

⁵² Her ses der bort fra de klare tilfælde, hvor en læge fx behandler personoplysninger for at markedsføre sin egen lægepraksis, hvor formålet med behandlingen utvivlsomt er markedsføring, og formålet er fastlagt af lægen.

⁵³ ”Data controllers and data processors: what the difference is and what the governance implications are”, vejledning udstedt af Information Commissioner’s office (ICO, britisk datatilsyn), 20140506, s. 13.

professionelle udøvelse. Hvis selvstændigheden er tilstrækkelig stærk, gennembryder advokatens formål klientens eget formål (*formålsgennembrud*).

I det hele taget kan det siges, at advokatens behandling må have et meget bredere formål end klienten, hvorfor de umuligt kan have det samme formål med behandlingen. Mens klienten kan have et snævert ønske om at få fastlagt, om han har et retskrav mod en handelspartner, skal en agtsom advokat vurdere retsstillingen generelt: Har klientens modpart et eventuelt modkrav? Kan klientens krav bevises under en retssag? Er klientens eventuelle retskrav forældet? Hvordan kan klientens retskrav gennemføres, og vil det give retsøkonomisk mening at gennemføre kravet? Skal klienten rådes til at indgå forlig? Det må være forventeligt, at advokaten også vurderer sådanne forhold qua sin selvstændighed med opgavens udførelse og de høje etiske og juridiske krav til professionen, hvormed formålet med behandlingen bliver meget bredere end klientens formål.⁵⁴

Denne fortolkning bekræftes til dels af Artikel 29-gruppens vejledning, der udtaler, at revisorer og advokater, der leverer ydelser til befolkningen og småhandlende ud fra generelle instrukser (fx ”udarbejd min selvangivelse”), må anses for at være dataansvarlige.⁵⁵⁵⁶ Dette må bero på deres selvstændighed med udførelsen af opgaven, som netop er stor, når man kun er underlagt generelle instrukser.

Synspunktet om formålsgennembrud beror i sidste ende på en almindelig sproglig forståelse af ordlyden og en formålsfortolkning. Lovgiver har ikke givet faste retningslinjer for forståelsen af formålet med behandlingen, hvorfor der uundgåeligt er et usikkerhedsmoment. Det kan dog i det mindste siges, at denne fortolkning er i overensstemmelse med EU-domstolens udtalelse i C-131/12 Google Spain, hvorefter ”dataansvarlig” skal fortolkes udvidende for at sikre en effektiv og fuldstændig beskyttelse af de registrerede. Fortolkningen er også i overensstemmelse med ICO’s holdning, omend ICO ikke har formuleret holdningen eksplicit som et generelt princip, men kun kasuistisk med eksempler i vejledningen om dataansvarlig/databehandler-problematikken.⁵⁷ Holdningen kan til dels også ses i det nævnte eksempel fra Artikel 29-gruppens vejledning.⁵⁸

3.5.1. Konklusion

Formålet med behandlingen er ikke endeligt defineret i PDD, men skal formentlig forstås bredt, således at en modtager af oplysninger kan have et andet formål end afsenderen, selvom modtageren behandler oplysningerne i afsenderens interesse. Dette beror i høj grad på modtagerens selvstændighed med opgavens udførelse. Har modtageren en stor grad af selvstændighed, vil hans formål gennembryde afsenderens formål, selvom han handler i afsenderens interesse.

3.6. Nærmere om kontrol

Det kan være svært at definere, hvornår en part har kontrol over behandlingens formål eller hjælpemidler. Forholdet mellem to personer vil altid på en eller anden måde hvile på en aftale, hvor parterne skal blive enige, og hvor ingen part kan diktere aftalens indhold, herunder behandlingens

⁵⁴ Pædagogisk kan forholdet sammenlignes med en mekaniker på et bilværksted. Kunden kan have sendt bilen på værksted for at få motoren repareret, men hvis mekanikeren ser, at bilens bremses ikke fungerer, må mekanikeren have en pligt til at gøre opmærksom på dette.

⁵⁵ WP 169, s. 30, eksempel 23.

⁵⁶ Særligt vedrørende advokater, se afsnit 4, hvor disse betragtninger uddybes.

⁵⁷ ”Data controllers and data processors: what the difference is and what the governance implications are”.

⁵⁸ WP 169, s. 30, eksempel 23.

formål eller hjælpemidler, uden den anden parts accept. Med andre ord kan det være svært at forestille sig en kontrollerende part i et miljø med aftalefrihed. For så vidt angår tjenesteydelser, der omfatter behandling af personoplysninger, kan der dog opstilles nogle situationer, hvor det kan siges, at den ene part har kontrollen over behandlingen.

Udbyderen af tjenesteydelsen vil ofte have standardiserede og detaljerede vilkår for behandlingen af personoplysninger, som han måske endda ikke er villig til konkret at ændre på. Herefter kan det forestilles, at tjenesteudbyderen suverænt er den, der bestemmer over behandlingen, siden det er ham, der har fastsat vilkårene for behandlingen. Det er imidlertid op til køberen af tjenesteydelsen, om han i det hele taget vil antage tjenesteudbyderen, hvorfor det reelt er køberen, der bestemmer vilkårene. Dette antages af Artikel 29-gruppen:⁵⁹

”Det forhold, at kontrakten og de detaljerede forretningsbetingelse heri udarbejdes af tjenesteudbyderen og ikke af den registeransvarlige, er dog ikke i sig selv et tilstrækkeligt grundlag til at konkludere, at tjenesteudbyderen skal anses for at være en registeransvarlig, for så vidt den registeransvarlige utvunget har accepteret kontraktbestemmelserne og således påtager sig det fulde ansvar for dem”.

Artikel 29-gruppen bruger som eksempel en virksomhed, der skal bruge en e-mail-platform til sine ansatte. E-mail-platformen har fastlagt, hvor lang tid, e-mails gemmes, hvilket ikke er til forhandling. Da virksomheden frit kan vælge en anden udbyder, må virksomheden anses for dataansvarlig, såfremt han vælger den pågældende e-mail-platform.⁶⁰

Dette må selvfølgelig forudsætte, at der er tale om kendelige vilkår i en kontrakt, eller at tjenesteudbyderens måde at behandle personoplysninger på er kendelige på anden vis. Hvis køberen af ydelsen i øvrigt selv har udfærdiget kontrakten og vilkårene for behandlingen, må han anses for at være den dataansvarlige og tjenesteudbyderen som databehandler.

Derudover kan kontraktens ordlyd betyde, at en af parterne er databehandler, og den anden er dataansvarlig. Det kan således i kontrakten være bestemt, at den ene part skal adlyde den anden parts instrukser vedr. behandlingen. Dette kunne fx være en virksomhed, der antager et markedsføringsbureau til at foretage en spørgeskemaundersøgelse, som virksomheden selv har udfærdiget, og hvor virksomheden selv har planlagt, hvem der skal spørges osv. Bureauet parerer blot ordrer og er dermed en databehandler.⁶¹ Bureauet kan naturligvis komme med forslag, men de bliver kun udført, såfremt den dataansvarlige accepterer dem. Det kan også følge af selve kontraktforholdet, at den ene part skal gøre, hvad den anden bestemmer, uden at parterne har nedskrevet det eksplicit i kontrakten.

Køber virksomheden derimod en tjenesteydelse, hvor det er meningen med ydelsen, at den skal udføres og planlægges uafhængigt af køberen, vil de to parter derimod være selvstændige dataansvarlige for hver deres behandling. Et eksempel kunne igen være en virksomhed og et markedsføringsbureau, hvor virksomheden ønsker forbrugernes vaner undersøgt, men pga. manglende indsigt i markedsføring, lader markedsføringsbureauet bestemme, hvem der skal spørges og hvilke spørgsmål, der skal stilles osv. Virksomheden er herefter dataansvarlig for de behandlinger, den

⁵⁹ WP 169, s. 26-27.

⁶⁰ Se WP, s. 27, eksempel 18.

⁶¹ Se WP 169, s. 13, eksempel 2.

foretager (fx videresende råmateriale om deres kunder til bureauet), mens bureauet er dataansvarlig for sine behandlinger. Situationen adskiller sig fra ovenstående, hvor virksomheden antager et lønudbetalingsfirma og accepterer dets standardvilkår ved, at vilkårene for behandlingen ikke er bestemt på forhånd og kendelige for virksomheden, og en del af ydelsen fra bureauets side består i at planlægge behandlingen, hvormed bureauet har kontrol over behandlingen. Havde bureauet indrettet spørgeskemaundersøgelsen på en anden måde, måtte virksomheden acceptere dette, mens virksomheden kunne vælge et andet lønudbetalingsfirma, såfremt det ikke kan acceptere dets på forhånd kendelige standardvilkår.

Dernæst kan det siges, at kontrol over en behandling må forudsætte kendskab til behandlingen. Hvis en oprindelig databehandler på egen hånd udfører en behandling til et nyt formål eller tager et nyt væsentligt hjælpemiddel i brug, må databehandleren for denne behandling blive dataansvarlig. Dette kan dog modificeres, hvis den dataansvarlige bevidst har holdt sig i uvidende om behandlingen, hvorefter han må have accepteret den. Dette følger nu også af PDF art. 28, stk. 10.

Når to virksomheder indgår et samarbejde, hvor de sammen udbyder en tjenesteydelse til forbrugere, og samarbejdsaftalen har været udtryk for reelle forhandlinger, kan det siges, at der er etableret fælles kontrol over behandlingen, der hører sammen med tjenesteydelsen.

3.7.Hvad er man dataansvarlig for?

Som det blev redegjort for tidligere, kan man kun være databehandler i det omfang, man ikke er dataansvarlig. Efter man har vurderet, hvem der afgør formål eller hjælpemidler, er det derfor nødvendigt at fastslå, **hvad** man er dataansvarlig for. Man kan således have et samarbejde med en partner, hvor man er dataansvarlig for nogle ting, men databehandler for andre.

