Databehandleren
i nugældende og fremtidig persondataret

The Data Processor
in present and future data protection law

af KASPER BILDE NIELSEN

Persondataretten er særlig relevant at beskæftige sig med i denne tid, idet vi befinder os i en overgangsperiode mellem den danske lovgivning, der dels baserer sig på den ældre registerlovgivning samt direktiv 95/46/EF, og den nye supranationale persondataforordning (EU) 2016/679.

Specialet er afgrænset til at behandle persondataretlige spørgsmål i relation til databehandleren, idet de i praksis mødte problemstillinger ofte koncentrerer sig om denne aktør. Af samme grund er specialet skrevet med det mål for øje, at dets praktiske anvendelighed skulle være i hovedsædet, hvilket i undertegnedes optik gør specialet særligt velegnet til at blive bragt i Rettid.

Med udgangspunkt i den danske retstilstand analyseres bestående udfordringer i relation til databehandleren, ligesom det vurderes, hvorvidt forordningen på det foreliggende grundlag imødegår disse.
Herunder behandles blandt andet og helt basalt den tvivl i retsanvendelsen, der består i grænsedragningen mellem den dataansvarlige og databehandleren.
Videre behandles det kontraktretlige forhold mellem den dataansvarlige og databehandleren, der kan vise sig særdeles vanskeligt at kontrollere via databehandleraftalen og den pligtige instruks, når parternes indbyrdes 'styrkeforhold' ikke er i balance.
Den teknologiske udvikling og leverandørernes fortsat større specialisering har medført, at databehandleren ofte gør brug af såkaldte underdatabehandlere, hvilket næppe kan siges at lette ansvaret og dets praktiske håndtering. Ofte involverer behandlingen af persondata et helt net af aktører spredt over flere lande, herunder tredjelande. Cloud-computing er et godt eksempel på, hvor hurtigt en simpel behandling kan ske at krydse grænser. Jo lettere behandlingen af data gøres qua den teknologiske udvikling, desto lettere er det også at overse sådanne afledte effekter, hvilket specialet fremhæver flere praktiske eksempler på.
Specialet belyser tillige, at forordningens forøgede fokus på aktørernes ansvar og videreførelse af flere af direktivets værktøjer i høj grad forekommer velbegrundet, men også at ikke alle bestående udfordringer er løst, ligesom nye er stødt til.
Særligt forpligtelserne til at foretage løbende selvjustits, dokumentere og samarbejde med tilsynene samt opfyldelsen pligterne over for de registrerede kan lægge beslag på ikke ubetydelige ressourcer hos databehandleren. Det er en af specialets anbefalinger, at sådanne spørgsmål proaktivt håndteres gennem parternes kontraktforhold.
Hidtil har den dataansvarlige og databehandleren gennem deres kontraktforhold også haft mulighed for at indskrive ansvarsbegrænsningsklausuler gældende i deres indbyrdes forhold. Forordningens forøgede fokus på at sikre de registrerede oprejsning via den solidariske hæftelse blandt de ansvarlige og særligt deres ret til efterfølgende at gøre regres ifølge artikel 82, stk. 5 synes imidlertid at udelukke sådanne klausulers videreførelse, hvilket næppe synes at have klare grunde for sig.

Indholdsfortegnelse

Resumé (eng.)

The ways of processing data have changed over time – so have the challenges for the current data protection law. The development in technology has created new forms of data processing, which has brought new parties into the processing, e.g. cloud computing. To make things further challenging, these additional data processers can be underlying contracting parties to another processor, and/or be established in third countries due to the globalization and the easy ways of transferring data made by the Internet. Current EU data protection law is based upon Directive 95/46/EF, which is repealed with effect from 25th of May 2018 due to the new Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR). The focus of this thesis is data processors and which problems there might exist in relation to them, and if and how these problems will be solved by the GDPR. The analysis has pointed out, that the definition of data processors are similar between the Directive and the GDPR, but special services can lead to different application of law between member states. The European Data Protection Board under the GDPR should solve this due to its importance for dividing liability and obligations between the parties. Under the directive the use of underlying data processors was not regulated separately, which is changed with the GDPR. This leads to clear lines between the data controller, the data processor and the data processors underlying data processor with regard to responsibility. The objectives and principles of the Directive remain sound in the GDPR, but one of the main innovations is the more severe responsibility and sanctions, which serve as a lifting bar for the data controller and data processor's incentives to keep up their obligations, hereunder the documentation for the processing and the appropriate level of security. A surprise is the apparently eliminated possibility for the data processor to limit his liability in the internal relationship to the data controller.

Afsnit 1 Indledning og problemformulering

I informationssamfundet anvendes nutidens teknologi som en helt integreret del af hverdagen. At være ansat hos en arbejdsgiver, være i kontakt med den offentlige sektor, handle på internettet, benytte sociale medier, tjekke e-post eller tage et billede og gemme det i 'skyen', er alle aktiviteter, der på hver sin måde involverer elektronisk behandling af personoplysninger.

De færreste af os tænker imidlertid over den bølge af underliggende behandlingsaktiviteter, f.eks. opbevaring, brug eller overførsel, som disse helt almindelige gøremål kan indebære.

Sådanne underliggende behandlingsaktiviteter har historisk været udført internt i den enkelte organisation, forudsat at aktiviteterne overhovedet har været teknisk mulige. Sådan er det ikke i dag, hvor den teknologiske udvikling har foranlediget så mange forskellige former for elektronisk databehandling som led i moderne virksomhedsdrift, at hensynet til effektiv ressourceanvendelse ofte nødvendiggør anvendelsen af en række forskellige databehandlere. Når den dataansvarlige, som kendetegnes ved at fastsætte formål og hjælpemidlerne til behandlingen, ikke selv kan overkomme samtlige behandlingsaktiviteter, uddelegeres opgaverne i dag almindeligvis til specialiserede databehandlere, som hver inden for deres felt foretager behandling på den dataansvarliges vegne. Dette kan være systemunderstøttende tjenester udført af EDB-servicebureauer eller mere enkeltstående tjenester, f.eks. markedsføringsaktiviteter, revisor- og advokatrådgivning.

Ofte overlader databehandleren flere af de ham påhvilende opgaver til såkaldte underdatabehandlere. Situationen opstår f.eks. ved anvendelsen af helt almindelige hjælpemidler som tekstbehandlings-, e-mail eller lagringsprogrammer med cloud-baseret teknologi. Cloud-computing kan rejse særlige persondataretlige spørgsmål, idet der gennem underdatabehandlere lagres data via inter-

nettet på store servere og datacentraler, som f.eks. grundet strømprisen kan være placeret i et tredjeland.[1] Der forekommer i praksis eksempler på, at dataansvarlige og databehandlere i sådanne tilfælde har overset brugen af (under)databehandlere, hvilket udgør en faldgruppe.[2]

Ovennævnte eksempler på behandlingsaktiviteter gør det let at forestille sig, at den enkelte dataansvarlige har et stort netværk af databehandlere og underdatabehandlere 'under' sig. De mange og vidt forskellige behandlingsformer og –konstruktioner er ikke uden risici for de registrerede.[3] [4] Hensynet til beskyttelsen af de registreredes interesser, herunder deres integritet, begrunder, at der i lovgivningen opstilles visse grænser for, hvordan og i hvilket omfang den dataansvarlige kan lade personoplysninger behandle.

Den nuværende regulering følger af Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 (persondatadirektivet, i det følgende direktivet) implementeret ved lov om behandling af personoplysninger nr. 429 af 31. maj 2000 med efterfølgende ændringer (persondataloven, i det følgende 'PDL').[5]

Direktivet omtaler ikke direkte brugen af underdatabehandlere, herunder forholdet mellem dem og den dataansvarlige hhv. databehandleren. Da der ikke foreligger en fast juridisk ramme i form af regler, der særligt tager sigte på underdatabehandleren, har det hidtil været de almindelige regler for databehandlere, som har fundet anvendelse.

PDL § 42 kræver af den dataansvarlige, at denne sikrer og påser, at databehandleren formår at træffe visse sikkerhedsforanstaltninger. Det er derfor vigtigt for den dataansvarlige at have kontrol over sine databehandlere – og underdatabehandlere.

Måden, hvorpå denne kontrol sikres, er primært et kontraktligt anliggende. Midlerne er kontrakten om den ydelse, som databehandleren skal præstere, samt den lovpligtige instruks og databehandleraftale. Med den dataansvarliges overordnede ansvar synes den retlige regulering at forudsætte, at den dataansvarlige rent faktisk er i stand til at styre og kontrollere databehandleren. Dette er ikke nødvendigvis tilfældet i praksis. Selvom private behandlinger i de fleste tilfælde tager afsæt i den dataansvarliges interesse og initiativ, og at den dataansvarlige frit kan vælge mellem databehandlere, er det ofte databehandleren, som præsenterer sin egen databehandleraftale. Den dataansvarliges accept af sådanne aftaler kan skyldes, at databehandleren er så mange gange større end den dataansvarlige, at databehandleraftalens indhold slet ikke står til forhandling. Sidstnævnte antages at være tilfældet for store edb- og softwareleverandører, hvor den dataansvarlige nødtørftigt må acceptere indholdet af den fortrykte databehandleraftale, såfremt den dataansvarlige ønsker

[1] Måden hvorpå nutidens datastrømme ikke lader sig begrænse af landegrænser og via den tilgængelige teknologi kan spredes hurtigt og til brug for mange formål betegnes i faglig sprogbrug som 'big data' jf. *Data Protection on the Move*, 2016, s. 165 f, citat: *"Big data as a phenomenon is enabled by new developments in distributed computing like cloud technology, allowing to deal with very large amounts of data at much higher speed. However, big data cannot be equated with these technologies or cannot be limited to these aspects of volume and velocity. It also implies qualitative changes in terms of what can be done with this data: a variety of structured and unstructured data source scan be much easier linked with each other and analysed in new ways"*.

[2] Datatilsynet har ved flere lejligheder forholdt sig til brugen af cloud-løsninger, herunder Odense Kommunes brug af Google Apps online kontorpakke (j.nr. 2010-52-0138), KL's overførsel af køreprøvesystem til en cloud-løsning (j.nr. 2011-631-0136) og IT-Universitetet i Københavns brug af cloud-løsning i Microsoft 365 (j.nr. 2012-54-0123/0124). Eksemplerne illustrerer vigtigheden af at være opmærksom på indholdet af de anvendte hjælpemidler.

[3] Jf. *Privacy and Legal Issues in Cloud Computing*, 2015, s. 35 ff.

[4] Jf. *Reforming European Data Protection Law*, 2015, 333 ff.

[5] Retten til beskyttelse af personoplysninger har ophav i TEUF art. 6, stk. 1, der bl.a. henviser til EU's charter om grundlæggende rettigheder (charteret). Charterets art. 7 og 8 overlapper begge delvis retten til respekt for privatlivet i EMRK art. 8, stk. 1.

databehandlerens ydelse. Dette kan give anledning til problemer for parterne, når aftalen ikke lever op til de gældende krav.

Den danske persondatalovgivning befinder sig midt i en overgangsperiode, idet Europa-Parlamentet og Rådets Forordning (EU) 2016/679 af 27. april 2016 (persondataforordningen, i det følgende forordningen) erstatter direktivet og store dele af PDL, hvilket også får betydning for databehandleren.[6]

Forordningen gør fremadrettet reguleringen overstatslig.[7] Det ligger derfor også i forordningens natur, at medlemsstaterne ikke må opretholde national lovgivning, der er i modstrid med forordningen, medmindre der undtagelsesvis skulle være hjemmel herfor i anden ikke lavererangerende lovgivning.[8] Det er således givet, at den danske persondatalov ikke kan opretholdes med sit nuværende indhold, når forordningen får virkning den 25. maj 2018 jf. dennes art. 94, stk. 1. Derpå er det relevant at stille spørgsmålet, hvordan direktivet og PDLs bestemmelser finder anvendelse på databehandleren og i hvilket omfang forordningen afstedkommer ændringer af betydning for dennes retsstilling, herunder også om de udfordringer og faldgrupper, der knytter sig til forholdet mellem den dataansvarlige og databehandleren under direktivet, f.eks. brugen af underdatabehandlere, er imødeset i forordningen.

Navnlig udsigten til forordningens væsentlig strengere ansvars- og sanktionsbestemmelser forekommer at have vakt de dataansvarlige og databehandlernes opmærksomhed. Spørgsmålet er således ikke alene, hvordan databehandlerens retlige forhold tager sig ud, men også af særlig relevans for denne afhandling, hvordan databehandleren bedst muligt kan agere i forholdet med den dataansvarlige og andre databehandlere efter den 25. maj 2018.

Afhandlingen vil på ovennævnte baggrund søge at besvare nedenstående styrespørgsmål, der samtidig tjener som afgrænsning:

---

[6] Begrundelserne for at forlade direktivet er flere. Direktivet er som sådan ikke forældet, hvilket også ses i forordningen, der i hovedsagen viderefører direktivet samt alle dets målsætninger og principper jf. forordningens præambel 9. Direktivet har imidlertid ikke formået at følge med tidens udvikling. Cloud- og internetteknologien er i vidt omfang produkter af en anden tid. Direktivet blev vedtaget i 1995 oven på en tilblivelsesproces over årene 1990-1995. At direktivet ikke tager højde for nutidens it og måder, hvorpå persondata kan behandles, forekommer forståeligt, når internettet i form af WEB 2.0, først i 2004 udviklede sig til dét, som vi kender i dag jf. Gyldendal, *Den Store Danske (online)*. Hertil kommer, at direktivet foreskrev uhensigtsmæssige procedurer, f.eks. anmeldelsessystemet, der ifølge forordningens præambel 89 har medført en administrativ og finansiel byrde, som ifølge EU-kommissionens Fact Sheet (01/2016) årligt koster erhvervslivet mere end 130 mio. €. Reguleringsformen, der med sine nationale særregler og dermed begrænsede gennemskuelighed og harmonisering, har tillige gjort det besværligt at behandle data på tværs af landegrænser, hvilket er aktualiseret med globaliseringen og den teknologiske udvikling. Hindringen har dermed udgjort en konkurrencefaktor i det ellers frie indre marked, som har afholdt nogle udbydere, medens andre har påtaget sig de forbundne omkostninger, og helt andre blot har set stort på reguleringen. Direktivet har ifølge forordningen ikke skabt tillid og respekt for databeskyttelse, idet ikke alle medlemsstater, herunder i Danmark, har håndhævet det på effektiv og afskrækkende vis.

[7] En forordning er almengyldig, bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat jf. TEUF art. 288, stk. 2. I modsætning til et direktiv skal en forordning for at få virkning derfor ikke implementeres i national ret, idet den allerede ved vedtagelsen har status som sådan. Som retligt instrument betegnes forordningen derfor også som supranational.

[8] Det følger af EU-praksis, at medlemslandene heller ikke må foretage gennemførelsesforanstaltninger af nogen art, således at der kan sås tvivl om forordningens EU-retlige ophav, medmindre det udtrykkeligt er tilladt i forordningen eller såfremt forordningens indhold har et så nært sammenspil med national ret, at gentagelser fra forordningen kan være nødvendige af hensyn til at skabe klarhed til gavn for reglernes adressater. jf. sag C-272/83, *Kommissionen mod Italien*, præmis 26-27.

- Hvilke særlige karakteristika kendetegner databehandleren og hvad er dennes retsstilling under direktivet?[9]
- Hvilke ændringer medfører forordningen og løser den de udfordringer, der under direktivet særligt består i relation til databehandleren?[10]
- Hvordan kan private databehandlere bedst muligt indrette sig efter forordningen og samtidig skabe balance i det interne forhold til den dataansvarlige?[11]

1.1 Juridisk metode, kilder og afgrænsning

Besvarelsen af ovennævnte spørgsmål nødvendiggør bevidsthed om den gældende danske retstilstand under direktivet, samt om de ændringer, som forordningen afstedkommer. Med henblik på at beskrive, fortolke og overskueliggøre gældende ret[12] både før og efter forordningens virkningstidspunkt, den 25. maj 2018, anvendes den retsdogmatiske analyse.

Analysen vil tage komparativ form de steder, hvor forordningen medfører relevante ændringer til retsstillingen under direktivet.

Afhandlingen vil gøre brug af henvisninger til klassisk juridisk litteratur, artikler samt praksis fra EU-domstolen og Datatilsynet.[13]

Da forordningen blev vedtaget 27. april 2016 og Justitsministeriets betænkning herom ikke var udkommet på tidspunktet for afhandlingens afsluttende redigering, men dog få dage forinden afleveringen, har udbuddet af fortolkningsbidrag ved siden af forordningens præambler og Artikel 29-gruppens enkelte vejledninger været begrænset. Betænkningen[14] har således ikke kunnet indarbejdes i forudsat omfang.

Med førnævnte styrespørgsmål er afhandlingen er søgt afgrænset til primært at fokusere på de forpligtelser, som databehandleren er i tættest berøring med, herunder særligt den dataansvarliges instruks og databehandleraftalen.

Afsnit 2 Databehandleren

2.1. Definition

For at forstå databehandlerens rolle og det retlige miljø, som denne navigerer i, er det væsentligt at gøre sig klart, hvem den dataansvarlige egentlig er. Særligt forholdet mellem den dataansvarlige og databehandleren begrunder, at disse personer klart kan adskilles fra hinanden, således at der ikke opstår tvivl om opgaver og ansvar i forhold til de registrerede.

---

[9] Definition, afgrænsning og eksempler på roller i behandlingen, som kan give anledning til tvivl, behandles i afsnit 2. I afsnit 3 gennemgås databehandlerens pligter samt forholdet til den dataansvarlige.

[10] Gennemgående i afsnit 2, 3 og 4 tages afsæt i det nugældende direktiv og PDL, hvorefter forordningens ændringer af hensyn til afhandlingens sammenhængskraft behandles specifikt i relation til de enkelte underafsnit. Af systematiske hensyn er bestående udfordringer tillige søgt identificeret og behandlet efter samme opbygning.

[11] Under beskrivelse af forpligtelserne i afsnit 3 gives flere steder konkrete forslag til, hvordan reglerne kan anvendes i praksis med henblik på ikke at aktualisere de under afsnit 4 beskrevne retsfølger, ligesom der i afsnit 5 på mere overordnet vis konkluderes, hvordan forordningen kan og bør imødekommes.