I registerlovenes tid var man ansvarlig for *et register*. Registerlovgivningsudvalget mente, at det var bedst ved implementeringen af PDD at omdøbe direktivets ”registeransvarlig” til ”dataansvarlig”. Udvalget begrunder ikke dette nærmere, men må vel bero på, at udvalget ønskede at præcisere, at man ikke længere var ansvarlig for et register, men for (person)*data*.⁶² Efter ordlyden af PDD (og PDL), er den dataansvarlige den, der bestemmer formålet og hjælpemidlerne i forhold til *behandlingen*. I det hele taget må de persondataretlige regler anses for at være en regulering af *behandlinger* af personoplysninger, og ikke en regulering af personoplysninger i sig selv.⁶³ Denne pointe understreges også af Artikel 29-gruppen i vejledningen om den dataansvarlige og databehandleren, hvor de peger på den udvikling, der er sket fra Europarådets konvention 108 til PDD:

”For det første blev ”den registeransvarlige for filen” i konvention 108 erstattet med ”den registeransvarlige” ved ”behandling af personoplysninger” [...] **Begrebet ”den registeransvarlige” blev således ikke længere anvendt for et statisk objekt (”filen”), men henviste til aktiviteter, der afspejlede oplysningers livscyklus fra deres indsamling til deres tilintetgørelse [behandlinger]”.**

Mere pædagogisk havde det derfor været, hvis Registerlovgivningsudvalget havde omdøbt den registeransvarlige til den *behandlingsansvarlige*, da det er behandlingen af personoplysninger,

⁶² Betænkning nr. 1342/1997, s. 210. Udvalget gjorde dog klart opmærksom på, at omdøbningen ikke skulle have nogen retlige konsekvenser.

⁶³ Se fx PDD art. 3, stk. 1: ”Dette direktivs bestemmelser anvendes på *behandling* af personoplysninger [...]”

man som dataansvarlig er ansvarlig for.⁶⁴ Dette kan yderligere præciseres: *Man er dataansvarlig for lovligheden af behandlingen.*

”Behandling” defineres i PDD art. 2, litra b, som:

”enhver operation eller **række af operationer** [...] som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring samt blokering, slettelse eller tilintetgørelse”.

En behandling er derfor en hvilken som helst form for operation som oplysninger er genstande for. En behandling kan dog defineres som *en række af operationer*, i det omfang operationerne hænger sammen. Man er derfor dataansvarlig for en række af operationer, eller enkelte, isolerede operationer. Denne anskuelse har Artikel 29-gruppen også i sin vejledning, hvor den i flere eksempler anskuer behandlingen på *makro-niveau*⁶⁵, og således tildeler dataansvar for en række af operationer, og ikke dataansvar for hver enkelt behandling. Dette må dog forudsætte, at der er noget, der binder operationerne sammen. Det vil være meget nærliggende, at lade formålet (på makroniveau) være det, der binder operationerne sammen, da operationer med forskellige formål næppe kan siges at hænge sammen. PDD nævner da også flere steder *formålet* med behandlingen.⁶⁶

Der er flere grunde til at anskue det på denne måde. For det første tilsiger hensynet til gennemsigtighed, at det skal være så enkelt som muligt for både erhvervslivet og de registrerede at identificere den dataansvarlige – dette er umuligt at opnå, hvis man skal vurdere spørgsmålet om ansvar for hver eneste operation. For det andet, og i tæt sammenhæng med hensynet til gennemsigtighed, vil det i praksis være en uoverkommelig opgave at vurdere ansvaret for hver eneste operation. Derfor er man dataansvarlig for rækker af operationer, der har samme formål, eller enkelte, isolerede behandlinger med deres eget formål.

Udgangspunktet må derfor klart være, at man er ansvarlig for lovligheden af en behandling på makro-niveau, når man bestemmer behandlingens formål eller hjælpemidler. Kan ansvaret imidlertid i visse situationer opdeles yderligere? I Artikel 29-gruppens vejledning, åbnes der op for denne mulighed:

”En person eller enhed, som f.eks. afgør, hvor længe oplysninger skal gemmes, eller hvem der skal have adgang til de behandlede oplysninger, **handler som den [dataansvarlige] med hensyn til denne del af oplysningernes anvendelse** og skal derfor opfylde alle den [dataansvarliges] forpligtelser”.

Den person, der fx fastlægger, hvor længe oplysninger skal gemmes, er således dataansvarlig for lovligheden af denne del af behandlingen.⁶⁷ Dette hænger sammen med, at lovligheden af behandlingen kan deles op i flere dele. En behandling af personoplysninger kan være ulovlig, hvis den har et usagligt formål. Den person, der har fastlagt formålet er derfor ansvarlig i tilfælde af, at formålet skulle være usagligt. Behandlingen kan imidlertid også være ulovlig, hvis man har brugt

⁶⁴ Denne definition har man da også valgt i den norske persondatalov.

⁶⁵ WP 169, s. 20.

⁶⁶ Fx PDD, art. 6, stk. 1, litra b, litra c og litra d.

⁶⁷ Efterfølgende opbevaring af oplysninger vil dog ofte have sit eget selvstændige formål, der er forskelligt fra formålet med den tidligere behandling., hvorefter opbevaringen er en selvstændig behandling.

et ulovligt hjælpemiddel (fx have inddraget behandlingen af en bestemt (følsom) personoplysning uden at sørge for et gyldigt behandlingsgrundlag). Den person, der har fastlagt et ulovligt hjælpemiddel er dermed dataansvarlig for lovligheden af dette aspekt af behandlingen. Databehandleren, der rent faktisk udfører behandlingen, men ikke har fastlagt hverken formål eller hjælpemidler, er ikke dataansvarlig for lovligheden af behandlingen.

Når det først er blevet afgjort, om man er dataansvarlig, og hvad man er dataansvarlig for, kan det herefter siges, at man har alle de pligter, der fremgår af PDL, for det pågældende forhold, og man kan blive erstatnings- eller strafferetligt ansvarlig for manglende opfyldelse af disse pligter.

3.7.1. Konklusion

Man er dataansvarlig for lovligheden af en behandling. Behandlingen skal som udgangspunkt ses på makro-niveau som en række af operationer med et eller flere fælles mål, hvor dataansvaret fastlægges efter, hvem der har fastlagt formålet og/eller hjælpemidlerne. I det omfang, en operation stikker ud, kan man dog fastlægge et isoleret dataansvar, alt efter hvem der fastlagde formålet eller hjælpemidlerne, så længe databeskyttelsen er effektiv, og der er en høj grad af gennemsigtighed.

3.8. Kan den registrerede være dataansvarlig?

Spørgsmålet er, om den registrerede kan være dataansvarlig for behandling af oplysninger om vedkommende selv. Dette kan have betydning for den person, der modtager oplysningerne direkte fra den registrerede. Personen, der behandler oplysningerne, kan kun være databehandler, hvis der er en dataansvarlig, da en databehandler behandler oplysninger på vegne af den dataansvarlige.

Hvis man kigger isoleret på de to afgørende momenter - bestemmer vedkommende over formålet eller hjælpemidlerne for behandlingen - må en registreret kunne anses for også at være en dataansvarlig. En person kan således udlevere oplysninger om sig selv og instruere modtageren om behandlingens formål og hjælpemidler, hvorefter den registrerede er dataansvarlig, og modtageren er databehandler.

Spørgsmålet er blevet behandlet kort af Peter Blume i U.2013B.325:⁶⁸

”De oplysninger på en åben profil [på et social medie], der vedrører den person, som har oprettet profilen, har ikke interesse i denne sammenhæng, fordi det ikke giver mening at antage, at en person kan være dataansvarlig i forhold til sig selv.”

Peter Blume besvarer altså spørgsmålet benægtende, men har ikke nogen uddybende argumentation. Blume har dog en klar pointe i, at der er en stor fare for, at hele meningen med ordningen bryder sammen, hvis man kan være registreret og dataansvarlig på samme tid. Det må antages, at PDD forudsætter, at den registrerede og den dataansvarlige er to forskellige personer. Desuden er den dataansvarlige ansvarlig for behandlingens lovlighed. En registreret, der behandler oplysninger om sig selv, eller har instrueret en databehandler i at behandle oplysningerne, kan hverken blive straffet for evt. ulovlige behandlinger⁶⁹ disse oplysninger som både gerningsmand og offer, og han kan ikke ifalde et erstatningsansvar over for sig selv. I det omfang en person overlader

⁶⁸ U.2013B.325, ”Personen som dataansvarlig”, s. 326.

⁶⁹ Det kan i det hele taget diskuteres, om en behandling kan være ulovlig i denne sammenhæng.

oplysninger om sig selv til en anden med henblik på behandling, kan personen ikke være dataansvarlig, og modtageren kan ikke være databehandler.⁷⁰

3.8.1. Konklusion

En registreret kan ikke være dataansvarlig for behandlinger af personoplysninger om vedkommende selv. Som følge heraf kan modtageren af personoplysninger, han får af den registrerede, der omhandler den registrerede, ikke være databehandler.

3.9. Hvilke personer er dataansvarlige og databehandlere?

Både definitionen af den dataansvarlige og databehandleren begynder med:

”den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ”.

Hermed fastslår ordlyden, at alle kan være dataansvarlige og databehandlere, både fysiske og juridiske personer, hvad enten de er offentlige eller private. Ordlyden definerer ikke nærmere, hvad der skal forstås med juridiske personer. Sprogligt må ordlyden dog i hvert fald kunne rumme juridiske personer med fuld rets- og partsevne⁷¹, såsom aktieselskaber, anpartsselskaber, konkursboer, fonde og foreninger. Der er ingen fortolkningsmomenter, der peger imod at udskille fx interessentskaber og partnerselskaber (kommanditaktieselskaber), selvom disse ikke er selvstændige skattesubjekter. Det kan tværtimod mindske gennemsigtigheden for den registrerede, hvis det er en ukendt interessent, der er dataansvarlig i stedet for interessentskabet.

Juridiske personer kan dog i sidste ende ikke behandle personoplysninger – det kan kun fysiske personer. Det er således altid en fysisk person, der foretager den konkrete behandling.⁷² Dette giver anledning til at undersøge, hvordan ansvaret skal fordeles mellem den juridiske person og den fysiske person, der er ansat hos den juridiske person. Artikel 29-gruppen har udtalt sig om problemet.⁷³

”Med henblik på en strategisk tildeling af ansvar og for at give de registrerede en mere stabil og pålidelig referenceenhed i forbindelse med udøvelsen af deres rettigheder i henhold til direktivet, bør det foretrækkes at anse selve virksomheden eller organet for at være den registeransvarlige [dataansvarlige] snarere end en bestemt person i virksomheden eller organet”.

Artikel 29-gruppen mener dermed, at den juridiske person i videst muligt omfang skal betragtes som den dataansvarlige for at sikre en stabil og pålidelig referenceramme for den registrerede. Dette er i fuld overensstemmelse med formålet med ordningen, der skal sikre en effektiv og fuldstændig beskyttelse af den registrerede.

Når selskabet er den dataansvarlige, kunne dette give anledning for nogle til at tro, at de ansatte er databehandlere, da de behandler data på vegne af den dataansvarlige. Dette ville bl.a. få den konsekvens, at selskaber skal indgå skriftlige databehandleraftaler med samtlige ansatte, der behandler

⁷⁰ Dette har betydning for bl.a. advokater, se afsnit 4.4.

⁷¹ Med retsevne forstås evnen til at være berettiget eller forpligtet subjekt i retsforhold. Med partsevne forstås evnen til at være part i en proces. Der henvises til ”Juridisk ordbog”, 12. udgave, af Bo von Eyben, s. 266 og 294.

⁷² Teknologien tillader dog i stigende omfang automatiske computerbehandlinger, men disse foretages stadig ikke direkte af juridiske personer.

⁷³ WP 169, s. 15.

personoplysninger, jf. PDL § 42, stk. 2. Det må dog være forudsat, at databehandleren er en person uden for den dataansvarliges organisation. De ansatte inden for organisationen er en del af den dataansvarlige og er dem, der faktisk udøver dataansvaret for organisationen. Der sker med andre ord identifikation mellem den ansatte og organisationen.

Der vil dog ikke altid ske identifikation mellem virksomheden og dens ansatte. Da dataansvaret kan følge af den faktiske råden over personoplysningernes formål og hjælpemidler,⁷⁴ må det følge heraf, at ansatte kan blive dataansvarlige for behandlinger, hvis de gennem deres faktiske råden selvstændigt bestemmer over behandlingens formål og væsentlige hjælpemidler. Som en vejledende grundsætning peger Artikel 29-gruppen på, at valget skal afgøres efter, hvilken person der normalt ville være civilretligt, forvaltningsretligt eller strafferetligt ansvarlig for handlingen.⁷⁵ Dette kunne fx være tilfældet, hvis en ansat i en virksomhed søger efter følsomme oplysninger om sin nabo i virksomhedens it-system for at bruge oplysningerne som ulovligt pressionsmiddel⁷⁶. Den ansatte er herefter den dataansvarlige, da det efter dansk strafferet er den ansatte, og ikke selskabet, der er ansvarlig for en sådan abnorm handling.⁷⁷ Virksomheden er dog stadig dataansvarlig for så vidt angår opbevaringen af oplysningerne og kan derfor ifalde et erstatnings- eller straffeansvar efter PDL, hvis virksomheden ikke førte tilstrækkeligt tilsyn med den ansatte eller i det hele taget ikke traf de nødvendige sikkerhedsforanstaltninger, herunder manglende eller mangelfuld instruktion af personalet.

3.9.1. Konklusion

Både fysiske og juridiske personer kan være dataansvarlige. Juridiske personer skal forstås bredt og indeholder fx interessentskaber og partnerselskaber. Det er som udgangspunkt selskabet, og ikke dets ansatte, der er den dataansvarlige, medmindre den ansatte har et selvstændigt straffeansvar.

3.10. Særligt om dataansvar i koncerner og joint ventures

Der kan opstå særlige problemer med fordeling af dataansvar og identifikation mellem koncernforbundne selskaber. Et moderselskab og dets datterselskab er to selvstændige juridiske personer, og efter dansk selskabsret kan moderselskabet ikke give retligt bindende instrukser til datterselskabets ledelse.⁷⁸ Dette må som udgangspunkt tale for, at datterselskabet, og ikke moderselskabet, er dataansvarlig for sine egne behandlinger af personoplysninger. Det klare udgangspunkt i dansk strafferet er da også, at moderselskabet ikke er strafferetligt ansvarlig for datterselskabets forseelser.⁷⁹

Moderselskabet kan på datterselskabets generalforsamling vedtage retligt bindende beslutninger for datterselskabet, jf. SL § 76. Skulle det ske, at datterselskabet igennem en beslutning på en generalforsamling bliver tvunget til at udføre behandlinger af personoplysninger, kan det diskute-

⁷⁴ Se afsnit 3.4.

⁷⁵ WP 169, s. 16-17.

⁷⁶ En sådan afpresning kan være strafbart efter STRFL § 281.

⁷⁷ Se "Strafferet I – Ansvar", 4. udgave, 2013, af Gorm Toftegaard Nielsen, s. 244. Valget mellem at straffe et selskab eller den ansatte kan være yderst kompliceret og vil ikke blive behandlet yderligere.

⁷⁸ Dette er i hvert fald den dominerende holdning i den danske retslitteratur, se "Selskabsstrukturer", 1. udgave, 2015, af Karsten Engsig, s. 272-273.

⁷⁹ "Strafferet I – Ansvar", s. 250.

res, om moderselskabet skal betragtes som dataansvarlig i det omfang, moderselskabet ved beslutningen bestemmer behandlingens formål eller væsentlige hjælpemidler. Generalforsamlingens gyldige beslutninger må dog snarere betragtes som datterselskabets egen vilje, og ikke moderselskabets, hvorfor datterselskabet skal betragtes som dataansvarlig for behandlingen.

Selvom datterselskabets ledelse ikke er forpligtet til at adlyde instrukser fra moderselskabet, vil det dog ofte ske alligevel, da moderselskabet kan true ledelsen med at vedtage en retlige bindende generalforsamlingsbeslutning (eller true med at afsætte datterselskabets ledelse ved generalforsamlingen). Datterselskabet vil endda ofte følge instrukserne ganske frivilligt ud fra den antagelse, at hvad der er godt for koncernen som helhed, er godt for datterselskabets kapitalejer (moderselskabet) og dermed godt for datterselskabet selv. Det må dog stadig fastholdes som udgangspunkt, at datterselskabets ledelse ikke er retligt forpligtet til at følge instruksen, og derfor må datterselskabet anses for at være dataansvarlig for behandlingen, selvom formålet og hjælpemidlet reelt er fastlagt af moderselskabet. Visse datatilsyn i EU har taget aktiv stilling til spørgsmålet. Således skriver det irske datatilsyn:⁸⁰

“It is common in the business world for a holding company to own one or more subsidiary companies. If personal data is flowing within the group of companies, who is the data controller? In answering this question, it should be noted that each company, whether it is a parent company or a subsidiary, is a distinct legal person with its own set of legal and data protection responsibilities. **Each company within a group may therefore be a data controller in respect of the personal data which it has obtained and for which it is legally responsible;** and it is necessary for each data controller to assess whether disclosures of personal data to other group companies are permissible. **It is only in rare cases that two or more companies may properly exercise legal or de facto control and responsibility for a given set of personal data. In such cases, the companies are regarded as joint data controllers.**”

Ifølge det irske datatilsyn skal udgangspunktet om dataansvaret for hvert selskab altså fastholdes, men i sjældne sager kan de to selskaber anses for at være fælles dataansvarlige, hvis de sammen udøver en faktisk eller juridisk kontrol over behandlingen. Det bliver ikke uddybet, i hvilke tilfælde dette kan ske. For at sikre formålet om en effektiv og fuldstændig beskyttelse af den registrerede, må moderselskabet dog kunne ifalde et fælles dataansvar med et datterselskab, hvis et moderselskab af omgåelseshensyn opdeler aktiviteter forbundet med risikable behandlinger af personoplysninger i forskellige datterselskaber, uden at der er en reel forretningsmæssig baggrund for opdelingen (men opdelingen udelukkende sker for at forhindre hæftelse for bøder, som alene datterselskaberne hæfter for). EU-domstolen kan på denne baggrund anse moderselskabet som meddataansvarlig for sine datterselskabers behandlinger, hvis der er tale om en formel-juridisk indretning med det formål at omgå reglerne.

Kan moderselskabet ikke anses som meddataansvarlig, fx fordi moderselskabets ledelse ikke havde en viden om en konkret behandling af personoplysninger foretaget af datterselskabet, kan det overvejes om der kan ske identifikation mellem de to selskaber. Der er ikke nogen klar retspraksis for, hvornår der generelt kan ske identifikation mellem to koncernforbundne selskaber,

⁸⁰ The Office of the Data Protection Commissioner, An Coimisinéir Cosanta Sonraí, “Are you a “data controller”?”.

men man må kunne lægge vægt på, om der foreligger et misbrug eller illoyalt brug af selskabsformen og om der har været en kvalificeret kontrol af datterselskabet.⁸¹ Hvis der netop har været en kvalificeret kontrol af datterselskabet, vil det dog være mere nærliggende at betragte moderselskabet som meddataansvarlig, da selskabets gennem sin kontrol er med til at fastsætte behandlingens formål eller hjælpemidler.