[12] Begrebet, gældende ret, de lege lata, anvendes som betegnelse for det resultat, som domstolene ved retskildernes anvendelse og den retsdogmatiske analyse må forventes at komme frem til i afgørelsen af tvister jf. *Retskilder og retsteorier*, 2011, side 29.

[13] Inddragelsen af publikationer fra private brancheorganisationer samt professionelle rådgivningsvirksomheder er søgt minimeret, idet sådanne *kan* bære subjektivt eller ideologisk præg, eller være båret af kommercielle interesser.

[14] JM's bet. nr. 1565 af 24. maj 2017.

I det følgende defineres databehandleren med udgangspunkt i direktivet og PDL, hvorefter det analyseres, i hvilket omfang forordningen medfører ændringer.

2.1.1. Direktivet

Ifølge PDL § 3, nr. 5 forstås ved databehandleren, citat: "*den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne*". [15]

Når der sker behandling af personoplysninger på vegne af den dataansvarlige, er der tale om *overladelse* af oplysninger i modsætning til videregivelse.[16] Databehandleren kendetegnes derfor særligt ved, at de overladte oplysninger behandles efter den dataansvarliges instruks.

Beslutter den dataansvarlige at lade en behandlingsaktivitet udføre internt af dennes egne medarbejdere, anses medarbejderne ikke for databehandlere, men derimod fortsat som en integreret del af den dataansvarlige, idet databehandleren – foruden at handle på den dataansvarliges vegne – også skal være en retligt selvstændig enhed i forhold til den dataansvarliges organisation.[17] Sagt med andre ord kommer databehandleren således i spil, når den dataansvarlige helt eller delvist uddelegerer behandlingen.

Selvom databehandleren handler og optræder i eget sted, bliver han identificeret med den dataansvarlige fsva. den behandlingshjemmel, som i første omfang giver den dataansvarlige adgang til at behandle oplysningerne, herunder at lade dem indsamle. Databehandlerens frihed er imidlertid begrænset af parternes kontrakt om den ydelse, som databehandleren skal præstere, samt databehandleraftalen og ikke mindst instruksen. Grænsen for, hvad den dataansvarlige kan bemyndige databehandleren til, markeres af grænserne for den dataansvarliges egen behandlingshjemmel.

2.1.2. Forordningen

Definitionen af databehandleren ses grundlæggende videreført i forordningens art. 4, nr. 8[18], hvorfor der ikke umiddelbart er teknisk forskel på, hvem der forinden og efter forordningens virkningstidspunkt er at betragte som databehandlere.

Dette medfører, at den udviklede fortolkningspraksis under direktivet som udgangspunkt fortsat er anvendelig. Da fortolkningen af direktivet – ligesom forordningen – i første omgang primært har været og er et nationalt anliggende, og den nationale anvendelse af bestemmelserne kun sjældent forelægges EU-domstolen, kan det imidlertid ikke udelukkes, at der under direktivet kan være udviklet forskellige nationale fortolkninger, f.eks. om advokaten som databehandler jf. nedenfor. Den såkaldte sammenhængsmekanisme ifølge forordningens art. 63 ff., der rummer målsætningen om et nært samarbejde mellem nationale tilsynsorganer, Kommissionen og Databeskyttelsesrådet

[15] Bestemmelsen implementerer direktivets art. 2, litra e, der på tilsvarende vis definerer 'registerføreren', hvormed i nutidig juridisk sprogbrug forstås 'databehandleren', idet der i bet. nr. 1345/1997, s. 210 og *Nødvendig behandling af personoplysninger*, 2007, s. 32, note 42 tilkendegives, at begreberne skal forstås synonymt.

[16] Om begrebet 'overladelse' henvises til Dt's årsberetning 2000, s. 20 hvorefter citat: "*Udtrykket "overførsel" omfatter ud over videregivelse af oplysninger også overladelse, hvorved forstås overførsel af oplysninger til en databehandler eller personer under databehandlerens direkte myndighed. Endelig omfatter udtrykket den dataansvarliges interne anvendelse af oplysninger.*". I samme retning bet. nr. 1345/1997, s. 283-284, hvorefter videregivelse anføres at rumme mere end overførsel til en databehandler under henvisning til den engelske oversættelse, 'transfer'.

[17] jf. Artikel 29-gruppens udtalelse 1/2010, WP169, s. 27.

[18] Citat: "*en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne*".

(dav. 'Artikel 29-gruppen' under direktivet), kan formentlig ses som en målsætning om og tilskyndelse til, at medlemsstaternes regelanvendelse tilnærmes, uden at EU-domstolen nødvendigvis skal inddrages. I den sammenhæng kan det ikke udelukkes, at nationale tilsyn må ændre fortolkning, således at retsstillingen i den enkelte medlemsstat praktisk kan *forekomme* ændret under forordningen.

2.2. Afgrænsning over for den dataansvarlige

Både PDL under direktivet, og forordningen, pålægger den dataansvarlige og databehandleren selvstændige pligter. Pligterne og ansvaret for reglernes overholdelse er forskellige og det er derfor væsentligt at være opmærksom på grænsen, hvorved databehandleren selv bliver dataansvarlig.

Ifølge PDL § 3, nr. 4 forstås ved den dataansvarlige, citat: *"den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger"*.[19]

I hovedsagen anvender forordningens art. 2, nr. 7 samme definition, idet eneste forskel er ændringen fra direktivets 'hvilket formål' til 'hvilke formål', hvormed tilkendegives, at der for behandlingen kan være tale om flere af hinanden uafhængige og legitime formål.[20]

De oplysninger, som databehandleren f.eks. behandler om egne medarbejdere, herunder fagforeningsmedlemsskab[21], medfører, at databehandleren stort set altid også vil være dataansvarlig – dette blot i andre og for databehandleropgaven uvedkommende henseender.[22] [23]

Sondringen mellem den dataansvarlige og databehandleren har først og fremmest betydning derhen, at det som hovedregel er den dataansvarlige, som er ansvarlig for, at behandlingen overholder PDL hhv. forordningen, herunder at den er lovlig via den anvendte behandlingshjemmel. Dette ses bl.a. ved ansvarsbestemmelserne i PDL § 69 og forordningens art. 82, foruden forordningens fremhævede princip om ansvarlighed i art. 5, stk. 2.

Det er tillige den dataansvarlige, som under anmeldelsesordningen i PDL § 48 ff. skal anmelde og i visse tilfælde indhente Datatilsynets forudgående tilladelse, og under forordningen foretage den såkaldte konsekvensanalyse (data protection impact assessment) jf. art. 35 og i visse tilfælde høre og afvente tilsynsmyndigheden forinden behandlingens iværksættelse jf. art. 36.

Derudover er det den dataansvarlige, som er ansvarlig for at imødekomme de registreredes rettigheder, herunder dels i form af den information, der skal meddeles af egen drift, samt dels ved opfyldelse af anmodninger om indsigt, sletning, blokering/begrænsning, berigtigelse, indsigelse m.v. ifølge PDL og i videre omfang forordningen.[24]

---

[19] Bestemmelsen implementerer direktivets art. 2, litra d, der på tilsvarende vis definerer 'den registeransvarlige', hvormed i nutidig juridisk sprogbrug forstås 'den dataansvarlige'.

[20] Forordningens art. 5, stk. 1, litra b understøtter fravigelsen af princippet om formålsbegrænsning (finalité-princippet), idet behandling kan ske i andre formål, når disse ikke er uforenelige med det oprindeligt angivne formål jf. fremgangsmåden for viderebehandling i art. 6, stk. 4.

[21] Se *Persondataret i ansættelsesforhold,* 2011, s. 49.

[22] Artikel 29-gruppens udtalelse 1/2010, WP169, s. 27 udtrykker således, citat: *"Rollen som registerfører stammer desuden ikke fra arten af en enhed, der behandler oplysninger, men fra dennes konkrete aktiviteter i en bestemt sammenhæng*".

[23] Se også Dt j.nr. 2005-632-0077.

[24] Særligt forordningens ret til dataportabilitet i art. 20 samt 'retten til at blive glemt' (sletning) i art. 17 fremstår som en udvidelse, selvom det for sidstnævnte kan bemærkes, at denne ret langt fra er ubetinget jf. undtagelserne i art. 17, stk. 3.

Såfremt databehandleren ønsker at viderebehandle oplysninger til andet formål end dét, som denne er instrueret i at varetage på den dataansvarliges vegne, skal databehandleren herefter som dataansvarlig selvstændigt opfylde førnævnte forpligtelser, herunder kravet om behandlingshjemmel, foruden at oplysningerne såvel retligt som praktisk skal kunne indsamles lovligt. Problematikken aktualiseres let i praksis, f.eks. når databehandleren har fuldført den opgave, der begrundede adgangen til personoplysningerne, og herefter ikke sletter eller tilbagegiver oplysningerne[25], men derimod fortsætter opbevaringen eller viderebehandler dem. Oplysningerne bliver næppe databehandlerens egne af den grund, at databehandleren måtte have hjemmel til at behandle dem som dataansvarlig, idet det ikke er givet, at den oprindeligt dataansvarlige kan eller vil strække sin hjemmel til at videregive oplysningerne i dette formål, ligesom hensynet til den registreredes integritet også kan tale imod.

Er det anderledes en forudsætning, at den dataansvarlige ikke længere skal have rådighed over oplysningerne og at 'databehandleren' (modtageren) skal behandle dem i egne formål, vil denne anses som tredjemand og dermed ny dataansvarlig.[26]

Direktivet og PDL nævner ikke direkte muligheden for et delt dataansvar, selvom Artikel 29-gruppen[27] og Datatilsynet i få tilfælde har anerkendt dette.[28] Forordningens art. 26 er klarere på dette punkt, idet der hjemles et fælles dataansvar, når flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til en behandling – f.eks. en hotelkæde, et flyselskab og et rejsebureau, som sammen beslutter sig for at forfølge den fælles interesse i at administrere en samlet ordning, der formår at tiltrække turister til en bestemt egn af verdenen.

For de registrerede rummer det delte dataansvar den ulempe, at gennemskueligheden mindskes og at det kan forekomme vanskeligt at udøve de tildelte rettigheder, men også den fordel, at der er flere solidarisk hæftende for behandlingen jf. art. 82, stk. 4, hvorved skyldsspørgsmålet har fået en tilbagetrukket rolle.

Det må antages, at databehandleren godt kan rådgive den dataansvarlige og i et vist omfang hjælpe med at vælge de mest hensigtsmæssige behandlingsmidler, men er realiteten dén, at 'databehandleren' i fællesskab med den dataansvarlige *bestemmer* formålene med og/eller hjælpemidlerne til behandlingen, typisk fordi at dette er i begge parters interesse, vil der være tale om et delt dataansvar.[29]

2.3. Teorien i praktisk kontekst

Det bemærkes, at databehandleren både kan være en fysisk eller juridisk person. En gennemgang af Datatilsynets afgørelser afslører dog, at databehandleren som regel vil være en juridisk person i den private sektor. Hermed udelukkes ikke, at en offentlig myndighed kan være databehandler. Dette forudsætter imidlertid, at myndigheden udelukkende behandler oplysninger på vegne af en

[25] Ifølge forordningens art. 28, stk. 3, litra g skal den dataansvarlige som noget nyt i databehandleraftalen vælge, om oplysningerne skal tilbageleveres eller slettes efter endt behandling.
[26] Jf. *Lov om behandling af personoplysninger*, 2015, s. 166.
[27] Jf. Artikel 29-gruppens udtalelse 1/2010, WP169, s. 24.
[28] F.eks. Dt's j.nr. 2007-212-0042, *FDB og Coop Danmark A/S' medlemsprogram*, hvor der citat: *"[lægges] til grund, at medlemsprogrammet skal drives i en enhed, som organisatorisk er forankret i begge virksomheder. Datatilsynet kan herefter tiltræde, at behandlingen af oplysningerne i det nye medlemsprogram sker med fælles dataansvar mellem FDB og Coop. Tilsynet forudsætter herved, at der foreligger klare retningslinjer og instruktionsbeføjelser for så vidt angår behandlingen af oplysningerne, og at de registrerede kan gøres deres rettigheder gældende over for begge dataansvarlige virksomheder*".
[29] Af Artikel 29-gruppens udtalelse 1/2010, WP169, s. 26, fremgår citat: *"Uddelegering kan dog stadig skabe en vis grad af frihed i forhold til, hvordan den registeransvarliges interesser bedst opfyldes, hvilket giver registerføreren mulighed for at vælge de mest velegnede tekniske og organisatoriske hjælpemidler*".

dataansvarlig, hvorfor man antageligt lettest forestiller sig scenariet som led i borgerservice eller et myndighedssamarbejde, hvor der ikke er tale om et delt dataansvar.

Eksemplerne på databehandlere rummer de tilfælde, hvor der behandles personoplysninger på vegne af andre. Der kan f.eks. være tale om uddelegering af administrative opgaver som lønudbetaling, bestilling af arbejdsbeklædning, medarbejderudvikling og -uddannelse, eller rekruttering til ledige stillinger. Mere markedsorienteret kan der f.eks. også være tale om markedsføringsydelser, drift og vedligeholdelse af hjemmesider, herunder e-handelsløsninger, eller udviklingen af helt nye it-systemer.

Følgelig skildres konkrete eksempler på databehandlere, ligesom der peges på særlige situationer, der grundet de faktiske omstændigheder kan give anledning til fortolkningstvivl.

2.3.1. EDB-servicebureauer

EDB-servicebureauer forekommer at være typeeksemplet på en databehandler. Begrebet har i Danmark en særlig historisk betydning, idet der forud for PDL fandtes lov om private registre § 20, der indeholdt definitionen på et edb-servicebureau[30], og som i forarbejderne til PDL blev anset for at svare til definitionen af en databehandler.[31]

Som edb-servicebureau anses virksomheder, der varetager praktisk databehandling for andre eller f.eks. udbyder systemunderstøttende tjenester.

Driver databehandleren udelukkende virksomhed med det formål at udøve edb-service i kommercielt og erhvervsmæssigt sigte og udbydes denne driftsafvikling af databehandlinger på almindelige markedsvilkår[32], skal der forinden behandlingens påbegyndelse foretages anmeldelse til Datatilsynet jf. PDL § 53.[33] Fritaget for anmeldelse er således edb-service, der udbydes som biaktivitet eller som alene eksisterer ved, at f.eks. flere offentlige myndigheder benytter et kun for dem tilgængeligt bureau.

At en databehandler, som udøver edb-servicevirksomhed som biydelse, f.eks. som led i softwareudvikling, ikke skal foretage anmeldelse til Datatilsynet, medfører ikke, at vedkommende ikke anses for databehandler, eller at der i øvrigt er forskel på anmeldelsespligtige og ikke-anmeldelsespligtige databehandleres forpligtelser ifølge PDL.

2.3.2. Rådgivere, herunder advokater

Rådgivere og konsulenter inden for de liberale erhverv vil hyppigt behandle personoplysninger som led i varetagelsen af klienternes interesser. Revisions- og advokatvirksomheder er gode eksempler herpå, hvorfor fokus i det følgende rettes mod advokaten.

---

[30] Lov om private registre § 20, citat: ”*virksomheder, der for tredjemand, herunder for en offentlig myndighed, udfører elektronisk databehandling af oplysninger som nævnt i § 1, skal forinden foretage anmeldelse til registertilsynet. Stk. 2. Virksomheden må ikke uden samtykke fra ejeren af registeret anvende de modtagne oplysninger i andet øjemed end til udførelsen af den opgave, aftalen vedrører, eller lade oplysningerne opbevare eller bearbejde hos andre eller i udlandet*”.

[31] Jf. *Lov om behandling af personoplysninger*, 2015, side 164.

[32] Jf. Dt’s anmeldelsesblanket, *EDB-servicebureau*, samt *Lov om behandling af personoplysninger,* 2015, s. 611.

[33] Ifølge Dt’s vejledning, *EDB-servicebureauer*, af 06.05.2015, fremgår citat: ”*Efter Datatilsynets praksis er der kun anmeldelsespligt efter [PDL] § 53, hvis der er tale om en egentlig edb-servicebureauvirksomhed, dvs. hvor dette er virksomhedens egentlige formål. Hvis virksomheden tillige udøver andet erhverv end edb-servicevirksomhed, er der efter Datatilsynets opfattelse som udgangspunkt ikke anmeldelsespligt. Der er således efter Datatilsynets praksis f.eks. ikke anmeldelsespligt efter [PDL] § 53, hvis virksomheden også udvikler software*”.

Med udgangspunkt i ovennævnte definition vil det være muligt at anse advokaten som databehandler for de oplysninger, han får overladt af klienten til brug for sin varetagelse af klientens interesser, og som selvstændig dataansvarlig for de nødvendige oplysninger, der indsamles om klienten som led i opfyldelsen af kontrakten med denne, eller som det f.eks. efter hvidvaskningsloven påhviler advokaten at indhente.[34]

Der er imidlertid tale om et på EU-plan teoretisk omtvistet spørgsmål.

Det britiske datatilsyn, ICO, anser advokaten for generelt dataansvarlig, da advokaten er "herre over" egen rådgivning og er pålagt særlige forpligtelser i relation til denne, herunder dokumentation og fortrolighed.[35] Argumentet er herefter, at klienten ikke kan give advokaten instrukser i, hvordan advokaten skal udføre sit opdrag, herunder behandlingen af personoplysninger. Artikel 29-gruppen[36] synes fsva. procederende advokater at støtte op om ICO's opfattelse.[37]

Imod at anse advokaten for generelt dataansvarlig kan det formentlig indvendes, at det i mange sagstyper, herunder inddrivelsessager, trods alt er klienten, som vælger at gøre brug af advokaten, vel vidende at der for advokatens bistand gælder særlige forhold. Her står det klienten frit at ophæve samarbejdet med advokaten og vælge en anden, hvorefter advokaten følgelig ikke bør fortsætte, f.eks. inddrivelsen, *uden* sin klients mandat.