PDF art. 83, stk. 4-6, synes at åbne op for identifikation som en mulighed. Ifølge bestemmelserne kan en virksomhed straffes med 2-4 % af sidste års omsætning. Ifølge betragtning 150 skal "virksomhed" forstås i overensstemmelse med TEUF art. 101 og 102. Ifølge retspraksis til disse bestemmelser, kan en koncern betragtes som en "virksomhed":⁸²

"Det bemærkes indledningsvis, at det fremgår af fast retspraksis, at i henhold til artikel 101 TEUF kan et datterselskabs adfærd tilregnes moderselskabet, bl.a. når datterselskabet, selv om det er en selvstændig juridisk person, ikke frit bestemmer sin adfærd på markedet, men i det væsentlige følger instrukser fra moderselskabet, navnlig under hensyn til de økonomiske, organisatoriske og juridiske forbindelser mellem disse to virksomheder. I en sådan situation, hvor moderselskabet og datterselskabet er en del af samme økonomiske enhed og således udgør én virksomhed i artikel 101 EF's forstand, kan Kommissionen således rette en beslutning, hvorved der pålægges en bøde, til moderselskabet, uden at der kræves en konstatering af, at sidstnævnte var direkte impliceret i overtrædelsen".

Når forordningen træder i kraft, kan man således argumentere for, at moderselskabet kan pålægges en bøde for datterselskabets overtrædelse af de persondataretlige regler, hvis datterselskabet i det væsentlige følger instrukser fra moderselskabet, selvom det ikke kan konstateres, at moderselskabet direkte har været involveret i den konkrete overtrædelse (og dermed pålægge moderselskabet en bøde uden at konstatere, at moderselskabet er dataansvarlig). Omvendt forudsætter forordningen flere steder⁸³, at den der bliver pålagt bøden er enten dataansvarlig eller databehandler. Art. 83, stk. 4-6 kan således tænkes at være rettet imod det tilfælde, at moderselskabet og datterselskabet er fælles dataansvarlige. Retsstillingen er på dette punkt ikke klar, og der er en stor fare for, at medlemsstaterne vil anlægge forskellige fortolkninger.

I det omfang selskaber inden for den samme koncern kan indgå aftaler med hinanden, er der selvfølgelig ikke noget til hinder for, at selskaberne indgår aftaler om behandlinger af personoplysninger. Antager moderselskabet således et datterselskab som databehandler, er moderselskabet naturligvis dataansvarlig, ligesom hvis moderselskabet i stedet havde antaget et selskab uden for koncernen.

Mht. til dataansvaret i joint ventures, må dette komme an på samarbejdsformen. Er der tale om et "contractual joint venture", der er et løst aftalebaseret samarbejde mellem to virksomheder, vil de to virksomheder alt efter de faktiske omstændigheder være enten selvstændige dataansvarlige eller fælles dataansvarlige. I et eksempel fra Artikel 29-gruppens vejledning,⁸⁴ blev et rejsebureau, et

⁸¹ "Selskabsstrukturer", s. 320.

⁸² Sag C-508/11 P, ENI SpA mod Kommissionen.

⁸³ Fx art. 83, stk. 3: "Hvis en dataansvarlig eller en databehandler forsætligt eller uagtsomt i forbindelse med de samme eller forbundne behandlingsaktiviteter overtræder flere bestemmelser i denne forordning, må den administrative bødes samlede størrelse [...]".

⁸⁴ WP 169, s. 20, eksempel 8. Se også eksempel 7, hvor de samme parter var selvstændige dataansvarlige.

flyselskab og en hotelkæde, der dannede en fælles internetbaseret platform, hvor kunder kunne bestille rejser, anset som fælles dataansvarlige.

Hvis samarbejdet mellem de to virksomheder i stedet foregår i et ”corporate joint venture”, hvor virksomhederne danner et fælles datterselskab, vil det som udgangspunkt være datterselskabet, der er den dataansvarlige for sine behandlinger. Dette må kunne fraviges ud fra betragtningerne ovenfor om koncerners dataansvar, således at moderselskaberne kan være fælles dataansvarlige sammen med datterselskabet.

3.10.1. Konklusion

Koncernforbundne selskaber er selvstændige juridiske personer, der ikke automatisk deles om dataansvaret. Ved omgåelse af reglerne gennem etablering af datterselskaber kan det dog ikke udelukkes, at moderselskabet kan anses som meddataansvarlig for alle de behandlinger, datterselskaberne er dataansvarlige for. Kan moderselskabet ikke betragtes som meddataansvarlig, kan der muligvis ske identifikation. Ved contractual joint ventures er de deltagende selskaber enten selvstændige eller fælles dataansvarlige, alt efter hvor tæt samarbejdet er. Ved corporate joint ventures er det det fælles datterselskab, der som udgangspunkt er den dataansvarlige, medmindre man af omgåelseshensyn må anse moderselskaberne for meddataansvarlige.

3.11. Undtagelsen om privat/familiemæssig brug og en generel bagatelgrænse for dataansvaret

Ifølge PDD art. 3, stk. 2, 2. led, finder direktivet ikke anvendelse på behandlinger foretaget af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter. Dette betyder, at en person, der foretager en sådan behandling, ikke kan være dataansvarlig. Spørgsmålet er, hvornår en sådan behandling er rent personlig eller familiemæssig. Dette bliver delvist afklaret i direktivets betragtning nr. 12:

”[En] fysisk persons behandling af oplysninger som led i rent personlige eller familiemæssige aktiviteter **som f.eks. korrespondance og føring af en adressefortegnelse**, bør dog ikke være omfattet”.

Man er således ikke dataansvarlig for de behandlinger, der foretages i forbindelse med korrespondance og føring af adressefortegnelser. Hvad der mere positivt kan lægges i undtagelsen er usikkert. Derimod må man kunne formulere en negativ definition: Erhvervsmæssige⁸⁵ og foreningsmæssige aktiviteter kan ikke have privat eller familiemæssig karakter og falder derfor uden for undtagelsen.⁸⁶

Undtagelsen er blevet fortolket af EU-domstolen i sag C-101/01-Lindqvist, hvor domstolen udtalte, at offentliggørelse af oplysninger på internettet, hvorved oplysningerne blive tilgængelige for et ubestemt antal af personer, ikke er en behandling af personlig eller familiemæssig karakter.

⁸⁵ Det fremgår nu eksplicit af PDF betragtning nr. 18, at dette falder uden for. Desuden slås det fast, at brug af sociale medier falder ind under undtagelsen.

⁸⁶ Se KPDL s. 113-116.

I sit forslag til afgørelse af sag C-131/12, Google Spain, omtalte generaladvokat brugere af søgemaskiner:⁸⁷

”Internetbrugere anvender også typisk søgemaskiner i aktiviteter, som ikke er rent personlige, f.eks. aktiviteter i forbindelse med **arbejde, studier, forretninger eller den tredje sektor**”.

Generaladvokaten mente således ikke, at behandlinger af oplysninger i forhold til arbejde, studier, forretninger eller køb af serviceydelser er rent personlige eller familiemæssige.⁸⁸ Da der stadig kan være et behov i det praktiske liv for at udelukke sådanne aktiviteter fra PDD område, foreslog generaladvokaten i stedet, at man begrænsede dataansvaret efter princippet om rimelighed og proportionalitetsprincippet:

”Under de nuværende forhold vil de brede definitioner af personoplysninger, behandling af personoplysninger og registeransvarlig på grund af den teknologiske udvikling sandsynligvis dække en hidtil uset bred vifte af nye faktiske situationer. Mange, hvis ikke de fleste, websites og filer, som kan tilgås på disse websites, indeholder nemlig personoplysninger som f.eks. navne på nulevende fysiske personer. **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**”.

Det er utvivlsomt rigtig, at efterhånden som teknologien udvikler sig og bliver mere og mere tilgængelig for den almene befolkning, jo større vil behovet være for at undtage ”almindelige” mennesker for dataansvaret ud fra et pragmatisk synspunkt. Dette er anerkendt på andre retsområder. fx har man på det immaterialretlige område udviklet grundsætningen ”de minimis non curat lex” (retten interesserer sig ikke for bagateller), hvorefter immaterialretten ikke omfatter rene bagatelagtige krænkelse af ophavsretten ved fx at fløjte en sang eller spille høj musik i bilen.⁸⁹ Hvis man ikke ønsker at anerkende denne grundsætning fuldt ud i persondataretten af frygt for at underminere den registreredes databeskyttelse, bør man i det mindste lade den bagvedliggende pragmatisk ide have indflydelse på fortolkningen af undtagelsen om personlig og familiemæssige aktiviteter, således at undtagelsen fortolkes udvidende. Proportionalitetsprincippet er fuldt ud anerkendt i EU-retten og bør også føre til en udvidet fortolkning af undtagelsen. En nærmere udfyldning af undtagelsen må dog ske i EU-domstolens praksis, der må finde en fornuftig balance mellem hensynet til personers databeskyttelse og pragmatisk hensyn i takt med den teknologiske udvikling i samfundet.

3.11.1. Konklusion

Ud over korrespondance og føring af adressefortegnelser kan det ikke siges nærmere, hvornår en behandling falder ind under undtagelsen om familiemæssig karakter. Erhvervsmæssige, foreningsmæssige og offentliggørende behandlinger må dog falde uden for. Ud fra pragmatisk hensyn og proportionalitetsprincippet, må undtagelsen skulle fortolkes udvidende i takt med den teknologiske

⁸⁷ Forslag til afgørelse fra generaladvokaten N. Jääskinen, fremsat den 25. juni 2013, i sag C-131/12, Google Spain, s. 17, fodnote 57.

⁸⁸ Da sagen ikke omhandlede brugernes dataansvar, men udbyderens, tog EU-domstolen ikke stilling til dette.

⁸⁹ Se ”Immaterialret”, 1. udgave, 2008, af Jens Schovsbo og Morten Rosenmeier, s. 195.

udvikling gør det mere normalt for almindelige personer at behandle personoplysninger, dog uden at den registreredes databeskyttelse undermineres.

3.12.Samlet konklusion af den abstrakte fortolkning af de to begreber

Det er antaget i forarbejderne til PDL, at de to begreber skal forstås i overensstemmelse med den tidligere skelnen mellem den registeransvarlige og edb-servicebureauer. Dette må siges at være forkert, da de to begreber er selvstændige EU-retlige begreber, hvis indhold ikke påvirkes af tidligere national ret. Begrebet den dataansvarlige skal fortolkes udvidende, hvilket må ske på bekostning af databehandleren, der bliver underlagt en snæver fortolkning.