I bl.a. inddrivelsessager, hvor klienten er styrende for behandlingen, synes det således ikke ubegrundet at anse advokaten som databehandler for de oplysninger, som klienten kan behandle efter interesseafvejningsreglen PDL § 6, nr. 7 hhv. forordningens art. 6, stk. 1, litra f. Denne konklusion understøttes af Datatilsynets vejledning af 06.05.2015, *'Hvornår er man henholdsvis dataansvarlig og databehandler?'*, hvorefter citat: *"…en databehandler kan være et inkassobureau, som overlades oplysninger fra en dataansvarlig med henblik på inddrivelse af gæld for den dataansvarlige*".[38]

---

[34] Opfattelsen har støtte i dansk teori af Jens Harkov Hansen i Advokaten nr. 7 2015, *Persondataloven – gælder den også for advokater?*, samt af Waaben et al. i *Lov om behandling af personoplysninger*, 2015, s. 165.

[35] ICO vejledning, *Data controllers and data processors*, 2014, s. 12-13.

[36] Artikel 29-gruppen er en hyppigt anvendt betegnelse for den gruppe vedr. beskyttelse af personer i forbindelse med behandling af personoplysninger, som bl.a. består af repræsentanter fra medlemsstaternes tilsyn, og i medfør af direktivets art. 29 er nedsat til bl.a. at undersøge ethvert spørgsmål vedrørende EU-medlemsstaternes anvendelse af de nationale bestemmelser, som implementerer direktivet. Gruppen er uafhængig og har alene rådgivende beføjelser over for medlemslandene, herunder mulighed for at vejlede og afgive henstillinger med henblik på at søge harmonisering i direktivets implementering og anvendelse. Ikke desto mindre er gruppens udtalelser og publikationer relevante fortolkningsbidrag til forståelsen af direktivet jf. bl.a. Martin Gräs Lind i *Medarbejderes integritetsbeskyttelse i dansk ret*, 2006, s. 306.

[37] Se Artikel 29-gruppens udtalelse 1/2010, WP169, s. 29, om advokaten citat: *"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" ved behandlingen af oplysninger under den juridiske repræsentation af deres klienter.*" og om den mere modificerede tilgang til revisoren citat: *"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 denne dog generelt om ikke en almindelig medarbejder så registerfører pga. instruksernes klarhed og det konsekvente begrænsede omfang af frihed. Dette er dog med forbehold af ét større forbehold, idet de, hvis de finder, at der er givet vildledende oplysninger, som de har pligt til at rapportere, pga. deres professionelle forpligtelser handler selvstændigt som registeransvarlige*".

[38] Ifølge *Lov om behandling af personoplysninger*, 2015, s. 164, er antagelsen lagt til grund i Dt's j.nr. 2000-219-0019.

Retsstillingen er dog omtvistelig og Artikel 29-gruppens opfattelse vil formentlig trække stærkt i modsatte retning, såfremt spørgsmålet forelægges EU-domstolen.

Det må dog erindres, at advokater og juridiske rådgivere varetager mange forskellige funktioner. Hvor inddrivelsesopgaver i høj grad varetages *for* klienten i tæt sammenspil med denne, vil f.eks. kuratoren have en noget anderledes og mere selvstændig rolle, idet han bl.a. overtager fallentens rådighed som led i sin varetagelse af boets afvikling med henblik på kreditorernes fyldestgørelse. Såfremt kurator ikke blot anses for dataansvarlig, vil der formentlig opstå en vanskelig rollefordeling mellem boets parter, herunder særligt kurator, skifteretten, kreditorerne etc. – hvem har i så fald ansvaret og hvad med instruksen og databehandleraftalen?

Overvejelserne bør nok være, om det i sagens natur er hensigtsmæssigt at se på advokaten uden hensyntagen til den konkrete funktion, der varetages. Såfremt retsstillingen anskues mere nuanceret, kan det videre overvejes, om den inden for EU ikke umiddelbart modstridende definition af databehandleren, som dog forekommer uens anvendt på faktum, overhovedet dækker over en modstridende forståelse af retsstillingen eller om der nærmere er tale om, at *for* mange funktioner er søgt omfattet af samme begreb med en ufyldestgørende konklusion som følge.

Forordningen løser ikke direkte spørgsmålet, men det må forventes, at det forøgede fokus på ensartet regelanvendelse og samarbejde mellem nationale tilsynsmyndigheder vil foranledige Databeskyttelsesrådets stillingtagen til sådanne videreførte uklarheder.

2.3.3. Udbydere af internetbaserede tjenester

2.3.3.1. Søgemaskineudbydere

EU-domstolen har i 2014 taget stilling til søgemaskineudbyderes retlige kvalificering og vurderede, at der er tale om dataansvarlige (registeransvarlige).[39]

Begrundelsen er, at søgemaskineudbyderen både fastsætter formålet med og hjælpemidlerne til den aktivitet, der består i at drive søgemaskinen, og dermed også formålene med og hjælpemidlerne til behandlingen. Domstolen fastslår i tilknytning hertil, at begrebet registeransvarlig er bredt og at det vil være ordlyds- og formålsstridigt, såfremt søgemaskineudbyderen ikke ansås for ansvarlig, uanset at søgemaskineudbyderen ikke har indflydelse på hvilke personoplysninger, der offentliggøres på tredjemands websider.

Om det faktum, at websideudbyderne via udelukkelsesprotokoller har mulighed for at angive over for søgemaskineudbyderen, at et bestemt indhold ikke ønskes delt via søgemaskinen, bemærker domstolen endvidere, at dette ikke ændrer på, at formålet og hjælpemidlerne fortsat besluttes af søgemaskineudbyderen.[40] Websideudbyderens påvirkning af det indhold, som søgemaskineudbyderen kan dele, kan alene have den virkning, at websideudbyderen og søgemaskineudbyderen kan ske at blive betragtet som fælles dataansvarlige alt afhængigt af omstændighederne.

Søgemaskineudbydere anses således *ikke* for databehandlere, hvilket bl.a. giver anledning til overvejelser i forhold til de forpligtelser, der består i imødekommelsen af de registreredes rettigheder.

[39] EU-domstolens afgørelse af 13.05.2014 i sag C-131/12, Google Spain SL, Google Inc. mod AEPD (Spanien), særligt præmis 32-41.

[40] Denne udtalelse og den brede forståelse af begrebet, den dataansvarlige, kan perspektiveres til førnævnte om advokaten, hvilket dermed understøtter Artikel 29-gruppes udtalelse.

2.3.3.2. Udbydere af hosting- og webhotel-løsninger

Ifølge Datatilsynet er en udbyder af et webhotel, der leverer websideløsninger til sine kunder, at anse for databehandler.[41] [42]

Der er tale om endnu et eksempel, hvor Artikel 29-gruppen ikke er enige i den danske fortolkning, eller måske snarere retsanvendelse. Artikel 29-gruppen anser hosting-udbyderen som dataansvarlig for de oplysninger, der offentliggøres af dennes kunder på den webside, som udbyderen hoster og vedligeholder. Foretages der udover at vedligeholde og stille websiden til rådighed yderligere behandling af oplysningerne til egne formål, vil hosting-udbyderen også anses for dataansvarlig i forhold til denne specifikke behandling.[43]

Lægger kunden f.eks. oplysninger om sine medarbejdere ud på hjemmesiden, må det dog antages, at der er tale om et fælles dataansvar.

Da Det Europæiske Databeskyttelsesråd under forordningen overtager den rolle, som Artikel 29-gruppen havde fået under direktivet, og samtidig får til opgave at føre tilsyn med forordningens anvendelse samt adgang til at udstede retningslinjer, henstillinger og bedste praksis jf. art. 70, stk. 1, bliver det interessant at følge, hvordan disse uforenelige fortolkninger konkret vil blive løst i praksis. Indtil da vil der herske uklarhed på dette område.

2.3.3.3. Udbydere af cloud-løsninger

Cloud-løsningen må anses som et teknisk hjælpemiddel, hvormed dén, som anvender det, vil være dataansvarlig. Udbyderen af cloud-løsningen er derimod databehandler, idet opgaven er at opbevare oplysninger på den dataansvarliges vegne.

Det kan umiddelbart være vanskeligt at gennemskue årsagen til, hvorfor hosting-udbyderen, som stiller en webside til rådighed, anses for dataansvarlig, medens cloud-udbyderen, som basalt stiller lagerplads til rådighed via internetinfrastrukturen, anses for databehandler. Det kan overvejes, om hosting-udbyderen således får videregivet oplysninger, hvorimod cloud-udbyderen blot får overladt oplysninger.

Forskellen kan måske være begrundet af forhold, der kræver en it-teknisk indsigt, som undertegnede ikke har. Udbyderen af en hosting-løsning bestemmer godt nok, hvordan løsningen ser ud og hvordan oplysningerne teknisk behandles. Køberen bestemmer imidlertid at gøre brug af hostingløsningen, ligesom køberen bestemmer, i hvilket omfang der lægges personoplysninger ud på cloud-løsningen.

Ovennævnte afsnits modstridende fortolkninger giver generelt det indtryk, at sondringen mellem dataansvarlige og databehandlere muligvis ikke er så ligetil, som definitionerne ellers antyder. Artikel 29-gruppens fortolkninger synes gennemgående at fokusere på det moment, som dog direkte fremgår af direktivets ordlyd, nemlig at den dataansvarlige (registeransvarlige) fastsætter

---

[41] Jf. Dt's vejledning af 06.05.2015, *Hvornår er man henholdsvis dataansvarlig og databehandler?*, citat: *"I praksis kan en databehandler f.eks. være en virksomhed, som varetager en anden virksomhed eller en myndigheds IT-systemer. Endvidere kan en databehandler være en udbyder af et webhotel, der hoster hjemmesider for andre, ligesom en databehandler kan være et inkassobureau, som overlades oplysninger fra en dataansvarlig med henblik på inddrivelse af gæld for den dataansvarlige.*". samt endvidere *Lov om behandling af personoplysninger*, 2015, s. 165.

[42] Opfattelsen er konkret lagt til grund i Dt's j.nr. 2014-623-0025, *Inspektion af Nyborg Kommunes brug af Skolesundhed.dk*, hvor TDC, som skulle fungere som nyt hostingfirma i stedet for Danhost, blev anset for at være databehandler med dertil følgende krav om udarbejdelsen af en databehandleraftale.

[43] Jf. Artikel 29-gruppens udtalelse 1/2010, WP169, s. 25, hvor det også bemærkes, at analysen adskiller sig i forhold til leverandører af e-mailtjenester eller internet- og teleleverandører, som er dataansvarlige for trafik- og faktureringsdata, men *ikke* for de data, der transmitteres via løsningerne jf. s. 11.

formålene med og hjælpemidlerne til en behandling. Således synes det i ovennævnte eksempler ikke at indgå som afgørende moment, at f.eks. advokaten eller webhotel-udbyderen først og fremmest udfører opgaven efter at have fået den uddelegeret.

Imod at fortolke begrebet dataansvarlig *for* bredt taler, at det antageligt ofte vil føre til den situation, at der bliver tale om et delt dataansvar og at den person, som efter dansk fortolkning ville være databehandler, ofte vil være i en rolle, hvor det kan være svært selvstændigt at kunne imødekomme de registreredes rettigheder.

Afsnit 3 Databehandlerens forpligtelser

3.1. Før eller senest på tidspunktet for behandlingen

3.1.1. Krav til databehandleren

Forholdet mellem den dataansvarlige og databehandleren er et kontraktligt anliggende på flere plan. Selve hovedydelsen, f.eks. et reklamebureaus analyse af den dataansvarliges kundesegmenter og målrettede reklame til disse, vil være reguleret i det, der bedst kan betegnes som hovedkontrakten.

Lovgivningsteknisk er det ikke vanskeligt blot at bestemme, at den dataansvarlige er ansvarlig for behandlingen og erstatningspligtig for den skade, der måtte opstå som følge heraf. Beskyttelsen af de registreredes interesser, herunder den personlige integritet, tilsiger imidlertid, at mulighederne for kompensation ikke nødvendigvis kan udligne den ulempe, som en regelstridig behandling kan ske at medføre. Med henblik på at de persondataretlige forpligtelser ikke omgås eller rent praktisk ikke iagttages til skade for de registrerede i tilfælde af uddelegering af opgaver til en databehandler, indeholder PDL under direktivet, og forordningen derfor flere bestemmelser, som sideløbene med parternes hovedkontrakt tager sigte på at opretholde en vis behandlingssikkerhed og -fortrolighed.

3.1.1.1. Behandlingssikkerhed

Ifølge PDL § 41, stk. 3, 1. pkt. jf. 2. pkt. skal databehandleren citat: ”… *træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.*”.

Der er tale om en forpligtelse, der består uafhængigt af indholdet af den dataansvarliges instruks eller den indgåede databehandleraftale.[44] Forpligtelsen må i forhold til instruksen og databehandleraftalen anskues som minimumskravene til sikkerhed, som databehandleren skal iagttage.

Da foranstaltningerne samlet set skal være passende i forhold til den konkrete behandling, rummer bestemmelsen et skøn.[45] Justitsministeren er ifølge PDL § 41, stk. 5 delegeret kompetence til at fastsætte nærmere regler om de fornødne sikkerhedsforanstaltninger. For den offentlige forvaltning har ministeren bl.a. udstedt bekendtgørelse nr. 528 af 15. juni 2000 med senere ændringer (sikkerhedsbekendtgørelsen), hvortil hører Datatilsynets vejledning nr. 37 af 2. april 2001 (sikkerhedsvejledningen). Der er ikke fastsat bestemmelser for den private sektor, der således har måttet træffe foranstaltninger på baggrund af rammerne i PDL § 41, stk. 3. Idet Datatilsynet i praksis har

[44] Jf. *Lov om behandling af personoplysninger*, 2015, s. 549.

[45] Bestemmelsen har ophav i direktivets art. 17, stk. 1, hvoraf det i 2. led fremgår, at foranstaltningerne træffes under hensyn til den på tidspunktet tilgængelige teknologi og de forbundne omkostninger. Således skal ikke enhver økonomisk barriere overvindes, ligesom ’state-of-the-art-teknologi’ ikke er påkrævet, så længe sikkerhedsniveauet dog er tilstrækkeligt.

stillet samme krav til behandlinger i det private som i det offentlige, har sikkerhedsbekendtgørelsen dog i et vist omfang hjulpet den private sektor i fortolkningen af indholdet i de passende tekniske og organisatoriske foranstaltninger.[46] [47]

Det omtalte skøn påhviler – udover databehandleren – også den dataansvarlige, idet denne i medfør af PDL § 42, stk. 1 er ansvarlig for at vurdere, hvad der er påkrævet, samt at sikre sig, at databehandleren dels kan opfylde disse foranstaltninger, og dernæst dels påse deres iagttagelse. Det forudsættes således, at databehandleren giver en vis indsigt i sine systemer.

Foranstaltningerne mod at oplysninger slettes m.v. kan f.eks. bestå i sikkerhedskopiering. Derudover kan foranstaltninger til beskyttelse mod uautoriseret adgang f.eks. bestå i autorisation og adgangskontrol, kryptering af datamedier eller kommunikationsforbindelser til e-post mv., registrering og kontrol af afviste adgangsforsøg samt registrering (logning) af anvendelsen af oplysninger, eller brugen af private netværk eller VPN-kryptering.[48]

Forordningen
Afledt af forordningens art. 28, stk. 1 skal databehandleren kunne stille fornødne garantier for at kunne gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på reglernes overholdelse, herunder beskyttelsen af overladte oplysninger. Det er i første omgang op til den dataansvarlige at vurdere, hvad der er tilstrækkeligt. Oplysninger om databehandlerens ekspertise, pålidelighed og ressourcer, herunder antageligt både tekniske og økonomiske, kan være elementer i den konkrete vurdering.[49] Samme kan opfyldelsen af forordningens regler om godkendte adfærdskodekser jf. art. 40 eller certificering jf. art. 42 jf. art. 28, stk. 5.

Databehandlerens interesse i ikke at give fortrolige oplysninger, herunder forretningshemmeligheder, til den dataansvarlige, tilgodeses i et vist omfang af muligheden for certificering.

Retstillingen ifølge PDL § 41, stk. 3, 2. pkt. videreføres hovedsageligt i forordningens art. 32, stk. 1, hvorefter citat "*Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, …*"

Forordningen fremhæver som eksempler; pseudonymisering og kryptering, evnen til at sikre opretholdt fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester, evnen til at rettidigt at genoprette tilgængeligheden i tilfælde af teknisk nedbrud eller anden fysisk hændelse, samt procedurer for afprøvning, vurdering og evaluering af de foretagne foranstaltnin-

[46] I Dt's Årsberetning 2001, s. 68 tilkendegives denne opfattelse, citat: " *I flere konkrete sager har Datatilsynet ved vurdering af de sikkerhedsforanstaltninger, som har været truffet af private dataansvarlige, taget udgangspunkt i de anvisninger, som fremgår af sikkerhedsbekendtgørelsen og sikkerhedsvejledningen. Konklusionen har været, at de beskrevne sikkerhedskrav bør følges, både når den dataansvarlige er en offentlig myndighed, og når der er tale om en privat virksomhed m.v. Det er således Datatilsynets opfattelse, at [PDL] § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i private virksomheder m.v. som i den offentlige forvaltning*".
[47] Af Dt's høringsnotat af 01.06.2007, j.nr. 2005-630-0002, fremgår dog, at Datatilsynet på baggrund af en høring i det private fandt det hensigtsmæssigt, at de krav om kryptering, der stilles til offentlige myndigheder i sikkerhedsbekendtgørelsen, frafaldes over for den private sektor fsva. transmission af almindelige oplysninger via internettet og e-mail, f.eks. købte varer i e-handel, økonomiske oplysninger fra bankforretninger eller afslag på jobansøgninger mv.
[48] Nærmere teknisk beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger findes bl.a. i Dansk Standard DS 484, *Norm for EDB-sikkerhed*, der dog er erstattet af den internationale standard for informationssikkerhed, ISO/IEC 27001 fra 2017 (ledelsesteknikker) og 27002 fra 2017 (sikkerhedsteknikker).
[49] Jf. forordningens præambel 81.

ger. Overholdelsen af et godkendt adfærdskodeks eller opnåelsen af certificering kan som førnævnt skabe formodning for et passende sikkerhedsniveau, dog alt afhængigt af den konkrete behandlings karakter jf. også art. 32, stk. 3.

I art. 32, stk. 2 præciseres endvidere, at den konkrete vurdering af det passende sikkerhedsniveau ikke alene skal tage hensyn til de hændelige risici, som behandlingen afstedkommer i almindelighed, men også i tilfælde af, at der sker ulovlige hændelser, som fører til tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteres, opbevares eller på anden vis behandles. Sådanne risici består bl.a. ved it-kriminalitet, herunder hacking, som ikke sjældent ses. I takt med at ny teknologi anvendes af it-kriminelle, vil det påkrævede sikkerhedsniveau hos databehandleren skulle stå mål hermed, hvilket understreger de potentielt anseelige omkostninger ved bestemmelsens overholdelse.

Risici kan også bestå internt. Herved forstås den risiko, som den dataansvarliges eller databehandlerens personale udgør. Der kan være tale om uagtsomme fejl fra deres side eller forsætligt misbrug af adgangen til oplysningerne. De organisatoriske foranstaltninger skal bl.a. sikre, at de ansatte, som har behov for adgang til oplysningerne, besidder de rette kvalifikationer og alene behandler oplysningerne efter den dataansvarliges instruks jf. art. 32, stk. 4.

Uden fortolkningsbidrag er det en vanskelig opgave at vurdere, hvad der er passende. I det oprindelige forslag til forordningen var EU-kommissionen tillagt kompetence til at udstede retsakter med henblik på fastlæggelse af kriterierne og betingelserne for de tekniske og organisatoriske foranstaltninger omfattet af den vedtagne forordnings art. 32 (jf. forslagets art. 30, stk. 3-4). Denne mulighed udgik i den endelige forordning.[50] [51] Dette efterlader som udgangspunkt de dataansvarlige og databehandlerne med rammebetingelserne.

Det kan forventes, at Databeskyttelsesrådet vil benytte sin adgang til efter art. 70, stk. 1, litra e at udstede retningslinjer, henstillinger eller bedste praksis, idet de nationale tilsyns fortolkninger ikke nødvendigvis vil leve op til motiverne om harmonisering.

Da store dele af direktivet, herunder alle dets målsætninger og principper[52], er videreført i forordningen, kan det i Danmark formentlig også antages, at sikkerhedsbekendtgørelsen og Datatilsynets sikkerhedsvejledning *i mangel af andet* fortsat kan give en vis vejledning i, hvad der udgør et passende niveau.

3.1.1.2. Anmeldelse

Som omtalt ovenfor skal visse EDB-servicebureauer forinden behandlingens påbegyndelse foretage anmeldelse til Datatilsynet jf. PDL § 53. Anmeldelsesforpligtelsen hidrører lov om private registre og er derfor særlig for dansk ret[53], idet forpligtelsen heller ikke er indført med forordningen, hvori direktivets anmeldelsesordning generelt er fravalgt.

[50] *Den Nye Persondataret*, s. 120 anfører herom, at retsstillingen forekommer 'uheldig'.
[51] I Datatilsynets udtalelse af 11.07.2012 om EU-kommissionens forslag til forordning om databeskyttelse (j.nr. 2012-111-0013) kritiseres forslagets muligheder fsva. delegerede retsakter, idet det bemærkes, at EU-kommissionen ikke kan anses for uafhængig og at citat: "*en række af de områder, hvor der efter forslaget tillægges kompetence til at udstede delegerede retsakter, på ingen måde kan anses for ikke-væsentlig*", hvilket er en betingelse jf. TEUF art. 290.
[52] Forordningens præambel 9.
[53] Se bet. nr. 1345/1997, s. 349.

3.1.2. Den dataansvarliges instruks

Ifølge PDL § 41, stk. 1 og forordningens indholdsmæssigt ensartede art. 29 samt 32, stk. 4 skal databehandleren og enhver, der udfører arbejde for databehandleren, herunder både ansatte og andre databehandlere, udelukkende behandle oplysninger efter den dataansvarliges instruks, medmindre behandlingen kræves i henhold til EU-retten eller national ret.[54]

Instruktionsbeføjelsen, som *skal* udøves, er et udslag af forskellen mellem den dataansvarlige og databehandlerens rolle. Instruksen skal således markere, at databehandleren udelukkende behandler de overladte oplysninger på vegne af den dataansvarlige og ikke i andre uvedkommende formål, f.eks. databehandlerens egne. Af samme grund kan instruksen kun gives af den dataansvarlige.

Der gælder ikke særlige formkrav til instruksen, selvom den i dokumentationsøjemed bør foreligge skriftligt. Særligt for ansatte kan instruksen følge af arbejdsgiverens autorisering af dem til at have adgang til oplysningerne eller af stillingsfuldmagten[55], da det for de fleste stillinger er givet, at den ansatte ikke i andre arbejdssammenhænge eller i fritiden kan gøre brug af oplysninger hidrørende bestemte arbejdsopgaver.

Da instruksen også retter sig mod databehandlerens personel, kan der heri afklares praktiske sikkerhedsspørgsmål i relation til disse. Dette kan f.eks. være procedurer for autorisation til og anvendelse af den dataansvarliges it-system. Ligeledes kan der stilles krav om iagttagelse af særlige sikkerhedsforanstaltninger hos databehandleren og af dennes medarbejdere, herunder kvalifikationer, brugen af hjemmearbejdspladser, krav om kryptering af USB-stik etc. Private dataansvarlige kan på dette sted f.eks. henvise til sikkerhedsbekendtgørelsen.

Databehandleraftalen skal henvise til instruksen jf. PDL § 42, stk. 2 og forordningens art. 28, stk. 3, litra a. Ifølge forordningens art. 28, stk. 3, litra h, 2. led skal det tillige fremgå af databehandleraftalen, at den dataansvarlige er forpligtet til at underrette den dataansvarlige, såfremt databehandleren vurderer, at instruksen er i strid med forordningen eller andre databeskyttelsesbestemmelser ifølge EU-retten eller national ret. Denne forpligtelse gælder ikke implicit under direktivet, men kan i dansk ret formentlig udledes af den almindelige loyalitetspligt i kontraktforhold, som dog er vanskelig at sanktionere isoleret set.

3.1.3. Databehandleraftalen

PDL § 42, stk. 2, der implementerer direktivets art. 17, stk. 3, har følgende ordlyd, citat: *"Gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem"*.

Samme forpligtelse følger af forordningens art. 28, stk. 3.

Databehandleraftalen skal således ubetinget udarbejdes, når en eller flere databehandlere medvirker i behandlingen.[56] I forlængelse af ovenstående beskrivelse af advokaten som dataansvarlig hhv. databehandler, er betydningen af at anse advokaten som databehandler også, at der principielt skal udarbejdes en databehandleraftale.

Ifølge ordlyden skal databehandleraftalen vedtages i det bestemte 'klientforhold', hvorfor det ikke er tilstrækkeligt, at der ensidigt udarbejdes et generelt dokument, f.eks. i form af standardpolitikker

[54] *Den Nye Persondataret*, 2016, s. 116 antager, at undtagelser ifølge EU-retten eller national ret "*vist ikke*" kendes. bet. nr. 1345/1997, s. 324 finder anderledes, at tilsynsmyndighedernes lovbestemte ret til at indhente oplysninger til udførelsen af dens opgaver er et eksempel på lovgivning, der kan føre til fravigelse af instruksen.
[55] Jf. bet. nr. 1345/1997, s. 323.
[56] jf. også *Lov om behandling af personoplysninger*, 2015, s. 572.

eller forretningsbetingelser. Derimod er der intet til hinder for, at parterne indgår en aftale på baggrund af den ene parts standardparadigme jf. i det hele nærmere nedenfor om problematikken med ulige partsforhold.

Det er den dataansvarliges ansvar, at databehandleraftalen udarbejdes, og databehandlerens ansvar at overholde sine forpligtelser ifølge denne, hvilket den dataansvarlige fsva. aftalens lovpligtige indhold også er overordnet ansvarlig for. Det er således kritisk, når den dataansvarlige ikke kender identiteten på en underdatabehandler eller ikke er opmærksom på involveringen af en databehandler, f.eks. fordi behandlingsaktiviteten foregår i et e-mail- eller tekstbehandlingsprograms cloudløsning.[57]

3.1.3.1. Databehandleraftalens indhold (direktivet)

PDL § 42, stk. 2, 2. pkt. er yderst kortfattet i formuleringen af databehandleraftalens indhold, citat: "*Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren*".

Det antages, at de fleste databehandleraftaler udarbejdet under direktivet i praksis har omfattet mere end dette.

Databehandleraftalen har til formål at gøre databehandleren bekendt med de almindeligt og særligt gældende vilkår, som skal iagttages. Således er det hensigtsmæssigt, at databehandleraftalen henviser til særlige bestemmelser i lovgivningen, som parterne skal være opmærksomme på, så længe der ikke er modstrid mellem aftalen og gældende ret.

Derudover tjener aftalen sammen med instruksen som elementer i dokumentationen for de bestræbelser, der er gjort fra den dataansvarliges side for at sikre en forsvarlig og lovlig behandling. Da dokumentationen ofte og navnlig under forordningen forudsætter databehandlerens medvirken, f.eks. ved at stille tid og ressourcer til rådighed i forbindelse med løbende revision og kontrol, bør aftalen generelt tage højde herfor. Aftalen kan også indeholde bi-bestemmelser om eventuelle varslers længde og hvordan omkostningerne ved udøvelse af parternes rettigheder og forpligtelser skal fordeles, således at spørgsmålet om ekstrabetaling ikke fører til senere tvister.

Kravet, at databehandleren alene handler efter instruks, kan og vil som regel indgå i form af en standardformulering. Da der ikke gælder formkrav til instruksen, er det således ikke givet, at denne indarbejdes eller i øvrigt foreligger på skrift. I forlængelse af forrige afsnits anbefaling om skriftlighed kan instruksen dog passende indsættes som bilag for at skabe klarhed.

Sikkerhedsniveauet ifølge PDL § 41, stk. 3-5 afhænger af den analyse, som foretages med henblik på at fastslå dets indhold. For behandlinger i den offentlige sektor følger det af sikkerhedsbekendtgørelsens § 7, at databehandleraftalen skal henvise til denne bekendtgørelse. De nærmere sikkerhedskrav, der stilles ifølge instruksen og databehandleraftalen, vil mere teknisk kunne omtales og uddybes i bilag.

[57] Virkningen af den manglende udarbejdelse af en databehandleraftale rammer først og fremmest den dataansvarlige, men der skabes samtidig formodning for, at der ikke er ført tilsyn med de resterende behandlingsaktiviteter, herunder databehandlerens aktiviteter, således at det heller ikke kan tages for givet, at disse nødvendigvis opfylder kravene til sikkerhed mv., jf. bl.a. Dt j.nr. 2014-623-0025, *Inspektion af Nyborg Kommunes brug af Skolesundhed.dk*, hvori citat: "*Datatilsynet må konstatere, at der ikke har været indgået databehandleraftale med den anvendte (under)databehandler Danhost. I den forbindelse må tilsynet derfor også stille spørgsmålstegn ved, om Nyborg Kommune har påset, at sikkerheden ved databehandleren er tilstrækkelig, når kommunen ikke kendte identiteten på (under)databehandleren*".

3.1.3.2. Behovet for revision af eksisterende databehandleraftaler inden 25. maj 2018?

Direktivet ophæves med virkning fra den 25. maj 2018 jf. art. 94, stk. 1. På dette tidspunkt vil det være en realitet, at langt størstedelen af de behandlinger, der finder sted *efter* denne dato, også fandt sted forinden.

Da forordningen vil blive håndhævet fra første dag, kan dens bestemmelser ikke siddes overhørigt.[58] Fortsættelsen af behandlinger, der er lovlige under direktivet, forudsætter dermed, at de opfylder forordningens krav. Sagt med andre ord består opgaven fsva. databehandleraftaler i, at der sikres compliance med forordningens regler inden 25. maj 2018. Opgavens størrelse afhænger konkret af, i hvilket omfang den eksisterende databehandleraftale afviger fra forordningens i det følgende beskrevne krav.[59]

Forordningen viderefører kravet om en skriftlig databehandleraftale specielt til regulering af parternes persondataretlige forpligtelser jf. art. 28, stk. 3.[60] Heri fremhæves, at databehandleraftalen bl.a. skal fastsætte og regulere, citat: "*genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder*" under hensyntagen til databehandleres specifikke opgaver og ansvar samt de med behandlingen forbundne risici for de registrerede.[61] Forordningens krav tjener bl.a. til opfyldelse af den generelle dokumentationsforpligtelse, der påhviler den dataansvarlige, jf. bl.a. princippet om ansvarlighed i art. 5, stk. 2.

Forordningen præciserer i modsætning til direktivet de indholdsmæssige krav i art. 28, stk. 3, litra a-h, hvor instruks (litra a) og sikkerhedsforanstaltninger (litra c) kendes fra direktivet. Af nyt kræves bestemmelser om fortrolighed (litra b), brugen af underdatabehandlere (litra d) og forholdsregler ved behandlingens afslutning, herunder tilbagelevering eller sletning af oplysninger (litra g).

Ydermere tydeliggøres en gennemgående loyalitetsforpligtelse i litra e, f og h. Under hensyn til behandlingens karakter kræves herved bestemmelse om, at databehandleren med passende tekniske og organisatoriske foranstaltninger bistår den dataansvarlige i opfyldelsen af de registreredes rettigheder i forordningens kapitel 3, herunder meddelelse, indsigt, berigtigelse, sletning, blokering og dataportabilitet (litra e). Dette er især relevant, når databehandleren varetager den fulde behandling, således at den dataansvarlige selv har vanskeligt ved at opfylde disse rettigheder. Foranstaltningerne kan f.eks. bestå i elektronisk afvikling af anmodninger om indsigt etc. Som yderligere punkt fastsættes bestemmelser om, at databehandleren bistår den dataansvarlige

[58] Det ligger uden for rammerne af denne afhandling at beskrive samtlige steder, hvor forordningen medfører nye og/eller skærpede pligter, som parterne såvel direkte som indirekte pålægges over for omverden og hinanden indbyrdes. Særligt hvor der er tale om helt nye regler, f.eks. kravet om en rådgivende DPO jf. art. 37-39, vil eksisterende praksis og fortolkningsbidrag under direktivet ikke føre til nogen afklaring. Da det kan være vanskeligt at forudsige den 'rette' fortolkning af nye regler, vil en korrekt anvendelse af reglerne fra 25. maj 2018 forudsætte, at f.eks. Artikel 29-gruppen, og fremtidig Databeskyttelsesrådet, udvider omfanget af vejledninger om bedste praksis m.v.

[59] At en databehandleraftale ikke opdateres til at være i overensstemmelse med forordningens krav, betyder ikke, at aftalen vil være ugyldig eller på anden måde bortfalde inter partes. Virkningen er derimod, at forordningens krav til databehandleraftalen ikke er overtrådt med de for sanktionen skærpende omstændigheder, dette kan antage.

[60] Præambel 81 præciserer, at citat: "*Den dataansvarlige og databehandleren kan vælge at anvende en individuel kontrakt eller standardkontraktbestemmelser, der er vedtaget enten direkte af Kommissionen eller af en tilsynsmyndighed i henhold til sammenhængsmekanismen og derefter vedtaget af Kommissionen*".

[61] Jf. forordningens præambel 81.

fsva. meddelelsesforpligtelsen ved sikkerhedsbrud, foretagelsen af konsekvensanalyser og forudgående høring, samt håndtering af dialogen med tilsynene inden for mulighedernes rammer under hensyn til behandlingens karakter og databehandlerens involvering (litra f).[62]

Da anmeldelsessystemet under direktivet i stor udstrækning er erstattet af en forøget vægt på den dataansvarliges analyse af behandlingen og dokumentationspligter, herunder at pligten til at udvise ansvarlighed samt påse databehandlerens overholdelse af reglerne, forekommer det velbegrundet at fastsætte regler om, at databehandleren stiller alle nødvendige oplysninger til rådighed for den dataansvarlige og deltager i dennes kontrol og revision (litra h).

At databehandleraftalen *'navnlig'* skal have det i litra a-h nævnte indhold, markerer, at indholdet ifølge disse bestemmelser ikke nødvendigvis er udtømmende.

Bl.a. pligterne til at stå til rådighed for og bistå den dataansvarlige kan og bør reguleres indgående, idet opfyldelsen rummer væsentlige ressourcespørgsmål. Praktisk kan der indsættes bestemmelser om, i hvilket omfang databehandleren skal afse tid og ressourcer til at bistå den dataansvarlige, samt om databehandleren har krav på yderligere betaling herfor, såfremt det ikke er reguleret i parternes hovedaftale.

Som alternativ til parternes egen databehandleraftale kan Kommissionens eller de nationale tilsyns standardkontraktbestemmelser jf. art. 28, stk. 7-8 benyttes. Disse kontrakter må gennemsnitligt antages at tilføre parterne en velbalanceret aftale, men bør formentlig altid tilpasses de konkrete forhold, idet hensigten ikke er, at databehandleraftalen blot skal udgøre formalia.[63] Standardkontrakter bør således ikke anvendes i det formål at 'spare' tid eller omkostninger til ekstern rådgivning.

3.1.3.3. Betydningen af forholdet mellem den dataansvarlige og databehandleren

Den dataansvarlige er ansvarlig for at databehandleraftalen udarbejdes og kan langt af vejen selv udøve indflydelse på indholdet, selvom det erindres, at der skal være to til en aftale. Grundet databehandlerens ofte større hjemvanthed i persondataretten vil det imidlertid hyppigt være denne, som tager initiativet til udarbejdelse af en databehandleraftale – ofte ved anvendelse af eget (standard)paradigme.[64] [65] Dette kan være en fordel for databehandleren, som ofte på samme tid er databehandler for mange andre dataansvarlige/kunder, idet databehandleraftalerne inden for dennes berøringsflade således sikres et nogenlunde enslydende indhold til lettelse af den administrative 'byrde'. For den dataansvarlige kan løsningen også være god, når blot resultatet bliver en velbalanceret aftale, som lever op til forordningens krav.

Uligheden mellem parternes position, der kan være begrundet i manglende indsigt eller størrelsen på databehandlerens organisation, kan imidlertid medføre, at databehandlerens foreslåede databehandleraftale fører til en uhensigtsmæssig fordeling af rettigheder og pligter, eller i værste fald ikke opfylder kravene til en databehandleraftale.