Man er dataansvarlig, hvis man har kontrol over en behandlings formål eller væsentlige hjælpemidler. Denne kontrol kan følge af en eksplicit juridisk kompetence, implicit kompetence (fx en arbejdsgivers behandling af personoplysninger om de ansatte) samt en faktisk indflydelse. Særligt den sidste måde at udøve kontrol på er svær at anvende i praksis, og der er en stor sandsynlighed for forskellig praksis i de forskellige EU-lande. Man kan dog pege på visse principper for vurderingen. Fx er køberen af en standardiseret tjenesteydelse (fx administration af lønudbetaling) dataansvarlig, når udbyderen ellers på forhånd har fastlagt alle vilkårene for behandlingen, da køberen i det hele taget vælger at gøre brug af udbyderen. Er behandlingen derimod ikke fastlagt på forhånd, og udbyderen har en stor selvstændighed med opgavens udførelse, må udbyderen have en sådan kontrol over behandlingens formål og hjælpemidler, at han typisk er dataansvarlig. Hvis parterne derimod har reelle forhandlinger om, hvordan behandlingen skal ske, kan parterne betragtes som fælles dataansvarlige.

Den dataansvarlige har det strafferetlige og erstatningsretlige ansvar for overholdelsen af en række pligter i PDL. Pligterne og ansvaret omfatter dog kun de behandlinger, hvor han anses for at være dataansvarlig, dog ligegyldigt, om behandlingen konkret er foretaget af den dataansvarlige eller databehandleren. En behandling kan betragtes på makro-niveau som en række af operationer med et fælles formål. Databehandleren har dog nogle få selvstændige pligter, som han også er ansvarlig for.

Der er et særligt problem vedrørende ansvarsfordeling og identifikation mellem selskaber og deres ansatte og moderselskaber og dets datterselskaber. Som udgangspunkt vil der ske identifikation mellem et selskab og dets ansatte, og der vil som udgangspunkt ikke ske identifikation mellem koncernforbundne selskaber.

Retsstillingen er dog ikke særlig klar, og der er behov for flere afgørelser om spørgsmålet fra EU-domstolen.

4.Advokaters dataansvar

4.1.Præsentation af problemstillingen vedr. advokater

Advokater lever i høj grad af at behandle oplysninger, herunder personoplysninger, på vegne af deres klienter. Dette giver anledning til at overveje forholdet mellem dem og deres klienter.

Spørgsmålet er, i hvilket omfang de er selvstændige dataansvarlige, deres klients meddataansvarlige eller deres klients databehandler. Som det allerede er gennemgået tidligere⁹⁰, er det et helt grundlæggende problem, der helst skal stå klart for parterne, inden behandlingen af personoplysninger begynder. Der skal fx foreligge en skriftlig databehandleraftale helt fra starten af, hvis der er tale om et dataansvarlig/databehandler-forhold, jf. PDL § 42, stk. 2. Advokater er særligt interessante, da der er uenighed mellem Datatilsynet og den danske retslitteratur på den ene side og Artikel 29-gruppen og ICO på den anden side om, i hvilket omfang advokater er dataansvarlige og databehandlere.⁹¹

4.2. Advokater i rådgiverrollen

Spørgsmålet er, om advokater skal betragtes som dataansvarlige eller databehandlere, når de modtager oplysninger fra en klient for at rådgive ham. Datatilsynet har i en e-mail⁹² om advokaters dataansvar henvist til KPDL:⁹³

”[...] Det samme vil efter omstændighederne kunne være tilfældet, når den dataansvarlige overlader personoplysninger til f.eks. en advokat eller revisor med henblik på, at denne skal rådgive, jf. herved også den ovennævnte sag, j.nr. 2000-219-0019. Sådanne forhold bør betragtes på den måde, at repræsentanten behandler personoplysningerne *for den dataansvarlige*, dvs. at repræsentanten kan behandle personoplysningerne i samme omfang, som den dataansvarlige.”

Udgangspunktet for Datatilsynet er altså, at når den dataansvarlige giver oplysninger til en advokat med henblik på at få rådgivning, vil rådgiveren blive betragtet som en databehandler, da han behandler personoplysninger på vegne af den dataansvarlige. For så vidt angår advokater, er dette synspunkt blevet bekræftet i en artikel af advokat Jens Harskov Hansen:⁹⁴

”Anderledes forholder det sig, når advokaten rådgiver klienten og til brug herfor modtager oplysninger fra klienten. **Her er udgangspunktet, at klienten overlader personoplysninger til advokaten. Advokaten fungerer derved som databehandler for klienten.**... Dette vil blandt andet være tilfældet, hvis advokaten modtager oplysninger om en virksomheds medarbejder med henblik på at vurdere, om der er grundlag for en bortvisning”.

I Danmark bliver advokater altså i høj grad betragtet som databehandlere. Synspunktet bygger til dels på Datatilsynets afgørelse j.nr. 2000-219-0019, der omhandlede et inkassobureau. Her udtalte Datatilsynet:

⁹⁰ Se afsnit 1.1. for gennemgangen af vigtigheden af afklaringen af rollerne mellem samarbejdspartnere.

⁹¹ Datatilsynet og den danske retslitteratur (bl.a. KPDL) mener, at advokater i mange tilfælde som rådgivere er databehandlere, mens Artikel 29-gruppen og ICO mener, de som udgangspunkt er dataansvarlige. Uenigheden vil blive gennemgået udførligt i afsnit 4.

⁹² Se bilag 1, e-mail fra Datatilsynet af 11. maj 2017., svar på en forespørgsel om advokaters dataansvar.

⁹³ KPDL s. 165.

⁹⁴ ”PDL – gælder den også for advokater?”, ”Advokaten”, udgivet af advokatsamfundet, 22. september 2015, af advokat Jens Harskov Hansen

”Datatilsynet finder herefter, at en overladelse af oplysninger fra [inkassofirmaets] kunder (den dataansvarlige) til [inkassofirmaet] til brug for databehandling i en konkret arbejdsopgave ikke er i strid med behandlingsreglerne i PDL § 11, stk. 2. Inkassofirmaet er således alene databehandler for kunden, og må ikke behandle oplysningerne selvstændigt eller uden instruktion fra den dataansvarlige”.

Der er dog tale om vidt forskellige situationer. I ovennævnte sag var inkassofirmaet ikke rådgiver, men tvangsinddrev penge på vegne af sine kunder. Da de faktiske forhold i sagen kan være afgørende for, om vedkommende bestemmer behandlingens formål eller hjælpemidler, er det farligt at slutte fra en situation til en anden uden en særdeles uddybende argumentation.

For så vidt angår forfatterne i KPDL, bygger de også deres synspunkt på Registertilsynets praksis om sondringen mellem den registeransvarlige og et EDB-servicebureau, som de mener i vidt omfang er det samme som sondringen i dag mellem dataansvarlige og databehandlere. I forhold til advokater og revisorer skrev Registertilsynet i RÅ 1979⁹⁵.

”**Overladelse** til virksomhedens revisor eller advokat eller til eventuel edb-behandling i edb-servicebureau **betragtes ikke som videregivelse i lovens forstand**”.

Dette beror på en sondring mellem *videregivelse* og *overladelse*. Når en registeransvarlig gav oplysninger til en anden registeransvarlig, var der tale om en *videregivelse*. Når en registeransvarlig gav oplysninger til et edb-servicebureau, var der derimod tale om en *overladelse*. Når Registertilsynet i årsberetningen fra 1979, således skriver, at der ikke er tale om en videregivelse, men en overladelse, når en virksomhed giver oplysninger til en advokat eller revisor, mener tilsynet således, at advokater er omfattet af reglerne om edb-servicebureauer, og ikke er omfattet af reglerne om registeransvarlige. Dette synspunkt blev fastslået i Rt.s j.nr. 1996-213-020⁹⁶, der omhandlede en konsulent. Sagen drejede sig om Statens Biblioteksstyrelse, der gav en konsulent disketter med oplysninger fra Biblioteksafgiftsregistret. Konsulenten skulle herefter rådgive styrelsen. Registertilsynet udtalte, at der ikke var tale om en videregivelse, men derimod en overladelse, hvormed konsulenten var omfattet af reglerne om edb-servicebureauer, og ikke blev betragtet som registeransvarlig.

Dermed kan det siges, at under registerlovene blev rådgivere omfattet af reglerne om edb-servicebureauer, og de blev ikke betragtet som registeransvarlige, i det omfang de fik oplysninger af deres klienter til at løse opgaver for dem og rådgive dem. Forfatterne i KPDL mener, man kan lægge vægt på denne praksis og slutte, at når advokater er i rådgiverrollen, er de databehandlere, ligesom de førhen var omfattet af reglerne om edb-servicebureauer. Som det blev gennemgået i afsnit 3.1., er begreberne den dataansvarlige og databehandleren selvstændige EU-retlige begreber. Betragtninger fra Registertilsynets praksis må derfor være irrelevante for vurderingen, selvom forarbejderne lægger stor vægt på denne praksis. Det gennemgående synspunkt i dansk ret bygger altså på et aldeles forkert grundlag. Det afgørende for vurderingen må være, hvem der i den konkrete situation fastlægger behandlingens formål og/eller væsentlige hjælpemidler.

Man kan dog argumentere for, at det vel netop er klienten, der bestemmer formålet og hjælpemidlerne, når han søger rådgivning hos en advokat. Klientens formål kan være at fastlægge et retskrav,

⁹⁵ Registertilsynets årsberetning, 1979, s. 203.

⁹⁶ Udførligt omtalt i KPDL s. 155-156

og han giver advokaten de nødvendige personoplysninger, som er væsentlige hjælpemidler i behandlingen. Dette er dog ikke en korrekt analyse, se straks nedenunder.

I Datatilsynets e-mail⁹⁷ om spørgsmålet henvises der udover KPDL også til ICO's⁹⁸ vejledning om dataansvar. ICO skriver i sin vejledning følgende om en advokat, der rådgiver et ingeniørfirma om en tidligere ansat, der bruger firmaets klientliste i et rivaliserende firma:⁹⁹

”Once she [ejeren af ingeniørfirmaet] hands over the personal data to the solicitors, **they take on data controller responsibility** for the data and process it for their own purposes, even though they are acting on behalf of their client.

The solicitors process this personal data for the broad purpose of providing legal services in accordance with their professional obligations. They will use the information the firm has provided and will collect any other information they need in order to carry out the instructions. **The solicitors determine the manner in which the personal data obtained from the firm will be processed.** The solicitors therefore act as the data controller”.

Ifølge ICO kan advokater altså i vidt omfang anses som dataansvarlige, når de rådgiver klienter.¹⁰⁰ Argumentationen bygger på, at advokaten har sit eget bredere formål med behandlingen af personoplysninger (fastslå retsstillingen og leve op til etiske, retlige og professionelle standarder), end klienten har. Advokatens brede formål gennembryder dermed klientens formål, og advokaten har dermed fastlagt formålet med behandlingen.¹⁰¹ Desuden vælger advokaten, hvilke oplysninger, der skal behandles, da han kan vælge at anse oplysninger fra klienten som irrelevante, bede klienten om yderligere oplysninger og indsamle flere oplysninger på egen hånd. Advokaten kan desuden sende oplysninger videre til tredjemænd. Advokaten bestemmer således også over behandlingens væsentlige hjælpemidler, og han må derfor være dataansvarlig i rådgiverrollen. Klienten må dog være dataansvarlig for selve videregivelsen af oplysninger til advokaten (og er dermed bl.a. ansvarlig for sikkerheden for videregivelsen, herunder om personoplysningerne skal sendes i krypteret form, hvilket er særlig relevant ved følsomme personoplysninger og CPR-numre).

Der må dog være situationer, hvor dette ikke er tilfældet. Artikel 29-gruppen skriver i deres vejledning om spørgsmålet:¹⁰²

”Revisorers kvalifikationer kan variere afhængigt af sammenhængen. Når revisorer leverer ydelser til den almene offentlighed og småhandlende på baggrund af meget generelle instrukser ("udarbejd min selvangivelse"), er revisoren – **ligesom praktiserende advokater**, der handler under lignende omstændigheder og af samme årsager – en registeransvarlig. **Når en revisor ansættes af et firma og pålægges detaljerede instrukser fra den interne revisor, evt. om at foretage en detaljeret revision, er**

⁹⁷ Bilag 1

⁹⁸ ICO's ”Data controllers and data processors: what the difference is and what the governance implications are”

⁹⁹ Vejledningen, s. 12-13.

¹⁰⁰ Man kan derfor undre sig over, hvorfor Datatilsynet henviser til ICO's vejledning, da vejledningens synspunkt er i direkte modstrid med KPDL, som Datatilsynet ligeledes henviser til.

¹⁰¹ Se afsnit 3.5.

¹⁰² WP 169, s. 30.

denne dog generelt om ikke en almindelig medarbejder så registerfører [databehandler] pga. instruksernes klarhed og det konsekvente begrænsede omfang af frihed”.

Advokatens dataansvar i rådgiverrollen må derfor begrænses i det omfang, advokatens selvstændighed indskrænkes med detaljerede og klare instrukser fra klienten, hvorefter advokaten ikke længere kan fastlægge formålet eller hjælpemidlerne. Dette vil formentlig kræve, at klienten selv har ansatte med en vis ekspertise inden for feltet – i eksemplet ovenfor er revisoren da også databehandler, efter han blev pålagt detaljerede instrukser af klientens interne revisor. En advokat vil herefter typisk være databehandler, når en stor virksomheds in-house jurist delegerer en bestemt delopgave til en specialiseret advokat og giver detaljerede og præcise instrukser for opgavens udførelse. Det samme vil formentlig gælde, når en advokat fungerer som underleverandør til en anden advokat, fx hvis der er et enkelt forhold i en virksomhedsoverdragelse, der skal afdækkes (og advokaten i forbindelse med opgaven bliver underlagt klare instrukser). I disse situationer skal advokaten løse en begrænset opgave, hvormed hans brede formål om at tilbyde helhedsorienteret rådgivning forsvinder, og hans handlefrihed er stærkt indskrænket af instrukserne, hvormed han ikke kan bestemme selvstændigt over behandlingens væsentlige hjælpemidler.

4.2.1. Konklusion

Advokater vil i rådgiverrollen som udgangspunkt være dataansvarlige, medmindre advokaten får en opgave en af klient, der selv råder over en vis ekspertise inden for det pågældende område, og som instruerer rådgiveren klart og tydeligt om opgavens udførelse, således at rådgiveren ikke har selvstændighed nok til at fastlægge behandlingens formål og væsentlige hjælpemidler. Dette vil være tilfældet, når et stort selskabs in-house jurist delegerer specifikke og afgrænsede delopgaver til en ekstern advokat (typisk en specialist inden for et afgrænset retsområde) for at få rådgivning om noget bestemt, og advokaten samtidigt bliver underlagt klare instrukser for opgavens udførelse.

4.3. Behandlingen er lovpligtig

Man kan ved lov være forpligtet til at behandle personoplysninger. Fx finder hvidvaskningsloven anvendelse på advokater, jf. hvidvaskningslovens § 1, stk. 1, nr. 13-14, og de kan derfor være forpligtet til at behandle personoplysninger efter hvidvaskningslovens regler. Er man forpligtet ved lov til at foretage en behandling af personoplysninger, har man en kontrol over behandlingens formål og hjælpemidler, der er baseret på eksplicit juridisk kompetence.¹⁰³ I det omfang advokater er forpligtet til at behandle personoplysninger ved lov, må de derfor være dataansvarlige.

Det samme må gælde, hvis en konkret behandling er fastlagt af andre normer. Advokater er underlagt normen om ”god advokatskik”, jf. RPL § 126, stk. 1. I det omfang en konkret behandling er krævet af normen, må advokaten også være dataansvarlig, da det er advokaten, og ikke klienten, der fastlægger formålet med behandlingen (opfylde sine professionelle forpligtelser). Det er fx god advokatskik at opbevare oplysninger fra en sag i en vis periode, efter sagen er afsluttet.¹⁰⁴ Denne efterfølgende opbevaring er en selvstændig behandling, som advokaten må være dataansvarlig for.

¹⁰³ Se afsnit 3.4.

¹⁰⁴ ”De advokatetiske regler”, Advokatsamfundet, fra 1. november 2016, s. 4, pkt. 10.

4.4. Behandling af oplysninger om klienten selv og dennes familie

Advokater behandler ofte oplysninger om klienten selv og klientens familiemedlemmer. Dette kan have betydning for vurderingen af dataansvaret. Ifølge advokat Jens Harskov Hansen, vil en advokat, der får oplysninger fra en klient for at udarbejde et testamente, være en databehandler:¹⁰⁵

”Advokaten fungerer derved som databehandler for klienten, og advokaten kan derfor behandle personoplysninger i samme omfang som klienten. Dette vil blandt andet være tilfældet, hvis advokaten modtager oplysninger [...] om klienten selv til brug for udarbejdelse af et testamente eller en ægtepagt”.

Som det allerede er beskrevet tidligere,¹⁰⁶ kan den registrerede ikke være dataansvarlig for behandlinger om ham selv, da dette savner al mening. Da der ikke er en dataansvarlig, som advokaten kan behandle personoplysninger på vegne af, kan han umuligt være databehandler. Får en advokat således oplysninger om klienten selv for fx at udarbejde et testamente eller udfylde en selvangivelse, må de altid være dataansvarlige for deres behandling af oplysningerne.

Dernæst er det også meget almindeligt, at advokater behandler personoplysninger om klientens familiemedlemmer. Her er spørgsmålet, om undtagelsen om behandlinger i rent privat eller familiemæssig interesse finder anvendelse, jf. PDD art. 3, stk. 2, 2. led. Det er klart, at en advokats behandling af oplysningerne om familiemedlemmerne falder uden for undtagelsen, da behandlingen sker som led i advokatens erhverv. Det kan dog diskuteres, om undtagelsen finder anvendelse på klientens behandlinger (indsamle og videresende oplysningerne til advokaten). Såfremt undtagelsen finder anvendelse, er klienten ikke omfattet af de persondataretlige regler, hvorefter klienten ikke kan være dataansvarlig. Er klienten ikke dataansvarlig, kan advokaten ikke være databehandler, da der ikke er en dataansvarlig at behandle oplysninger på vegne af.

Som det er beskrevet før, skal undtagelsen om personlige og familiemæssige behandlinger af oplysninger underlægges en udvidende fortolkning på baggrund af pragmatiske hensyn, men at indholdet af undtagelsen ellers ikke kan blive beskrevet endeligt og fyldestgørende.¹⁰⁷ Man kan dog argumentere for, at i hvert fald den juridiske indretning af familielivet kan falde ind under begrebet familiemæssige behandlinger. Herefter falder de behandlinger, en klient foretager i forbindelse hermed, uden for de persondataretlige regler. Dette vil bl.a. omfatte indsamling og overgivelse af oplysningerne til advokaten med henblik på at få udarbejdet et testamente og en ægtepagt. Hensynet til modparten må dog tale for, at der må vises en vis tilbageholdenhed, hvis der er potentiale for en konflikt, hvorefter klientens behandlinger i forbindelse med en skilsmisse og et dødsbo må falde uden for undtagelsen. I det hele taget må alle behandlinger med henblik på at fastlægge et retskrav mod et familiemedlem falde uden for undtagelsen, ligesom behandlinger i forbindelse med opløsningen af familielivet som udgangspunkt ikke kan betragtes som en del af familielivet.

Den praktiske relevans af ovenstående synspunkter er dog ikke særlig stor. Advokaten vil ofte være dataansvarlig af andre grunde, fx i rollen som rådgiver. Mht. de familiemæssige behandlinger vil familiemedlemmerne også ofte selv være klienter, hvorfor spørgsmålet om anvendelsen af undtagelsen slet ikke opstår (men dermed bliver betragtningen om refleksvirkningen af den registreredes manglende dataansvar for oplysninger om vedkommende selv, relevant).