---

[62] Det er således navnlig den dataansvarliges forpligtelser, som databehandleren skal bistå i opfyldelsen af, idet databehandlerens pligt til at samarbejde med tilsynene allerede selvstændigt følger af forordningens art. 31.

[63] Ifølge *Persondataforordningen – en håndbog for praktikere*, 2016, s. 120 forekommer standardkontrakter under forordningen mindre relevante, idet forordningens krav til databehandleraftalens indhold udfylder standardindholdet.

[64] Jf. også *Persondataforordningen – en håndbog for praktikere*, 2016, s. 118.

[65] I Artikel 29-gruppens udtalelse 1/2010, WP169, s. 26, note 18, fastslås, at det forhold, at databehandleren udarbejder kontraktbestemmelser, som parterne senere vedtager i fællesskab, ikke berører databehandlerens rolle som databehandler, da den dataansvarlige fortsat må anses for at fastlægge de væsentligste aspekter af behandlingen, herunder formål og hjælpemidlerne.

Fra praksis findes en meget illustrerende sag fra Datatilsynet[66], hvor Odense Kommune havde anvendt Google Apps Online kontorpakke, der bl.a. bestod af en cloud-løsning. Kommunen påstod, at der var 'indgået' en databehandleraftale med Google Ireland Limited, idet der henvistes til 'Google Apps General Terms', som var Googles standardbetingelser. Fra ordlyden[67] kan følgende uddrages, citat:

"*Customer therefore instructs Google to provide the Services and process End User personal data in accordance with the Google Privacy Policies and Google agrees to do the same*"

Google var med andre ord instrueret til at behandle oplysninger i overensstemmelse med sine egne 'privacy policies'[68]. Datarådet og Datatilsynet fandt, at en instruks med dette indhold måtte anses for materielt indholdsløs.

Herudover fandt Datatilsynet det kritisk, at Google næppe var forhindret i ensidigt at ændre sine standardbetingelser eller 'privacy policy'. Problematikken med aftaledokumenters henvisning til andre dokumenter, herunder generelle politikker og standardvilkår, består i, at det er op til aftalens fortolkning, hvorvidt der henvises til disse dokumenter, som de indholdsmæssigt så ud på tidspunktet for aftalens indgåelse, eller om det er hensigten, at det er vilkårenes til enhver tid værende udformning, der skal være gældende. Datatilsynet kan således have ret i den antagelse, at kommunen reelt ikke havde kontrol over, hvordan oplysningerne ville blive behandlet. På denne baggrund konkluderede Datatilsynet, at kommunen havde givet Google den fulde indflydelse på, hvordan oplysningerne ville blive behandlet, hvilket hverken opfylder kravet om den dataansvarliges instruks jf. PDL § 41, stk. 1 eller kravet om databehandleraftalens henvisning hertil jf. PDL § 42, stk. 2.

Datatilsynet kunne endvidere konstatere, at Googles standardvilkår ikke tog højde for, at Odense Kommune tilhører den offentlige sektor, hvorefter at databehandleraftalen skal henvise til sikkerhedsbekendtgørelsen jf. dennes § 7.

Det må antages, at kommunen reelt ikke havde nogen indflydelse på udformningen af instruksen og databehandleraftalen, hvilket dog er usagt i afgørelsen. Om dette var tilfældet, er for sin vis også underordnet, idet virkningen af sådanne vilkårs anvendelse er, at den dataansvarlige påtager sig det fulde ansvar.[69] Selvom den dataansvarlige bør være i en position til at sige fra og i yderste konsekvens må finde en anden leverandør, er situationen vanskelig i de tilfælde, hvor den dataansvarlige er afhængig af en bestemt software eller andre ydelser, som kun udbydes af store leverandører på vilkår, der populært sagt er "take it or leave it".

Afgørelsen begrunder, at selvom databehandleren måtte være i en forhandlingsposition til helt at styre indholdet af instruksen og databehandleraftalen, bør denne ud fra hensigten om et levedygtigt samarbejdsforhold med den dataansvarlige ikke 'gennemtrumfe' anvendelsen af egne standardparadigmer med et så potentielt uforpligtende indhold.

En generel gennemgang af forordningen viser, at der mange steder[70] fortsat er plads til nationale særregler trods hensigten om harmonisering. Dette betyder samtidig, at databehandlere, som bringer egne paradigmer i forslag, også bør sikre, at eventuelle nationale særregler overholdes, f.eks. som det i førnævnte sag burde være sket med sikkerhedsbekendtgørelsens § 7.

---

[66] Dt's j.nr. 2010-52-0138.
[67] Se bilag 1.
[68] Ved 'privacy policy' forstås ifølge Gyldendal, Engelsk/Dansk Fagordbog 2017, synonymerne 'fortroligheds- , privatlivs- eller datapolitik'.
[69] Jf. bl.a. Artikel 29-gruppens udtalelse 1/2010, WP169, s. 27.
[70] Ifølge *Den Nye Persondataret*, 2016, s. 18, rummer forordningen, citat: "*…mange, vist nok over 50, muligheder for fastsættelse af nationale regler*".

Forordningen kan ikke ændre på, at der altid vil bestå ulige partsforhold. Dog vil forordningens skærpede sanktionsbestemmelser jf. bilag 2 formentlig føre til, at den dataansvarlige i større omfang vil se sig tilskyndet til at søge mulige alternativer, såfremt databehandleren ikke kan/vil indgå på vilkår, der understøtter begge parters overholdelse af forordningen.

3.1.4. Særligt om underdatabehandlere

Den teknologiske udvikling har medført, at de dataansvarlige ikke kan klare alle behandlingsaktiviteter selv og at behovet for en eller flere databehandlere opstår. Når opgavernes varetagelse grundet de teknologiske muligheder kræver specialistkompetencer, er det samtidig en realitet, at behovet for ekstern hjælp også kan opstå hos den enkelte databehandler. Moderne databehandling vil derfor i praksis ofte involvere såkaldte underdatabehandlere til varetagelse af delelementer i den større behandling, f.eks. cloud-løsninger eller driften en sikker behandlingsløsning på en e-handelsplatform.

Ved en underdatabehandler forstås fortsat en databehandler, som jf. ovennævnte definition foretager behandling af personoplysninger på den dataansvarliges vegne. Det særlige ved underdatabehandleren er, at dennes medkontrahent er en anden databehandler, hvorfor underdatabehandleren så at sige er underleverandør af en behandlingstjeneste. Underdatabehandlerens kontraktpart, databehandleren, vil typisk stå i et direkte kontraktforhold med den dataansvarlige, selvom det ikke er udelukket, at underdatabehandlere også kan kontrahere med yderligere led af underdatabehandlere.

Modsat situationen, hvor den dataansvarlige blot gør brug af flere sidestående databehandlere, er rammerne for brugen af underdatabehandlere særligt relevant for databehandleren grundet dennes direkte involvering.

En særlig faldgruppe består i, at brugen af underdatabehandlere kan ske ubevidst i tilfælde af manglende indsigt i eller omtanke for egne aktiviteter. Praktisk erindres f.eks. brugen af software, der kan indeholde en cloud-funktion.

3.1.4.1. Underdatabehandlerens retlige indplacering

Brugen af underdatabehandlere er ikke omtalt i direktivet eller PDL. Der er således heller ikke regler, der direkte forhindrer databehandleren i at gøre brug af underdatabehandlere, selvom den dataansvarliges overordnede ansvar for behandlingen og kravet om instruks og databehandleraftale tilsiger, at databehandleren ikke uden videre kan lade sine opgaver udføre af en underdatabehandler på lempeligere vilkår eller at ansvaret for behandlingsaktiviteterne kan flyttes via komplicerede konstruktioner og netværk.[71]

Kravet om at databehandlere kun må behandle oplysninger på baggrund af den dataansvarliges instruks jf. PDL § 41 og databehandleraftalen jf. PDL § 42 gælder også underdatabehandlere, idet de per definition også er databehandlere.

Lovens ordlyd kan umiddelbart give anledning til den opfattelse, at det ikke er muligt, at instruksen gives af databehandleren eller at databehandleraftalen indgås mellem to databehandlere, men der-

[71] Der findes talrige eksempler under direktivet, som anerkender, at direktivet ikke står i vejen for samtidigt flere databehandlere eller brugen af underdatabehandlere. Heriblandt artikel 29-gruppens udtalelse 1/2010, WP169, s. 27 samt Dt's orienteringsbrev af 14. maj 2012 om nye regler om private dataansvarliges anmeldelsespligt, s. 9.

imod at underdatabehandleren skal handle i overensstemmelse med instruksen *fra* og databehandleraftalen *med* den dataansvarlige.[72] Under denne fortolkning er der formentlig ikke noget til hinder for, at kontrakten om den ydelse, som underdatabehandleren skal præstere, indgås med databehandleren.
Om fortolkningen er korrekt i sin helhed, kan imidlertid diskuteres. Overordnet set handler både databehandleren og dennes underdatabehandler på vegne af den dataansvarlige og er derfor underlagt dennes instruks. Der er heller ikke tvivl om, at den dataansvarlige er ansvarlig for, at underdatabehandleren også underlægges en databehandleraftale. Spørgsmålet er imidlertid, om det at være ansvarlig for, at der foreligger en databehandleraftale med underdatabehandleren, også medfører, at den dataansvarlige skal være kontraktpart i denne aftale.

Datatilsynets inspektion hos Styrelsen for Arbejdsmarked og Rekruttering (STAR)[73] kan her fremhæves. Inspektionen viste, at STAR ikke havde indgået en databehandleraftale med KMD, idet STAR ligesom andre offentlige myndigheder gjorde brug af Statens IT til varetagelse af it-driften. STAR henviste til, at det var Statens IT, som skulle indgå en databehandleraftale med KMD. Datatilsynet gav herefter udtryk for, citat: "*… at det er STAR's ansvar, at der foreligger de fornødne databehandleraftaler for så vidt angår de behandlinger af personoplysninger, som STAR er dataansvarlig for. Tilsynet forudsætter derfor, at STAR har sikret eller vil sikre sig, at der bliver indgået de nødvendige databehandleraftaler, herunder med KMD A/S og Statens IT*". I sagen synes det således anerkendt, at STAR opfyldte sine forpligtelser som dataansvarlig, når det blot sikredes, at der blev indgået en databehandleraftale.

Artikel 29-gruppen synes at forudsætte, at grænserne for uddelegerende databehandleres handlefrihed markeres af den dataansvarliges instruks til og databehandleraftale med denne. I den forbindelse fremhæves, at den dataansvarlige grundet sit overordnet ansvar for behandlingen bør *informeres* om brugen af underdatabehandlere og de aktiviteter, som disse konkret påtænkes at varetage[74]. Skal udtalelsen alene forstås sådan, at den dataansvarlige blot skal informeres, således at forpligtelsen til bl.a. at påse databehandlernes overholdelse af de tekniske og organisatoriske foranstaltninger jf. direktivets art. 17, stk. 2 kan overholdes, synes det således anerkendt, at databehandleren inden for rammerne af sin instruks fra og databehandleraftale med den dataansvarlige kan uddelegere opgaver til en underdatabehandler.[75] [76] Skal udtalelsen derimod forstås sådan, at

---

[72] Denne fortolkning lægges bl.a. til grund i *Persondataforordningen – en håndbog for praktikere*, 2016, s. 121.
[73] Dt's j.nr. 2015-621-0035.
[74] Særligt i situationer, hvor der er tale om komplicerede behandlingsaktiviteter eller mange led af databehandlere, kan det være vanskeligt for den dataansvarlige ensidigt at fastlægge hjælpemidlerne til behandlingen. Ifølge Artikel 29-gruppens udtalelse 1/2010, WP169, s. 28 er dette heller ikke påkrævet, men den dataansvarlige bør citat: "*… i det mindste informeres om hovedelementerne i behandlingsstrukturen (f.eks. de involverede aktører, sikkerhedsforanstaltninger, garantier for behandling i tredjelande osv.), så vedkommende stadig er i stand til at have kontrol over de oplysninger, som behandles på dennes vegne*".
[75] EU-kommissionen har i henhold til direktivets art. 26, stk. 4 formuleret en række standardkontraktbestemmelser, der frembyder tilstrækkelige garantier for beskyttelsen af de registrerede i forbindelse med overførsel af oplysninger til tredjelande. Om brugen af underdatabehandlere (subprocessors) fremgår følgende af *Commission Decision C(2010)593*, clause 11 citat: "*The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses*". Klausulen kan understøtte antagelsen om, at databehandleren inden for rammerne af sit eget forhold til den dataansvarlige, herunder den dataansvarliges accept til databehandleren om brugen af en underdatabehandler, kan styre underdatabehandleren, hvilket ydermere forekommer at være bekræftet af Artikel 29-gruppen, se evt. WP176 af 12.07.2010.
[76] Datatilsynet har i en sag omhandlende cloud-løsningen i Microsoft Office 365, j.nr. 2011-082-0216, udtalt, at citat "*De danske dataansvarlige skal bl.a. være opmærksomme på, om der kan blive tale om anvendelse af underdatabehandlere. Når dette som ved Office 365 er tilfældet, skal dette også håndteres med databehandleraftaler. Datatilsynet*

den dataansvarlige skal informeres med henblik på, at den dataansvarlige sættes i stand til at give den i direktivets art. 16 nævnte instruks og selv indgå den i art. 17, stk. 3 pligtige databehandleraftale, forekommer der ikke at være modstrid med den fortolkning, der bl.a. lægges til grund i *Persondataforordningen – en håndbog for praktikere*, 2016, s. 121.

Under alle omstændigheder bør den dataansvarlige via databehandleraftalen kunne udelukke, at der under direktivet gøres brug af underdatabehandlere, hvilket dog kan have betydning for behandlingens praktiske afvikling.

Forordningen
I lyset af det praktiske behov for underdatabehandlere er deres forhold til den dataansvarlige og databehandleren som noget nyt direkte reguleret i forordningen. Den førnævnte fortolkningstvivl under direktivet er blot ét blandt flere eksempler på områder, hvor direktivet kun ved videre-fortolkning har kunnet løse praktiske spørgsmål.

Førend databehandleren kan gøre brug af en eller flere underdatabehandlere, skal den dataansvarlige acceptere dette jf. forordningens art. 28, stk. 2. Accepten skal altid være forudgående og skriftlig. Indholdet kan enten være specifikt møntet på en bestemt underdatabehandler eller være generelt, dog sådan at databehandleren, forinden at den generelle accept udnyttes, giver den dataansvarlige mulighed for at gøre indsigelse mod den påtænkte tilføjelse eller erstatning af underdatabehandlere.
Databehandlere, som gør brug af særlige systemer, der forudsætter inddragelsen af bestemte underdatabehandlere, bør for at lette egen overholdelse af forordningen loyalt informere og opnå den dataansvarliges godkendelse allerede fra start.

I forordningens art. 28, stk. 4 pålægges underdatabehandleren samme databeskyttelsesforpligtelser som dem, der gælder i forholdet mellem den dataansvarlige og databehandleren, herunder ved databehandleraftalen jf. stk. 3. Formuleringen må forstås sådan, at afgørende er indholdet i databehandleraftalen og ikke med hvem, aftalen indgås, hvorfor databehandleraftalen derfor kan indgås mellem databehandleren og dennes underdatabehandler, når databehandleren vel at mærke har samtykket i brugen af underdatabehandlere.[77] Da bestemmelsens formål er databeskyttelse, ses principielt ikke noget til hinder for, at underdatabehandleren pålægges strengere forpligtelser.

Databehandlerens brug af underdatabehandlere ændrer ikke på den dataansvarliges overordnede ansvar over for omverden, herunder de registrerede jf. nedenfor under afsnit 4. Af art. 28, stk. 4, 2. pkt. præciseres dog, at den uddelegerende databehandler er fuldt ansvarlig i det interne forhold med den dataansvarlige *for* underdatabehandlerens pligter. Dette gælder uanset om der er flere led af underdatabehandlere, selvom der formentlig kan gøres regres ned gennem leddene.

3.1.5. Særligt om databehandlere i udlandet

Brugen af databehandlere etableret i andre lande kan være betænkelig grundet de potentielt andre regler, som gælder dér.

---

skal pege på, at man her vil kunne anvende den model, der er anvendt i Kommissionens standardkontrakt. Datatilsynet forudsætter herved, at samtlige elementer i standardkontrakten omhandlende "underkontraherede registerførere" anvendes". Bemærk, at der henvises til den i forrige note beskrevne standardkontrakt fra EU-kommissionen og at situationen i hovedsagen vedrører det yderligere element, at der er tale om overførsel af oplysninger til tredjelande.
[77] Jf. *Persondataforordningen – en håndbog for praktikere*, 2016, s. 122.

Førend direktivets og forordningens regler finder anvendelse, er det en forudsætning, at den pågældende behandling ligger inden for bestemmelsernes territoriale anvendelsesområde. Dette forudsættes i det følgende at være tilfældet, selvom det ikke altid er givet, f.eks. når en europæer uden nogen særlig anledning eller opfordring foretager indkøb via en e-handelsløsning i et tredjeland.

De føromtalte sager fra Datatilsynet om almindelige cloud-baserede tekstbehandlingsprogrammer viser, at anvendelsen af moderne it let kan føre til involveringen af en udenlandsk databehandler.

Grænseoverskridende behandlinger rummer i sig selv mange interessante persondataretlige vinkler, men berøres i det følgende kun overfladisk med henblik på at synliggøre de særlige hindringer for behandlingen, som f.eks. den tilfældige involvering af en underdatabehandler i USA kan medføre.

3.1.5.1. Databehandlere i en anden EU-medlemsstat

Både direktivets art. 1, stk. 2 og forordningens art. 1, stk. 1 og 3 hjemler fri udveksling af personoplysninger inden for EU.

Når der benyttes en databehandler, som er etableret i en anden medlemsstat, skal databehandleren opfylde de sikkerhedskrav, som gælder i etableringslandet jf. PDL § 42, stk. 2, 2. pkt. Dette skal fremgå af databehandleraftalen.

Er der f.eks. tale om et tysk et it-bureau, der udfører behandlingsaktiviteter i Danmark på vegne af en dansk dataansvarlig, skal de specielle tyske sikkerhedsregler iagttages af databehandleren.[78] For at retsstillingen forekommer acceptabel, må det forudsættes, at det både efter de tyske og danske regler er muligt at nå et *passende* sikkerhedsniveau.