¹⁰⁵ ”PDL – gælder den også for advokater?”

¹⁰⁶ Se afsnit 3.8.

¹⁰⁷ Se afsnit 3.11.

4.4.1. Konklusion

Behandles der oplysninger om klienten selv, vil man altid være dataansvarlig. Behandles der oplysninger om klientens familiemedlemmer, kan dette efter omstændighederne føre til et dataansvar. Den praktiske rækkevidde af disse synspunkter er ikke særlig stor.

4.5. Behandling af personoplysninger som procesførende advokat

Advokater behandler personoplysninger som led i repræsentationen af en klient i en retssag. Spørgsmålet er, om advokater i denne situation er dataansvarlige eller databehandlere.

Når advokaten repræsenterer klienten i fx en retssag, kan det for det første overvejes, om der sker identifikation mellem advokaten og klienten, således at advokaten bliver en del af klientens organisation, nærmest som var advokaten en ansat. Det må dog fastholdes, at advokaten beholder sin autonomi og ikke er underlagt en ansættelsesretlig instruktionsbeføjelse fra klientens side. Situationen adskiller sig dermed fra den ansattes situation, og dermed sker der ikke identifikation mellem klient og advokat.

Da der ikke sker identifikation, må parternes kontrol over behandlingens formål og hjælpemidler vurderes. Klienten kan i princippet instruere advokaten til at tage bestemte processuelle skridt, og advokatens handlinger i processen hviler på en aftale mellem advokaten og klienten, som klienten naturligvis har haft en vis indflydelse på. Umiddelbart kan det derfor ligne, at klienten er (eller i hvert fald har mulighed for at være) den dataansvarlige, og advokaten blot følger den aftale og de instrukser, klienten måtte give.

Ligesom med advokatens handlinger som led i rådgiverrollen, må dette synspunkt dog nuance- res betragteligt. Man er ikke en databehandler, blot fordi man antages af en person til at udføre en opgave. Artikel 29-gruppen udtaler sig om spørgsmålet i deres vejledning:¹⁰⁸

”En procederende advokat repræsenterer sin klient i retten og behandler i den forbindelse personoplysninger vedrørende klientens sag. Det juridiske grundlag for at gøre brug af de nødvendige oplysninger er klientens bemyndigelse. **Denne bemyndigelse er dog ikke rettet mod behandling af oplysninger, men mod repræsentation i retten, idet disse erhverv traditionelt har deres eget retsgrundlag for en sådan aktivitet.** Disse erhverv skal derfor anses som **uafhængige "registeransvarlige" [dataansvarlige] ved behandlingen af oplysninger under den juridiske repræsentation af deres klienter**”.

Artikel 29-gruppen peger altså på, at advokater har deres eget retsgrundlag for behandling af personoplysninger i en retssag, mens selve bemyndigelsen fra klienten ikke er rettet mod behandling af personoplysninger. Det særlige retlige grundlag for advokater fremgår af RPL §§ 131, 260, stk. 2, og 261, stk. 2, der fastslår, at advokater som udgangspunkt er eneberettigede til at procedere sager på vegne af andre. I kraft heraf er advokater udstyret med en særlig grad af uafhængighed i retsprocessen, hvorefter han må betragtes som den dataansvarlige. Klienten må dog stadig være dataansvarlig for de handlinger, han foretager i starten af forholdet (indsamle og videregående oplysninger til advokaten). Synspunktet om formålsgennembrud må også kunne føre til det samme

¹⁰⁸ WP 169, s. 29, eksempel 21.

resultat, da advokaten må have et bredere formål med behandlingen end klienten. Således varetager advokaten det brede formål at føre proces i overensstemmelse med sine professionelle forpligtelser, hvorimod klienten har formålet at få fastslået sin ret. Under advokatens brede formål falder også behandlinger af oplysninger, der kan føre til et alternativ til en hovedforhandling, fx behandlinger af personoplysninger i en vurdering af indgåelse af et eventuelt retsforlig. Desuden er advokaten forpligtet til at udføre mange af handlingerne som følge af god advokatskik (fx sætte modpartens advokat på en e-mail som "cc"), hvorefter formålet med behandlingen naturligvis er fastsat af advokaten og ikke af klienten. I det hele taget er advokaten som følge af god advokatskik underlagt en pligt til at være uafhængig i sin rolle som procesførende, hvilket også indebærer uafhængighed af klienten, hvilket ikke kan forliges med rollen som databehandler:¹⁰⁹

"Advokaten skal under udøvelse af sin advokatvirksomhed altid bevare fuld uafhængighed. Det er advokaten, der fører en retssag for klienten, og selv lægger navn til som procedør. Advokaten må ikke være følgagtig og skal kun gennemføre klientens ønsker, hvis advokaten finder dette rimeligt såvel som etisk og juridisk korrekt. Advokaten må ikke lade sig diktere af sin klient".

Ud fra alle disse synspunkter må procederende advokater derfor altid betragtes som den dataansvarlige. Herefter kan man overveje, hvilken rækkevidde, dette har. Ud fra lignende betragtninger, må ovenstående også gælde, når advokaten repræsenterer klienten i andre sammenhænge, fx ved domstolslignende organer, råd, nævn, voldgiftsretter og lignende, både ved mundtlig og skriftlig procedure.

4.5.1. Konklusion

Advokater er som procesførende altid dataansvarlige for alle handlingerne.

4.6. Ansvarsfordeling mellem advokaten som fysisk person og advokatselskabet

Udøvelsen af advokatvirksomhed kan gøres både ved enkeltmandsvirksomhed og igennem et selskab, hvilket kan give anledning til problemer om fordeling af dataansvaret. For så vidt angår enkeltmandsvirksomheden er der dog ingen problemer. Når en fysisk person er selvstændig erhvervsdrivende, er det den fysiske person, der er dataansvarlig eller databehandler. Har vedkommende ansatte i virksomheden sker der identifikation, medmindre den ansatte foretager en abnorm behandling på egen hånd, og arbejdsgiveren ellers har ført tilstrækkeligt tilsyn med den ansatte og har instrueret den ansatte i korrekt behandling af personoplysninger.¹¹⁰

For så vidt angår advokater, kan de vælge at organisere sig som et interessentskab, aktieselskab, anpartsselskab eller et partnerselskab, jf. RPL § 124. Som udgangspunkt er det selskabet, der er dataansvarlig eller databehandler (såfremt klienten indgår aftalen med selskabet og ikke med en af advokaterne), og der sker identifikation mellem selskabet og de enkelte advokater, ligesom ved ethvert andet selskab. Dette udgangspunkt må dog modificeres for så vidt angår retssager, da kun advokater, og ikke advokatselskaber, kan være rettergangsfuldmægtige, jf. modsætningsvis RPL § 131¹¹¹. Dette må have den konsekvens, at det er advokaten personligt, der er dataansvarlig som

¹⁰⁹ "Advokatetik – ret og rammer", 2. udgave, 2012, af Martin Lavesen og Lars Økjær Jørgensen. Bogen er udgivet af Advokatsamfundet og indgår i advokatuddannelsens kursus i god advokatskik.

¹¹⁰ Se afsnit 3.9.

¹¹¹ Se også "Den civile retspleje", 3. udgave, 2015, af Ulrik Rammeskov Bang-Pedersen og Lasse Højlund Christensen, s. 51.

procesførende, og ikke advokatselskabet.¹¹² Delegerer advokaten visse behandlinger som rettergangsfuldmægtig til en advokatsekretær eller en advokatfuldmægtig, vil der ske identifikation mellem dem. For så vidt angår advokater som rådgivere, er det ofte selve advokatselskabet, klienten indgår en aftale med. Det er derfor også advokatselskabet, der er den dataansvarlige (eller databehandler for klienten) for behandlingen, og ikke de enkelte advokater personligt. Der sker identifikation mellem de ansatte og advokatselskabet ligesom ved et almindeligt selskab.

4.6.1. Konklusion

Advokater er personligt dataansvarlige som rettergangsfuldmægtige. Der sker identifikation mellem advokaten og dem, han uddelegerer arbejde til i forbindelse med processen. Et advokatselskab kan være dataansvarlig eller databehandler som rådgiver, når aftalen indgås direkte mellem selskabet og klienten. I så fald sker der identifikation med de ansatte i selskabet.

4.7. Samlet konklusion af advokaters dataansvar

Advokater er i et meget videre omfang dataansvarlige, end hvad der i dag antages i den danske retslitteratur. Dataansvaret skyldes primært advokaternes store selvstændighed med løsning af opgaven og deres iagttagelse af god advokatskik. Det er dog ikke udelukket, at en advokat i visse tilfælde er databehandler, særligt når han er underleverandør for andre advokater eller løser meget præcist formulerede opgaver fra store virksomheders in-house jurister. Det kommer dog stadig an på en konkret vurdering af, om advokaten har selvstændighed og handlefrihed med løsningen af opgaven. Når advokaten behandler personoplysninger om sin klient, vil han altid være dataansvarlig, og det samme vil i et vist omfang gælde for behandling af oplysninger om klientens familie. Som procesførende er det den enkelte advokat, der personligt er dataansvarlig, mens det i rådgiverrollen ofte vil være advokatselskabet.