Reglen er ikke direkte videreført under forordningen, hvilket formentlig skyldes motivet om at harmonisere kravene.

3.1.5.2. Databehandlere uden for EU

Benyttes databehandlere i tredjelande, dvs. uden for EU eller EØS-lande, som ikke har tilsluttet sig EU-reglerne, gælder særlige begrænsninger for overførslen af oplysninger til dem. Formålet er, at det retspolitisk ønskes sikret, at der i tredjelandet gælder et beskyttelsesniveau svarende til det europæiske.

Der kan ske overførsel af oplysninger til databehandlere i tredjelande, der sikrer et tilstrækkeligt beskyttelsesniveau jf. PDL § 27. Under direktivets bestemmelser om videregivelse i art. 25, stk. 6 har EU-kommissionen således vurderet, at USA i flere år ansås for sikkert under de såkaldte Safe Harbour-principper.[79] Ved EU-domstolens afgørelse af 7. oktober 2015[80] blev denne ordning imidlertid kendt ugyldig, idet bl.a. Edward Snowdens afsløring af NSA's uhæmmede adgang til data viste, at beskyttelsesniveauet ikke var tilstrækkeligt.[81]

---

[78] Bet. nr. 1345/1997, s. 328 anfører herom citat: "*Reglen indebærer formentlig endvidere, at de sikkerhedsbestemmelser, som er fastsat i den medlemsstat, hvor den dataansvarlige er etableret, ikke gælder for en sådan behandling, hvorimod denne medlemsstats materielle behandlingsregler, rettigheder for den registrerede m.v. , fortsat er gældende for behandlingen jf. direktivets art. 4, stk. 1, litra a*".
I samme retning, *Lov om behandling af personoplysninger, 2015, s. 549 og 571.*

[79] jf. Kommissionens beslutning 2000/520/EF af 26. juli 2000.

[80] Sag C-362/14.

[81] Foranlediget af Safe Harbour-ordningens ugyldighed har Kommissionen og USA indgået en ny politisk aftale, således at Kommissionen den 12.07.2016 igen kunne godkende beskyttelsesniveauet i USA, nu under betegnelsen, *EU-U.S. Privacy Shield.* Den nye ordning må forventes revideret, når forordningen får virkning.

Overførsel til usikre tredjelande kan ske, såfremt det er hjemlet på listen i PDL § 27, stk. 3, eller at den dataansvarlige yder tilstrækkelige garantier for de registreredes rettigheder jf. stk. 4 eller at overførslen sker ifølge EU-kommissionens tidligere nævnte standardkontraktbestemmelser jf. stk. 5.

Forordningen
Under forudsætning af databehandlerens overholdelse af forordningens øvrige regler, videreføres mulighederne for overførsel af oplysninger til tredjelande i dennes kapitel 5, der samtidig udvider mulighederne, herunder fsva. betydningen af certificering jf. art. 46, stk. 2, litra f eller bindende virksomhedsregler jf. art. 47.

Den dataansvarliges pligter ifølge forordningens kapitel 5 sanktioneres i art. 83, stk. 5 med bøder op til 20 mio. euro eller 4 % af virksomhedens globale årlige omsætning, hvormed reglernes vægt markeres.

Databehandleren bør se reglerne om overførsel på den måde, at sikres ikke et tilstrækkeligt beskyttelsesniveau, kan der ikke ske overførsel til det pågældende land. I så fald kan behandlingen ikke ske som forudsat, hvilket bør få databehandleren til at bistå den dataansvarlige i dennes bestræbelser i at overholde overførselsreglerne.

3.2. Under behandlingen

Databehandleren skal udover opfyldelse af hovedkontrakten sikre overholdelsen af sine forpligtelser ifølge lovgivningen.

Selvom det passende sikkerhedsniveau er analyseret og fastlagt forinden behandlingen, tilsiger formålet med PDL § 41, stk. 3 og forordningens § 32, at der er tale om en løbende proces, hvor databehandleren – helst i samarbejde med den dataansvarlige – bør følge op på eventuelt ændrede risici og trusselsbilleder, ligesom det erindres, at den teknologiske udvikling er så hastig, at der sjældent går år imellem ny og forældet teknologi.

Under forordningen er databehandleren tillagt særlige pligter, der i vidt omfang fremgår af databehandleraftalens indhold. Forpligtelserne omtales kortfattet i det følgende under hensyn til, at afhandlingens fokus udgør forhold, som databehandleren kan påvirke.

3.2.1. Fortegnelse over behandlingsaktiviteter

Ligesom den dataansvarlige skal databehandleren føre en fortegnelse over sine behandlingsaktiviteter jf. forordningens art. 30, stk. 2, såfremt enten databehandlerens organisation beskæftiger mere end 250 ansatte eller at behandlingen sandsynligvis medfører risiko for de registreredes rettigheder, at behandlingen ikke er lejlighedsvis, eller at behandlingen omfatter følsomme oplysninger jf. art. 9 og 10.

Fortegnelsen har til formål påvise overholdelse af forordningen på den måde[82], at den skriftligt kan forevises tilsynsmyndigheden på anmodning, hvorefter det kan vurderes, om f.eks. de trufne tekniske og organisatoriske sikkerhedsforanstaltninger står mål med de behandlingsaktiviteter, der er oplyst hhv. konstateret udført.

[82] jf. forordningens præambel 82.

3.2.2. Generelt samarbejde med tilsynet

Forordningens art. 31 medfører en generel forpligtelse til at samarbejde med tilsynsmyndigheden i forbindelse med dennes opgaver. Dette kan forekomme problematisk, når reglerne er konstateret overtrådt.[83]

Bestemmelsen er relevant, når det erindres, at databehandleren reelt kan ske at udføre hele den praktiske behandling på vegne af den dataansvarlige. Den dataansvarliges overordnede ansvar medfører således ikke, at dette udelukkende er et spørgsmål mellem den dataansvarlige og de håndhævende myndigheder, idet tilsynet nødvendigvis skal have adgang til informationer dér, hvor behandlingen foregår.

3.2.3. Sikkerhedsbrister og samarbejde med tilsynet

It-sikkerhed rummer spørgsmål om beskyttelsen mod uautoriseret og utilsigtet adgang, ændring eller sletning af oplysninger. Metoder til kryptering og adgangsbegrænsning er alle teoretisk forudsigelige og dermed mulige at bryde, idet der bagved de anvendte teknologier er tale om programmering. Det er derfor givet, at besiddes de rette faglige, økonomiske og tidsmæssige ressourcer, kan ethvert sikkerhedsværn bestående af passende tekniske og organisatoriske foranstaltninger brydes ved kriminelle handlinger, foruden at brud på simpleste vis også kan skyldes nedbrud, fejl eller ansattes uagtsomheder.

Jo flere opgaver databehandleren varetager, des større er sandsynligheden for, at sikkerhedsbruddet sker i dennes regi. Pligten til at meddele datatilsynet hhv. de registrerede om sikkerhedsbrud påhviler den dataansvarlige[84], men databehandleren er ifølge art. 33, stk. 2 forpligtet til at underrette den dataansvarlige og skal i øvrigt bistå den dataansvarlige i dennes meddelelsesforpligtelser fsva. oplysninger, der er tilgængelige for databehandleren jf. databehandleraftalen jf. art. 28, stk. 3, litra f.

3.2.4. Databeskyttelsesrådgiver (DPO)

Databeskyttelsesrådgiveren[85] er en nyskabelse i forordningen. Der er tale om en helt ny aktør, hvis opgave er at bistå og vejlede den dataansvarlige hhv. databehandleren ved bl.a. at overvåge den interne overholdelse af forordningen. DPO'en overtager således *ikke* ansvaret for behandlingen.

Forordningens art. 37, stk. 1, litra a-c fastslår de tilfælde, hvor der er pligt til at udpege en DPO. Med undtagelse af domstolene skal offentlige myndigheder altid have en DPO tilknyttet (litra a).[86]

[83] Om juridiske personers eksisterende, men bl.a. fsva. deltagelse i kontrolundersøgelser begrænsede ret til at påberåbe sig forbuddet mod selvinkriminering, se Retssikkerhedskommissionens bet. nr. 1428/2003 (pkt. 6.5.) samt i relation til ledelsesrepræsentanters status som vidne eller tiltalt under bødesager Straffelovrådets bet. nr. 1289/1995.

[84] *Den Nye Persondataret*, 2016, s. 123 finder det hensigtsmæssigt, at databehandleren også var pålagt en meddelelsesforpligtelse, men vurderer, at fravalget må skyldes den dataansvarliges interesse i selv at håndtere bruddet over for omverden.

[85] Også kaldet Data Protection Officer (DPO).

[86] Dog kan myndigheder i overensstemmelse med deres organisationsstruktur og størrelse have en fælles DPO, således tilknytningen ikke nødvendigvis skal være på afdelingsniveau jf. stk. 3.

For databehandlere i den private sektor er DPO'en pligtig, hvis kerneaktiviteten enten indebærer regelmæssig og systematisk overvågning af registrerede i stort omfang (litra b), *eller* består behandling af følsomme oplysninger efter art. 9 og 10 i stort omfang (litra c).[87] [88]

Ved en 'kerneaktivitet' forstås virksomhedens hovedaktivitet og ikke biaktiviteter. Store virksomheder, som dermed i stort omfang behandler oplysninger om sine ansattes fagforeningsmæssig tilhørsforhold, hvilket er en biaktivitet, skal derfor ikke af den grund udpege en DPO. Hvad der forstås ved 'stort omfang' er derimod uklart og må finde sit niveau i praksis.[89]

Såfremt den dataansvarlige skal have en DPO grundet behandlingsaktiviteter, som udføres af en databehandler, skal databehandleren formentlig også have en DPO tilknyttet, men dette er ikke givet. Spørgsmålet afhænger konkret af, om betingelserne i primært litra b eller c er opfyldte.[90] Omvendt kan der også være tale om, at databehandleren for mange dataansvarlige udfører visse behandlingsaktiviteter i stort omfang, uden at dette behøver at være tilfældet for den enkelte dataansvarlige.

Foruden litra a-c følger det af stk. 4, at EU-retten eller national ret kan bestemme andre situationer, hvor der skal udpeges en DPO. I sådanne tilfælde kan sammenslutninger og andre organer udpege en DPO, som kan handle på vegne af de repræsenterede dataansvarlige og databehandlere.

Selv når DPO'en ikke er påkrævet, kan det alligevel være en fordel for databehandleren at tilknytte en sådan, idet der opnås en sparringspartner, som kan løbende kan byde sig til.

3.3. Efter behandlingen

Hovedkontrakten er opfyldt, når databehandleren har leveret sin ydelse, og modtaget betaling herfor. Det er dog ikke givet, at de persondataretlige forpligtelser ophører her. Såfremt databehandleren ikke lader behandlingen af oplysninger ophøre, f.eks. ved lovpligtig opbevaring i dokumentationsøjemed eller videregivelse, gælder behandlingsreglerne fortsat. Databehandleraftalen bør for god ordens skyld præcisere, at aftalen følger hovedaftalen, men varer ved, så længe der behandles oplysninger.

Under forordningen skal det fremgå af databehandleraftalen, hvorvidt databehandleren enten skal slette eller tilbagelevere oplysningerne til den dataansvarlige jf. art. 28, stk. 3, litra g. Såfremt databehandleren pålægges særlige forpligtelser, f.eks. at indhente en revisionsrapport med henblik på at dokumentere, at der ikke længere behandles oplysninger, bør databehandleren enten via kontraktsummen eller ad anden vej søge sig kompenseret for de ikke ubetydelige omkostninger hertil.

---

[87] Den vedtagne forordnings litra c har erstattet litra b i Kommissionens forslag, hvorefter DPO'en skulle udpeges, når en virksomhed beskæftigede mere end 250 medarbejdere. I den vedtagne forordning er det således behandlingen og de gennemsnitlige risici, den medfører, som begrunder kravet om en DPO.

[88] I koncernforhold kan der udpeges en fælles DPO, såfremt alle dele af koncernen, som ellers skulle have haft sin egen DPO, har let adgang til denne jf. stk. 2.

[89] Ifølge Artikel 29-gruppens reviderede vejledning af 05.04.2017, WP243, s. 7-8, foreslås niveauet vurderet ud fra følgende faktorer; antallet af registrerede, mængden og arten af personoplysninger samt behandlingens tidsmæssige og geografiske udstrækning. Gruppen peger bl.a. på hospitaler, banker, forsikringsselskaber samt udbydere af medlemsordninger, hvorimod behandlingen af patientdata foretaget af individuelle psykiatere, ikke vurderes at udgøre et stort omfang.

[90] Artikel 29-gruppens reviderede vejledning af 05.04.2017, WP243, s. 9, er enig i antagelsen, men bemærker, at tilknytningen af en DPO kan være et udtryk for god praksis.
Den Nye Persondataret, 2016, s. 131, finder anderledes, citat: *"Når den dataansvarlige er forpligtet til at have en rådgiver, må dette nærmest som en refleks indebære, at databehandleren også er forpligtet til at have en rådgiver tilknyttet*".

Afsnit 4 Databehandlerens ansvar i tilfælde af reglernes tilsidesættelse

I det følgende behandles retsfølgerne af databehandlerens overtrædelse af de i forrige afsnit analyserede forpligtelser ifølge PDL og forordningen. Dette f.eks. i tilfælde af mangelfulde tekniske og organisatoriske sikkerhedsforanstaltninger.

Ansvaret kommer håndgribeligt til udtryk via erstatningsansvaret over for de registrerede samt straffeansvaret, der præventivt tager sigte på adfærdsregulering m.v.

Straffeansvaret er omtalt i bilag 2 med henblik på at bevare sammenhængen mellem databehandlerens forpligtelser og ansvar, og analysen af mulighederne for at begrænse dette ansvar. Som løftestang for forordningens overholdelse er risikoen for bødestraf imidlertid så potentielt indgribende for databehandleren, at spørgsmålet ikke helt kan udelades.

4.1. Direktivet og persondatalovens sanktionsapparat

Under direktivet forpligtes medlemsstaterne til at håndhæve dets bestemmelser, herunder at indføre ansvars- og sanktionsbestemmelser jf. art. 23 og 24, ligesom domstolsprøvelsen ikke må afskæres jf. art. 22.

Reglerne er implementeret i PDL kapitel 18, hvor følgende gælder om erstatningsansvaret.

4.1.1. Erstatning og godtgørelse

Efter PDL § 69 skal den dataansvarlige erstatte skade forvoldt ved lovens overtrædelse, medmindre skaden ikke kunne afværges trods lovens overholdelse. Der er tale om et præsumptionsansvar, hvorved forstås et culpaansvar med omvendt bevisbyrde. Kan den dataansvarlige godtgøre, at skaden ville være indtrådt uafhængigt af reglernes overholdelse, f.eks. i tilfælde af omfattende hackerangreb, 'går han fri'.[91]

Den krænkelse og ulempe, som brud på PDL kan påføre de registrerede, er vanskelig at opgøre i et lidt tab. Principielt set er erstatning udelukket, såfremt der ikke kan dokumenteres noget lidt tab.[92] En gennemgang af retspraksis på området viser, der i sådanne tilfælde i stedet er tilkendt en godtgørelse for tort jf. erstatningsansvarslovens § 26, stk. 1.[93]

Selvom databehandleren ikke er nævnt i PDL § 69, der således langt ad vejen udtrykker den dataansvarliges rolle, kan det ikke udelukkes, at databehandleren kan have optrådt på en måde, der efter almindelige erstatningsretlige grundsætninger vil medføre et erstatningsansvar. Om disse tilfælde må det dog antages, at databehandleren formentlig samtidig vil have overskredet sin bemyndigelse i form af databehandleraftalen og instruksen på en sådan måde, at databehandleren muligvis kan anses for selvstændig eller fælles dataansvarlig, og ad denne vej omfattes af bestemmelsen i § 69.

[91] F.eks. U 2005.1639 V om en arbejdsgivers læsning af e-mails, hvor der ikke blev tilkendt erstatning.
[92] Ifølge *Den Nye Persondataret*, 2016, s. 161, fører krænkelsen af PDL sjældent til materiel skade, hvorfor § 69 aldrig har slået igennem i praksis.
[93] F.eks. U 2005.1113 Ø om en butiks offentliggørelse af en tidligere ansats bortvisning pga. tyveri, U 2007.1667 V om offentliggørelse af personoplysninger, U 2008.772/2 S om ulovlig Tv-overvågning samt U 2011.2343 H om ulovlig videregivelse af oplysninger.

4.2. Forordningens bestemmelser

I forordningens art. 77 gives den registrerede ret til at indgive en klage til en tilsynsmyndighed. Klagen skal ikke indgives til en bestemt tilsynsmyndighed, idet at retten '*navnlig*' kan udøves i bopæls- eller opholdslandet eller dér, hvor krænkelsen har fundet sted. Med de nye regler om sammenhængsmekanismen i art. 63 ff. samt tilsynenes indbyrdes forhold, herunder kompetencefordelingen ved udpegelse af en ledende tilsynsmyndighed i art. 56 og 60, forudsættes, at forordningens regler finder ensartet anvendelse i hele EU.[94] For både dataansvarlige og databehandleren rummer dette system ulemper i form af den utryghed, der kan bestå i kontakten med et andet lands myndigheder.

Retten til at klage til en tilsynsmyndighed berører ikke retten til at gå til domstolene, ligesom det af art. 77 fremgår, at den registrerede har ret til effektive retsmidler.

Værnetinget for sager mod private dataansvarlige eller databehandlere er i det medlemsland, hvor pågældende er etableret og alternativt hvor den registrerede har sit sædvanlige opholdssted. Sager der udspringer af offentlige myndigheders udøvelse af offentligretlige beføjelser anlægges i myndighedens hjemland. Internt i medlemslandet afgøres den stedlige kompetence efter nationale regler – i Danmark retsplejeloven.

De præceptive regler medfører, at den dataansvarlige og databehandleren ikke med værnetingsklausuler i deres indbyrdes forhold kan styre og begrænse *de registreredes* procesmuligheder. Relevant for de situationer, hvor behandlingen af personoplysninger sker på baggrund af et samtykke eller en aftale med den registrerede, vil værnetingsreglerne således begrænse den dataansvarlige i at indføre værnetingsklausuler med bindende virkning over for den registrerede – i hvert fald når den registrerede er en fysisk person. Reglerne hindrer imidlertid ikke den dataansvarlige og databehandleren i – gældende i deres indbyrdes forhold – at indgå aftaler om forum og lovvalg, hvilket er relevant fsva. de tvister, der kan opstå i kølvandet af følgende omtalte retsfølger.

4.2.1. Erstatningsansvar

Enhver, som har lidt skade grundet forordningens overtrædelse, har krav på erstatning jf. art. 82, stk. 1. Krav på erstatning kan ikke afgøres administrativt, idet der er tale om et domstolsanliggende.

Med begrebet '*skade*' forstås ifølge præambel 146 enhver skade, sådan som begrebet fortolkes af EU-domstolen. Hvor PDL § 69 alene omfattede den materielle skade, omfattes i forordningen herudover immateriel skade. Hjemlen for at 'erstatte' den ikke-økonomiske krænkelse, som den forurettede er påført, vil således fremadrettet være at finde i den persondataretlige regulering.[95]

---

[94] 'One-stop-shop-systemet', der bl.a. er relevant ved grænseoverskridende behandling jf. art. 4, nr. 23, har til formål, at behandlingens aktører alene har kontakt med én tilsynsmyndighed. Dette er dog ikke fuldt ud gennemført som forudsat i det oprindelige forslags art. 51, idet berørte nationale tilsyn jf. art. 4, nr. 22, bl.a. fordi en klage er indgivet dér eller at berørte registrerede har bopæl dér, kan behandle sagen uden om samarbejdsproceduren i art. 60-65, hvis den ledende tilsynsmyndighed ikke går ind i sagen, eller det berørte tilsyn på sit eget territorium træffer foranstaltninger efter hasteproceduren i art. 66.

[95] I *Juridisk Ordbog*, 2016, defineres 'tort' som, citat: *"Den ikke-økonomiske skade, som forvoldes ved krænkelse af en persons selv- og æresfølelse, …, jf. erstatningsansvarslovens § 26"*. Alt efter EU-domstolens fortolkning af begrebet '*immateriel skade*' er det ikke nødvendigvis givet, at dette lader sig begrænse til den danske forståelse af begrebet, tort.
Begrebsafklaringen af samt niveauet for 'erstatning'/godtgørelse for ikke-økonomisk skade bliver relevant at følge under forordningen.

Efter dansk juridisk sprogbrug forekommer det næppe korrekt at tale om erstatning fsva. ikke-økonomisk skade, idet erstatning forudsætter et dokumenterbart lidt tab. Den rette term havde været 'godtgørelse', hvori også ligger en mere skønsmæssigt opgørelse af det 'lidte tab'.

Den dataansvarlige hæfter som udgangspunkt for en skade, der skyldes forordningens overtrædelse.[96] [97]

Hvor PDL alene pålagde den dataansvarlige erstatningsansvar, fremhæves i forordningen, at også databehandleren kan være ansvarlig. Databehandlerens hæftelse er dog begrænset til skade forvoldt ved en behandling, hvor databehandleren ikke har opfyldt sine forpligtelser ifølge forordningen eller den dataansvarliges lovlige instruks jf. art. 82, stk. 2.

For både den dataansvarlige og databehandleren gælder fortsat, at der er tale om et præsumptionsansvar jf. art. 82, stk. 3.

Såfremt en eller flere dataansvarlige eller databehandlere, eller både den dataansvarlige og databehandleren er involveret i samme behandling og er ansvarlige efter forrige bestemmelser, hæfter de *solidarisk* jf. art. 82, stk. 4. Hensynet er ifølge præambel 146, at den registrerede bør sikres bedre muligheder for at opnå fuld erstatning, da det at have ret til og ved domstolene at være tilkendt erstatning ikke er nogen garanti for, at pengene udbetales. I præamblen nævnes dog muligheden for, at erstatningsansvaret under en retssag kan fordeles mellem f.eks. den dataansvarlige og databehandleren, så langt at den registrerede er sikret fuld erstatning.

Har databehandleren, f.eks. grundet sin umiddelbare betalingsevne, måtte betale fuld erstatning til en registreret efter stk. 4, kan pågældende gøre regres mod eksempelvis den dataansvarlige, svarende til den del af erstatningen, som denne skulle bære på baggrund af vedkommendes skyld jf. art. 82, stk. 5.

Retten til at gøre regres sikrer ikke nødvendigvis den berettigede at blive godtgjort det 'udlagte', idet spørgsmålet afhænger af modpartens betalingsevne.[98]

4.3. Klausuler i forholdet mellem den dataansvarlige og databehandleren

4.3.1. Værnetings- og lovvalgsaftaler

Hverken PDL under direktivet, eller forordningen hindrer den dataansvarlige og databehandleren i at indgå værnetings- og lovvalgsaftaler fsva. deres interne retlige opgør. Tvister i forholdet kan dels komme på tale i anledning af databehandlerens opfyldelse af hovedkontrakten, men også som følge af førnævnte regresspørgsmål.

Grundet forordningens brede materielle og territoriale anvendelsesområde jf. art. 2-3 vil lovvalget fsva. parternes ufravigelige persondataretlige forpligtelser for sin vis være givet på forhånd, ligesom de processuelle regler i hvert fald for dansk rets vedkommende følger værnetinget.

[96] Efter dansk juridisk sprogbrug forudsætter begrebet hæftelse ikke nødvendigvis den hæftendes eget erstatningsansvar, idet hæftelsen kan vedrøre andres ansvarspådragne handlinger eller undladelser jf. også *Juridisk Ordbog*, 2016, s. 222.

[97] Ifølge *Den Nye Persondataret*, 2016, s. 161, forstås ved 'forordningen' også regler fastsat i medfør af den indflydelse, som forordningen overlader til medlemsstaterne.

[98] Retspolitisk synes retsstillingen at være begrundet i antagelsen, at det forekommer mere rimeligt at pålægge de ansvarlige parter denne risiko, fremfor den skadelidte registrerede jf. også forordningens præambel 146.

4.3.2. Ansvarsbegrænsningsklausuler

Under direktivet og PDL er den dataansvarlige ikke hindret i efter almindelige erstatningsretlige regler at gøre regres mod sin databehandler, såfremt denne kan bebrejdes det tab, som den dataansvarlige har måttet udrede. Den dataansvarlige kan bl.a. adcitere databehandleren i en retssag ifølge retsplejelovens bestemmelser.[99] Parterne forhindres heller ikke i at lade typisk databehandlerens ansvar begrænse til kontraktsummen for hovedydelsen.[100]

Anderledes er retsstillingen under forordningen, idet der i kølvandet på art. 82, stk. 5 kan stilles det spørgsmål, om bestemmelsen udelukker aftaler om en anden ansvarsfordeling i det *indbyrdes* forhold mellem databehandleren og den dataansvarlige eller andre, såkaldte ansvarsbegrænsningsklausuler eller -fraskrivelser.

Klart er det, at databehandlerens ansvarsbegrænsning i kontraktforholdet med den dataansvarlige ikke kan påberåbes som grundlag for, at databehandleren ikke hæfter solidarisk efter stk. 4 over for den krænkede (den registrerede).

Spørgsmålet er imidlertid, om stk. 5 skal læses som en præceptiv ret for både den dataansvarlige og databehandleren til i det indbyrdes forhold maksimalt at bære et tab, der svarer til vedkommendes egen skyld. I den simple situation, hvor der alene er én dataansvarlig og én databehandler, vil databehandlerens vedtagne ansvarsfraskrivelse, der i det indbyrdes forhold pålægger den dataansvarlige at bære et større tab, således i den dataansvarliges optik fravige dennes ret ifølge stk. 5. Dette er f.eks. tilfældet, såfremt databehandlerens ansvar i det indbyrdes forhold er begrænset til vederlaget for kontraktens opfyldelse, men at opgørelsen af det pådragne ansvar viser sig at overstige dette niveau.

I udgangspunktet kan hverken national lovgivning eller private kontraktbestemmelser fravige forordningens præceptive regler, men spørgsmålet er videre, om forordningens beskyttelseshensigt har været at fratage kontraktparterne denne frihed.[101]

På den ene side ligger ordlyden fast, medens det på den anden side kan indvendes, at hensynet ifølge præambel 146 er at forbedre de registreredes muligheder for at få erstatning, og at den dataansvarlige og databehandlerens indbyrdes økonomiske opgør principielt ikke er af betydning for

[99] Betingelserne fremgår af RPL § 250, stk. 2, nr. 1-3 og forudsætter, at der er dansk værneting (nr. 1), at kravet mod tredjemand kan behandles efter samme processuelle regler, som sagens øvrige krav (nr. 2) og at tredjemand ikke gør indsigelse mod kravets inddragelse i sagen, eller at retten finder, at kravene grundet deres indbyrdes sammenhæng bør behandles under én sag (nr. 3) jf. også *Den Civile Retspleje*, 2015, s. 262 ff.

[100] Sådanne klausuler støttes bl.a. af EAL § 27, stk. 2, 2. pkt. som undtagelse til EAL § 25, og ses bl.a. som vilkår i statens *Standardvilkår for kortvarigt it-projekt K01, pkt. 18*, hvorefter citat: *"Erstatning og eventuelt bodsbeløb tilsammen er dog under alle omstændigheder begrænset til systemvederlaget"*.

[101] *Perspektivering:* Fsva. revisorer, der også behandler personoplysninger og hvis virksomhed i betydeligt omfang er underlagt EU-regulering, har EU-Kommissionen i henstilling 2008/473/EF af 08.07.2008 opfordret medlemsstaterne til at begrænse revisorernes civilretlige erstatningsansvar. Kommissionen foreslår, at ansvaret kan begrænses ved fastsættelse af et beløbsmæssigt loft, hæftelse pro rata eller friheden til at aftale ansvarsbegrænsning med virkning for tredjemand, så længe denne ikke fratages mulighederne for en *rimelig* erstatning jf. UfR 2011B.21. Revisorens rolle minder generelt noget om databehandlerens, idet de potentielle skadelidte ved revisorens fejl og forsømmelser ikke nødvendigvis er kunden, men derimod tredjemand, som f.eks. indretter sig i tillid til en fejlbehæftet årsrapport. På samme måde er det ikke den dataansvarlige, der *i første omgang* lider skade af databehandlerens fejl og forsømmelser, men derimod de registrerede. Henstillingen viser, at EU-Kommissionen er opmærksom på ansvarsbegrænsninger, hvilket dog taler imod, at retsstillingen ifølge forordningen skulle være tilfældig.

den registrerede. Indvendingen synes dog ikke at kunne føre til fravigelse af bestemmelsens ordlyd, selvom praktiske hensyn taler for, hvorfor det under forordningens anvendelse og fortolkning bliver interessant at følge problematikken.[102]

Førnævnte meget forsimplede eksempel tegner i øvrigt næppe virkeligheden. Tilsidesætter en Cloud-udbyder sine forpligtelser med den følge, at mange dataansvarliges oplysninger gives til pris for offentligheden og påfører dem tab eller krænkelse, risikeres et utal af regreskrav. Selvom urimelige aftalevilkår kan bortfortolkes og at meget taler imod, at forsætlige eller meget groft uagtsomme regeltilsidesættelser afblødes med ansvarsfraskrivelser, er der næppe tvivl om, at sådanne klausuler også har klare grunde for sig, såfremt der ikke skal indkalkuleres større risikotillæg i prisen for databehandlerens ydelse.

Såfremt bestemmelsen skal forstås som begrænsende for kontraktfriheden, må det understreges, at indskrænkningen formentlig er begrænset til regres på baggrund af erstatningsforpligtelser over for de registrerede.

Afsnit 5 Sammenfatning og konklusion

De forudgående afsnits analyse af databehandlerens retsstilling under direktivet og forordningen har vist, at direktivets regler i vidt omfang videreføres med forordningen, men også at der er indført nye regler af betydning for databehandleren.

På baggrund af afhandlingens søgen efter en entydig definition af databehandleren og afgrænsning over for den dataansvarlige, må det konkluderes, at en sådan følger af direktivets hhv. forordningens ordlyd, men at der i praksis forekommer grænsetilfælde, der kan give anledning til tvivl grundet definitionernes bredde. Disse rummer bl.a. leverandører af internetbaserede tjenester samt særligt regulerede rådgivningsydelser. Tvivlen, som formentlig skyldes de særlige faktiske forhold, der gør sig gældende for de omtalte aktiviteter, bør afklares grundet dens afgørende betydning for fordelingen af ansvar og pligter mellem behandlingens parter. Det må dog også konkluderes, at der altid vil være tvivlsomme eksempler, så længe den teknologiske udvikling konstant udfordrer reguleringen.

Cloud-computing har givet anledning til særlige udfordringer under direktivet. Der er tale om ny teknologi, hvis påvirkning af dataflowet er vanskelig at gennemskue. Risikoen er, at behandlingsaktiviteter utilsigtet krydser landegrænser eller involverer underdatabehandlere. Forordningen, der er formuleret teknologineutralt, løser ikke i sig selv disse udfordringer. Dog vil forøgede krav om dokumentation, herunder også databehandlerens forpligtelse til at føre en fortegnelse over sine behandlingsaktiviteter jf. art. 30, som understøttes af de skærpede sanktioner, helt sikkert skærpe parternes eget fokus.

Et af denne afhandlings formål var også at give bud på, hvordan databehandleren bedst muligt kan håndtere forordningen. Motiveret af parternes sammenfaldende interesse i at eksisterende behandlinger kan videreføres under forordningen, bør databehandleren, trods den dataansvarliges fortsatte overordnede ansvar, være behjælpelig med at sikre så smidig en overgang som muligt. Frem mod den 25. maj 2018 vil der blive indgået et utal af databehandleraftaler underlagt direktivet. Disse aftaler kan med fordel tage højde for forordningens krav. I en tid med begrænset udbud af officielle fortolkningsbidrag, bør et forbehold om genforhandling eller revision dog indsættes.

[102] JM's bet. 1565, s. 914 antager dog, at bestemmelsen *ikke* hindrer aftaler om den indbyrdes ansvarsfordeling, herunder fordi at dette også ville vanskeliggøre tegning af ansvarsforsikringer m.v.

Uanset om der er aftalt genforhandling eller ej, bør der i god tid forinden 25. maj 2018 foretages en gennemgang af bestående behandlinger med henblik sikre compliance med forordningens bestemmelser. At revisionen foretages i god tid motiveres både af forordningens ansvarsbestemmelser samt det forhold, at f.eks. databehandleraftalens opdatering kræver begge parters medvirken, og kortlægningen af behandlingsaktiviteterne muligt mange andre parter.

Da forordningen i vidt omfang viderefører direktivets krav, herunder at der skal træffes passende sikkerhedsforanstaltninger, er det dog et godt udgangspunkt at vurdere, hvorvidt direktivet allerede overholdes.

Under gennemgangen af databehandlerens forpligtelser konstateredes, at databehandleraftalens indhold i modsætning til direktivets meget summariske omtale nu er eksemplificeret i forordningen. Dette er positivt, men databehandleren er herved også pålagt flere forpligtelser, herunder til at bistå den dataansvarlige i flere af dennes pligter. Sådanne forpligtelser rejser økonomiske spørgsmål, idet der i uforudsigeligt omfang lægges beslag på databehandlerens ressourcer. Fremhæves skal derfor anbefalingen om, at disse afledte effekter reguleres i databehandleraftalens vilkår, således der ikke opstår spørgsmål om ekstrabetaling. Da behandlingen sker i den dataansvarliges interesse og at alle databehandlere underlægges pligterne, kan det ikke antages at rykke balancen i aftalen, at databehandleren søger sig kompenseret – og dette oplagt efter konkrete afholdte udgifter i stedet for en generel forhøjelse af kontraktsummen til skade for konkurrencen.

Da forordningen hjemler databehandlerens direkte ansvar for eventuelle underdatabehandlere, bør det generelt afdækkes, i hvilket omfang sådanne medvirker. Det er søgt belyst, at selv brugen af et tekstbehandlingsprogram kan involvere en underdatabehandler, som nemt kan være etableret i et tredjeland. Konstruktivt bør denne del af analysen således tage sigte på at kortlægge dataflowet og for hvert behandlingsled vurdere, om kravene er opfyldt, f.eks. at betingelserne for overførsel er til stede. En analyse af dataflowet kan også håndtere den risiko, der består i, at der kan være tilknyttet underdatabehandlere, som hverken den dataansvarlige eller databehandleren er bevidste om.

Forordningen har fsva. forholdet til underdatabehandlere afløst den tvivl, der kunne bestå under direktivet.

Forordningen har imidlertid også skabt nye udfordringer, idet art. 82, stk. 5 synes at udelukke, at der bl.a. i forholdet mellem den dataansvarlige og en solidarisk hæftende databehandler aftales ansvarsbegrænsningsklausuler. Alene de økonomiske konsekvenser for de registrerede af sikkerhedsbrud, der skyldes manglende sikkerhedsforanstaltninger, kan hurtigt overstige databehandlerens aftalte honorar. Da vurderingen af et passende sikkerhedsniveau rummer et skøn og den iboende mulighed for at skønne forkert, kan databehandleren i mangel af muligheder for at begrænse sit ansvar være nødsaget til at indregne et risikotillæg i sit tilbud. Alt efter hvordan dette håndteres, vil der således være tale om en konkurrenceparameter. I den sammenhæng er der af undertegnede stillet spørgsmålstegn ved, om det virkelig kan være hensigten, at parternes kontraktfrihed fsva. ansvarsfordelingen i deres *indbyrdes* forhold underlægges begrænsninger. Forordningens ordlyd efterlader ikke megen tvivl. Den danske betænkning[103] finder dog, at forordningen ikke udelukker sådanne aftaler, hvorimod der perspektiverende til den svenske betænkning[104] kan konstateres, at den nye retsstilling blot er nævnt uden yderligere kommentarer.