5. Samlet konklusion af specialet

5.1. Konklusion

Problemformuleringen for denne afhandling er, hvornår man er dataansvarlig eller databehandler, med særligt henblik på denne problemstilling i forhold til advokater. De mest centrale konklusioner må være, at begrebet dataansvarlig skal fortolkes udvidende, og begrebet databehandler skal fortolkes indskrænkende. Formålet med ordningen er at pålægge den dataansvarlige et ansvar for de behandlinger, han nøje har instrueret databehandleren i at foretage. Ved vurderingen skal man lægge vægt på graden af kontrol, selvstændighed og handlefrihed. Har vedkommende ingen handlefrihed med opgavens udførelse, han udfører på vegne af en anden, må han være databehandler. Det er også blevet anført, at man kan være dataansvarlig for forskellige dele af behandlingen, alt efter hvad man har kontrol over. Når det er blevet fastslået, hvad man er dataansvarlig for, påhviler der i forhold til dette en række pligter efter PDL, man skal overholde. Man er i denne forbindelse underlagt et erstatnings- og straffeansvar. Derudover er der en række problemer i forhold til ansvarsfordeling og identifikation mellem virksomheder, ansatte og koncernforbundne selskaber. Som udgangspunkt sker der identifikation mellem en virksomhed og dens ansatte. Koncernfor-

¹¹² Det samme må gælde for advokater, der er ansat i en anden advokats enkeltmandsvirksomhed.

bundne selskaber er som udgangspunkt selvstændige juridiske personer, der ikke deles om dataansvaret. Efter omstændighederne kan koncernforbundne selskaber dog være fælles dataansvarlige, eller der kan ske identifikation.

Vedr. advokater er disse i langt de fleste tilfælde dataansvarlige pga. deres store grad af selvstændighed med opgavens udførelse. Det er ellers antaget i den danske retslitteratur, at advokater i mange tilfælde er databehandlere. Den procederende advokat er personligt dataansvarlig, mens et advokatselskab kan være den dataansvarlige som rådgiver, hvorefter der sker identifikation med de ansatte.

6.Perspektivering

6.1.Perspektivering

Når PDF træder i kraft i maj 2018, bliver det særligt vigtigt for erhvervsdrivende at være i stand til at gennemskue, om de er dataansvarlige eller databehandlere. Der er stadig en række usikkerhedsmomenter ved vurderingen. Justitsministeriet er dog opmærksomme på dette og har planer om at udgive en vejledning herom i oktober 2017,¹¹³ hvilket forhåbentligt vil gøre retsstillingen klarere. I sidste ende må begrebernes indhold udfyldes gennem EU-domstolens case law, der dog formentligt vil have begrænset præjudikatsværdi, da vurderingen ofte er meget konkret begrundet. Da vurderingen netop ofte hviler på meget konkrete forhold, vil det være meget gavnligt, hvis de forskellige brancheforeninger udsteder vejledninger om spørgsmålet til deres medlemmer, således at hvert enkelt medlem ikke selv skal opfinde den dybe tallerken.

Litteraturfortegnelse

Dansk lovgivning:

Lov 2000-05-31 nr. 429 om behandling af personoplysninger (Persondataloven, PDL), med senere ændringer

Lov nr. 294 af 08/06/1978 om offentlige myndigheders registre (offentlig registerlov, ORL), med senere ændringer (nu ophævet)

Lov nr. 293 af 08/06/1978 om private registre m.v. (privat registerlov, PRL), med senere ændringer (nu ophævet)

Internationale aftaler

Treaty No.108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 01/10/1985

EU-retsakter:

Europa-Parlamentets og Rådets forordning af 2016-04-27 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og

¹¹³ ”Databeskyttelsesforordningen – tidsplan for vejledninger”.

om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (2016/679) (Persondataforordningen, forordningen, PDF)

Europa-Parlamentet og Rådets direktiv af 1995-10-24 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (95/46) (Persondatadirektivet, direktivet, PDD)

Udenlandsk ret:

Data Protection Act of 1998 (den britiske persondatalov)

Lov om behandling av personoplysninger (den norske persondatalov)

EU-domme (og generaladvokatens forslag til afgørelse):

C-149/15 Wathelet

C-131/12, Google Spain, Domstolens dom (Store Afdeling) af 13. maj 2014

Forslag til afgørelse fra generaladvokaten N. Jääskinen, fremsat den 25. juni 2013, i sag C-131/12, Google Spain

C-212/04 Adeneler

C-371/02 Björnekulla

C-14/83 von Colson

Registertilsynsafgørelser og årsberetninger

Rt.s j.nr. 1996-213-020

Registertilsynets årsberetning, 1979 (RÅ 1979)

Datatilsynsafgørelser og vejledninger

Dt.s j.nr. 2000-219-0019

Datatilsynets generelle vejledning om, hvorvidt man er dataansvarlig eller databehandler: <https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/>

Bøger:

”Advokatetik – ret og rammer”, 2. udgave, 2012, af Martin Lavesen og Lars Økjær Jørgensen

“Data Protection”, 4. udgave, 2015, af Peter Carey (sammen med Bridget Treacy)

”Den civile retspleje”, 3. udgave, 2015, af Ulrik Rammeskov Bang-Pedersen og Lasse Højlund Christensen

”Europæiseringen af danske ret”, 1. udgave, 2008, af Birgitte Egelund Olsen og Karsten Engsig Sørensen

”Immaterialret”, 1. udgave, 2008, af Jens Schovsbo og Morten Rosenmeier

”Lov om behandling af personoplysninger”, 3. udgave, 2015, af Henrik Waaben og Kristian Korfits Nielsen (KPDL)

”Selskabsstrukturer”, 1. udgave, 2015, af Karsten Engsig

”Strafferet I – Ansvar”, 4. udgave, 2013, af Gorm Toftegaard Nielsen

Artikler:

"Allocating responsibility among controllers, processors, and everything in between - the definition of actors and roles in directive 95-46 EC", "Computer Law and Security review", 2012, s. 25-43, af Brendan Van Alsenoy

”Persondataloven – gælder den også for advokater?”, ”Advokaten”, 22. september 2015, af advokat Jens Harskov Hansen. Link: <http://www.advokatsamfundet.dk/Service/Publikationer/Tidligere%20artikler/2015/Advokaten%207/Persondataloven.aspx>

Betænkninger:

Betænkning nr. 1342/1997: Behandling af personoplysninger, afgivet af udvalget om registerlovgivningen (Registerlovsudvalget). Link: <http://www.statensnet.dk/betaenkninger/vis.cgi?nummer=1345-1997>

Vejledninger:

”Udtalelse 1/2010 om begreberne "registeransvarlig" og "registerfører"”, vedtaget den 16. februar 2010 af Artikel 29-gruppen vedrørende databeskyttelse, (WP 169). Link: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_da.pdf

”Udtalelse 10/2006 om behandling af personoplysninger i Society for Worldwide Interbank Financial Telecommunication (SWIFT)”, vedtaget den 22. november 2006, (WP 128). Link: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp128_da.pdf

”Udtalelse nr. 5/2009 om internetbaserede sociale netværksaktiviteter”, vedtaget den 12. juni 2009 af Artikel 29-gruppen, (WP 163). Link: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_da.pdf

”Data controllers and data processors: what the difference is and what the governance implications are”, vejledning udstedt af Information Commissioner’s office (ICO, britisk datatilsyn), 20140506

Version: 1.0, kan revideres løbende. Link: <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>

“Are you a "data controller"?", vejledning udstedt af The Office of the Data Protection Commissioner, An Coimisinéir Cosanta Sonraí (det irske datatilsyn). Link: <https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm>

”De advokatetiske regler”, Advokatsamfundet, fra 1. november 2016. Link: <http://www.advokatsamfundet.dk/Advokatregulering/ReglerOgVedtaegter/Alle%20regler.aspx>

Databeskyttelsesforordningen – tidsplan for vejledninger”, udstedt af Justitsministeriet. Link: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/plan_for_vejledninger_om_forordningen.pdf

Bilag 1 – Mail fra Datatilsynet d. 11. maj 2017

Ved e-mail af 20. marts 2017 og telefonsamtale af 3. maj 2017 har du stillet forskellige spørgsmål vedrørende, hvornår Datatilsynet anser en advokat for at være dataansvarlig og databehandler.

I den forbindelse kan Datatilsynet generelt henvise til vores hjemmeside, hvor der findes bidrag til at vurdere, hvornår man henholdsvis er dataansvarlig eller databehandler.

<https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/>

Datatilsynet kan endvidere henvise til Lov om behandling af personoplysninger med kommentarer s. 165-167, hvor du ligeledes vil finde bidrag til vurderingen af, hvad der forstås ved begreberne dataansvarlig og databehandler. Det fremgår bl.a. heraf at:

"[...] Det samme vil efter omstændighederne kunne være tilfældet, når den dataansvarlige overlader personoplysninger til f.eks. en advokat eller revisor med henblik på, at denne skal rådgive, jf. herved også den ovennævnte sag, j.nr. 2000-219-0019. Sådanne forhold bør betragtes på den måde, at repræsentanten behandler personoplysningerne *for den dataansvarlige*, dvs. at repræsentanten kan behandle personoplysningerne i samme omfang, som den dataansvarlige."

Datatilsynet tidligere har udtalt i ovennævnte sag vedrørende inkasso, at der er tale om en overladelse af personoplysninger til en databehandler, når en virksomhed overlader oplysninger til et inkassobureau, der alene anvender oplysningerne i forbindelse med en arbejdsopgave for virksomheden. Kopi af sagen med j.nr. 2000-219-0019 vedhæftes.

Se endvidere Lov om behandling af personoplysninger med kommentarer s. 154-155 om begreberne "videregivelse" og "overladelse".

Konkret vedrørende dine spørgsmål om advokater kan tilsynet oplyse, at Datatilsynet i en enkelt sag har lagt til grund, at et advokatkontor var ansvarlig for tilmelding af oplysninger om navn og adresse til abonnement på oplysninger fra CPR (via Datavagten).

Det bemærkes dog, at afgørelsen ikke er et udtryk for Datatilsynets stillingtagen til spørgsmålet om dataansvarlig, idet tilsynet lagde advokatkontorets oplysninger herom til grund.

Afgørelsen kan ses her:

<https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/klage-over-behandling-af-personoplysninger-i-datavagten/>

Artikel 29 gruppen har også lavet et dokument om dataansvarlige og databehandlere. Dokumentet kan findes her:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Endelig kan Datatilsynet henvide til Information Commissioner's Office's bidrag til vurderingen af spørgsmålet via følgende link:

<https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>

Datatilsynet håber hermed at have besvaret din henvendelse. Hvis du har yderligere spørgsmål, er du velkommen til at kontakte undertegnede.