Under alle omstændigheder må det forventes, at spørgsmålet om sanktioner og erstatningsansvar i vidt omfang bliver forelagt domstolene allerede grundet det i forordningen tydeliggjorte motiv om, at kendskabet til pligter og de registreredes rettigheder skal udbredes. I denne retning er der

[103] JM's bet. nr. 1565, s. 913 ff.
[104] Betänkande av Dataskyddsutredningen, 2017, s. 277 f.

allerede i Frankrig og Tyskland indført lovændringer, hvormed at krænkelser af de registreredes rettigheder kan behandles under kollektive søgsmål anlagt af interesseorganisationer inden for forbrugerområdet.[105]

Når opmærksomheden på et retsområde stiger, og der er lagt op til en strengere håndhævelse, vil det ikke overraske, at antallet af sager mod dataansvarlige og databehandlere, sidstnævnte enten som direkte sagsøgt eller ved adcitation, vil stige og hvem ved; måske bliver påstande om kompensation for krænkelser af persondataretten lige så udbredte, som påstande om godtgørelse for krænkelse af ansættelsesbevisloven er det inden for ansættelsesretlige sager.

Bilag 1: Eksempel på en utilstrækkelig instruks og databehandleraftale

Uddrag af 'Google Apps General Terms', 2010:

"*1.4 Privacy Policies. Customer acknowledges that it has chosen to have its End Users personal data processed by Google as part of the Services within the scope of the Services' capabilities, which are reflected in the Google Privacy Policies.* ***Customer therefore instructs Google to provide the Services and process End User personal data in accordance with the Google Privacy Policies and Google agrees to do the same.*** *The Google Privacy Policies are hereby incorporated by reference into this Agreement. Customer agrees to protect the privacy of End Users by complying with a policy communicated to End Users which is no less protective than the Google Privacy Policies.*

1.5 Data Protection. In Section 1.4 and Section 1,5, the terms "personal data", "processing", "data controller" and "data processor" shall have the meanings ascribed to them in the EU Directive. For the purposes of this Agreement and in respect of the personal data of End Users, the parties agree that Customer shall be the data controller and Google shall be a data processor. Google shall take and implement appropriate technical and organisational measures to protect such personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access."

Eksemplet vedrører Datatilsynets sag i Odense Kommune. j.nr. 2010-52-0138, Behandling af følsomme personoplysninger i Cloud-løsning.

Se evt. omtale ovenfor under afsnit 3.1.3.3.

[105] Hunton & Williams, Privacy & Information Security Law Blog, indlæg af 22.12.05 og 30.11.2016.

Bilag 2: Databehandlerens straffeansvar

B 2.1. Strafansvaret under direktivet

Efter PDL § 70 straffes den, der som led i behandlingsaktiviteter udført *for* private overtræder de i stk. 1, nr. 1-6 nævnte bestemmelser[106], med bøde eller fængsel indtil 4 måneder. Samme gør den, der overtræder de i stk. 2 nævnte bestemmelser som led i en behandling udført *for* offentlige myndigheder. Det forhold, at databehandleren ifølge PDL ikke som udgangspunkt er erstatningsansvarlig over for den registrerede, medfører ikke, at databehandleren ikke kan pådrage sig et selvstændigt strafansvar ved reglernes tilsidesættelse.

Både PDL § 70, stk. 1 og stk. 2 viger for højere straf ifølge anden lovgivning, f.eks. straffelovens § 264 d om krænkelse af privatlivet hørende forhold ved *videregivelse* af private meddelelser eller billeder, der åbenbart kan forlanges offentligheden unddraget, eller straffelovens kapitel 16 om forbrydelser i offentlig tjeneste eller hverv, herunder tilsidesættelse af tavshedspligten under eller efter ansættelsen.

Da fængselsstraf ikke kan idømmes juridiske personer og behandlinger af rent privat karakter er undtaget ved PDL § 2, stk. 3, er denne sanktionsmuligheds anvendelsesområde begrænset, hvorfor det centrale for den typiske databehandler er bødeansvaret.

En analyse af bødeniveauets størrelse i årene 2000-2010 viser, at niveauet kun sjældent overstiger 10.000 kr.[107] I perioden er dette ifølge Datatilsynets oplysninger alene sket to gange; den ene sag vedrørende en virksomheds behandling af følsomme oplysninger (bødeforlæg på 10.000 kr.), og den anden vedrørende salget af en hel kundedatabase (bøde på 25.000 kr.). Om bødeniveauet bemærkes endvidere, at sager, der også rummer overtrædelse af anden bødesanktioneret lovgivning, f.eks. markedsføringsloven, næppe kan anvendes til at sige noget om bødeniveauet i PDL, idet en gennemgang af retspraksis tillige viser, at sådanne bøder sjældent udspecificeres eller fastsættes uafhængigt.

Hertil kommer den antagelse, at bødeforelæg ikke nødvendigvis størrelsesmæssigt er fastsat under iagttagelse af de retssikkerhedsgarantier, som anvendes hos domstolene, hvorfor bødeniveauet skabt ved vedtagelsen af sådanne ikke nødvendigvis udtrykker gældende ret. Det må hertil antages, at mindre bøder eller bødeforlæg vil blive betalt allerede af den grund, at andet ikke kan svare sig ud fra rene ressourcebetragtninger.

B 2.2. Straffeansvaret under forordningen

Under PDL kan juridiske personer pålægges straf efter straffelovens kapitel 5.[108] Datatilsynet er ikke under PDL kompetent til at udstede administrative bødeforelæg, hvilket er overladt til Anklagemyndigheden på baggrund af en politianmeldelse, evt. fra Datatilsynet.[109]

---

[106] Omfattet er bl.a. PDL § 41, stk. 3, 2. pkt., der også pålægger databehandleren at træffe fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, samt PDL § 53, der pålægger visse EDB-servicebureauer en anmeldelsesforpligtelse.

[107] Gennemgangen er baseret på Dt's årsberetninger, 2008, 2009 og 2010, idet disse udgør nyeste foreliggende oversigt, som samtidig indeholder de ved bødeforelæg udenretligt afgjorte sager.

[108] Ifølge straffelovens § 27, stk. 2, kan statslige myndigheder og kommuner alene straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private. Blume vurderer i U2014B.337, *Offentlige myndigheders persondataansvar*, at der under forordningen burde sikres et mere tilstrækkeligt værn over for overtrædelser begået af offentlige myndigheder, idet bøder ikke er velegnede, idet myndighedens opgaver jo skal udføres uanset evt. pålagte bøder.

[109] *Lov om behandling af personoplysninger*, 2015, s. 661 bemærker dog, at Datatilsynet fsva. rent formodede strafbare forhold har videreført det tidligere Registertilsyns praksis om indledningsvis at meddele forbud eller påbud, og dermed give virksomheden mulighed for at bringe forholdene i orden.

Forordningen forudsætter imidlertid, at tilsynsmyndighederne som udgangspunkt i tillæg eller som alternativ til sine øvrige beføjelser[110] kan pålægge administrative bøder jf. forordningens art. 58, stk. 2, litra i.[111]

I det tilfælde, hvor medlemslandets retssystem ikke muliggør administrative bøder, kan medlemslandet vedtage en procedure, hvorefter tilsynsmyndigheden tager det indledende skridt til bøden, som endeligt pålægges af domstolene. Hensigten er formentlig at muliggøre et system svarende til de områder i dansk ret, hvor offentlige myndigheder kan udstede administrative bødeforelæg, idet der således er tale om forelæggelsen af en bøde for lovovertræderen, som enten frivilligt kan vedtage denne eller lade sagen automatisk overgå til domstolssystemet, hvor bøden kan idømmes.

Forordningens præambel 151 nævner på baggrund af en indsigelse fra dansk side, at bøderne i Danmark kan anvendes ved, citat: "*… at bøderne pålægges af de kompetente nationale domstole som en strafferetlig sanktion*". Formuleringen udelukker formentlig hverken den i Danmark under direktivet anvendte løsning, hvor Anklagemyndigheden kan udstede et bødeforelæg, eller den alternative løsning, at Datatilsynet gøres kompetent til at udstede administrative bødeforelæg, som det kendes fra andre danske retsområder.[112] [113] [114]

Uanset hvilken løsning Danmark vælger at anvende, skal bøderne være effektive og i virkning svare til den praksis, som udvikler sig i de øvrige medlemslande fsva. administrative bøder, herunder at bøderne skal være proportionelle og have en afskrækkende virkning i almindelighed jf. art. 83, stk. 9.

Forordningen fastsætter i art. 83, stk. 4, litra a, at overtrædelse af den dataansvarliges og databehandlerens forpligtelser fsva. børns samtykke (art. 8), behandling uden identifikation (art. 11), foranstaltningerne i art. 25-39, herunder databeskyttelse gennem design og default, fælles dataansvarlige, repræsentanter, databehandlere, samarbejde med tilsynet, sikkerhedsforanstaltninger, anmeldelsespligt ved sikkerhedsbrud, konsekvensanalyse og høring, DPO samt regler om certificering (art. 42-43), kan medføre bødestraf op til 10.000.000 euro eller 2 % af en virksomheds globale årsomsætning, såfremt denne er højere.

Ifølge stk. 5 kan overtrædelse af de grundlæggende behandlingsprincipper og -hjemler (art. 5, 6, 7 og 9), de registreredes rettigheder i art. 12-22, overførsel af oplysninger til tredjelande (art. 44-49), specifikke behandlingssituationers regulering i national ret (art. 85-91), og tilsynets påbud,

---

Politianmeldelse kan dog indgives af andre, herunder den registrerede.

[110] Herunder at udtale kritik, give advarsler eller påbud om forordningens overholdelse, udstede forbud eller begrænsning af behandling, herunder suspension af overførsler jf. art. 58, stk. 2, litra a-j.

[111] Hensynet er ifølge præambel 150 at sikre harmonisering i anvendelsen af bødestraf.

[112] Sidstnævnte løsning, hvorefter offentlige myndigheder gives kompetence til at udstede administrative bøde*forelæg* er ikke sjældent anvendt i Danmark, idet konstruktionen formentlig ikke er i strid med grundlovens § 3. F.eks. kan bl.a. Finanstilsynet, Fødevarestyrelsen samt Arbejdstilsynet inden for visse rammer udstede administrative bødeforelæg – se f.eks. Arbejdstilsynet ved bekendtgørelse nr. 107 af 28. februar 2002 med senere ændringer om anvendelse af administrativt bødeforelæg ved overtrædelse af arbejdsmiljølovgivningen.

[113] Det fremgår af Justitsministeriets besvarelse af 07.11.2014 (j.nr. 2014-0030-2566) af spørgsmål nr. 1605 (Alm. del) stillet af Folketingets Retsudvalg på baggrund af Kommissionens forslag til forordningen, at ministeret finder, at citat: "*I dansk retspleje er det et grundlæggende princip, at bøder kun kan pålægges ved domstolene og efter retsplejelovens regler*", at "*Bestemmelsen i grundlovens § 3 må antages at indebære, at lovgivningsmagten ikke i almindelighed kan henlægge behandlingen af strafferetlige bødesager til administrative myndigheder*" og at "*Bestemmelser i forslag til EU-retsakter, navnlig direktiver og forordninger, der pålægger Danmark at indføre administrative bøder på bestemte områder, kan derfor give anledning til forfatningsretlige betænkeligheder*".

[114] Antagelsen synes bekræftet ved JM's bet. nr. 1565, s. 933 ff.

forbud eller begrænsning, suspension samt forhindring af tilsynets adgang (art. 58, stk. 1-2), straffes med bøde op til 20.000.000 euro eller 4 % af en virksomheds globale årsomsætning, såfremt denne er højere.

Det bemærkes, at hverken stk. 4 eller 5 pålægger bødestraf for overtrædelse af art. 10 om personoplysninger vedr. straffedomme og lovovertrædelser. Dette skyldes formentlig, at det er overladt til medlemsstaterne at udfylde bestemmelsen nationalt, herunder formentlig også med straffebestemmelser jf. præambel 151 og art. 84.

Herudover bemærkes, at overtrædelse af pligten til at underrette registrerede om sikkerhedsbrud i art. 34 udgør en mindre krænkelse end undladelsen at give meddelelse om behandlingen jf. art. 13-14, hvilket formentlig skyldes, at det forudsættes, at tilsynsmyndigheden bistår den dataansvarlige i beslutningen herom.

Det er antageligt hævet over enhver tvivl, at det danske bødeniveau for overtrædelse af PDL ikke kan fastholdes under forordningen, alene ud fra det synspunkt, at bøderne skal have afskrækkende virkning jf. stk. 9. Dette har bøder på 25.000 kr. i grelle tilfælde næppe.

De høje bødeniveauer medfører naturligvis ikke, at enhver overtrædelse af forordningen medfører eksorbitant høje bøder. I størrelsen ligger en vis symbolsk effekt, da det erindres, at forordningen har til formål at skabe større respekt om databeskyttelse.

Ved udmålingen af bøder tages hensyn til skærpende og formildende omstændigheder jf. stk. 2, herunder eksempelvis overtrædelsens karakter og skadevirkning, graden af fortsæt og uagtsomhed samt trufne afværgeforanstaltninger og samarbejdsviljen med tilsynet. Ud fra sammenhængsmekanismen og det tilsigtede europæiske samarbejde overlades det til Databeskyttelsesrådet og formentlig også EU-domstolen at fastlægge bødeniveauet og afvejningen af formildende og skærpende omstændigheder.

Bøder pålægges individuelt den, der har overtrådt loven. Således er der ikke i forordningen fastsat regler om bødehæftelse, hvormed eksempelvis den dataansvarlige må hæfte for en bøde, som alene kan pålægges databehandleren, f.eks. fordi at denne helt uretmæssigt har (mis)brugt oplysninger i ulovlige formål.

Det bemærkes, at medlemslandene i art. 83, stk. 7 er overladt beslutningen om, hvorvidt offentlige myndigheder skal kunne pålægges administrative bøder. Imod at pålægge offentlige myndigheder bøder taler, at pengene principielt blot flyttes fra den ene kasse til den anden inden for 'statskassen'. For taler imidlertid, at flere af ovennævnte eksempler på Datatilsynets praksis viser, at offentlige myndigheder også overtræder reglerne. Kan det offentlige ikke pålægges bøder, kan det ikke udelukkes, at det i en trængt økonomi ville være belejligt at gå på kompromis med sikkerheden for derved at billigøre behandlingen. Således risikeres udviklingen af et parallelt marked for behandlingstjenester. [115]

[115] Ifølge den svenske betænkning om forordningen, *Betänkande av Dataskyddsutredningen*, 2017, s. 282 ff, foreslås muligheden for at pålægge offentlige myndigheder bøder videreført i svensk ret. Dog foreslås vedtagelsen af et beløbsmæssigt loft (s. 290), der skal være mindre end dét, der gælder for private dataansvarlige, idet der henvises til myndigheders strafansvar inden for bl.a. patienterstatnings-, miljø- og arbejdsmiljølovgivningen samt EU-Kommissionens forslag af 10.01.2017 til forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer mv., art. 66, stk. 2 og 3, hvorefter der også for disse organer gælder mildere beløbsgrænser (COM(2017) 8 final, 2017/0002 (COD)).

Hvad Danmark beslutter og hvordan straffelovens § 27, stk. 2 vil blive inddraget, er ikke afklaret ved denne afhandlings indlevering.[116] [117] [118]

Medlemsstaterne gives efter art. 84 mulighed for at vedtage andre strafferetlige sanktioner, herunder også fsva. overtrædelsen af nationale regler, dog således at sanktionerne ikke strider mod forbuddet mod gentagen retsforfølgning (ne bis in idem) jf. præambel 149.

Disse regler kan som i PDL § 71 bestå i rettighedsfrakendelse til udøvelse af virksomhed, eller konfiskation af overskud.

Litteraturfortegnelse

Juridisk faglitteratur:

- Anne S. Y. Cheung & Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing*, Edward Elgar Publishing, UK & USA, 2015.
- Bo von Eyben, *Juridisk ordbog, 14. udgave*, Karnov Group, 2016
- Charlotte Bagger Tranberg, *Nødvendig behandling af personoplysninger*, Forlaget Thomson A/S, 2007.
- Henrik Waaben, Kristian Korfits Nielsen, *Lov om behandling af personoplysninger med kommentarer*, 3. udgave, Jurist- og Økonomforbundets Forlag, 2015.
- Martin Gräs Lind, *Medarbejderes integritetsbeskyttelse i dansk ret – med særlig fokus på databeskyttelse, kontrol og overvågning i den private sektor*, Jurist og Økonomforbundets Forlag, 2006.
- Nis Peter Dall, Jesper Langmark og Amalie Langebæk, *Persondataforordningen – en håndbog for praktikere*. Ex Tuto A/S, 2016
- Peter Blume og Jens Kristiansen, *Persondataret i ansættelsesforhold*, Jurist og Økonomforbundets Forlag, 2011.
- Peter Blume, *Persondataretten – i en brydningstid*, Jurist- og Økonomforbundets Forlag, 2014.
- Peter Blume, *Den Nye Persondataret – Persondataforordningen*, Jurist og Økonomforbundets Forlag, 2016.
- Ruth Nielsen og Christina D. Tvarnø, *Retskilder & Retsteorier*, 3. reviderede udgave, Jurist- og Økonomforbundets Forlag, 2011.
- Serge Gutwirth, Ronald Leenes, Paul De Hart et al., *Reforming European Data Protection Law*, Springer Science 2015
- Serge Gutwirth, Ronald Leenes, Paul De Hart, *Data Protection on the Move*, Springer Science 2016
- Ulrik Rammeskow Bang-Pedersen og Lasse Højlund Christensen, *Den Civile Retspleje*, 3. udgave, Pejus, 2015.

[116] Folketingets Retsudvalg (beretning om datasikkerhed af 15.01.2015) finder , at citat: "… *offentlige myndigheder og private virksomheder bør gøres til genstand for samme sanktionsmuligheder, og noterer sig, at denne ligestilling efter arbejdsgruppens opfattelse også er udgangspunktet i det foreliggende forslag til forordning.*"

[117] *Persondataforordningen – en håndbog for praktikere*, 2016, s. 139 forventer, at offentlige myndigheder vil kunne pålægges administrative bøder.

[118] JM's bet. nr. 1565 henskyder spørgsmålet til lovgiver, citat: "*Der vil i forbindelse med vedtagelsen af en ny persondatalov skulle tages stilling til, hvorvidt der skal gives adgang til at pålægge offentlige myndigheder bøder*".

Juridiske tidsskrifter etc.:

- Jens Harkov Hansen, *Persondataloven – gælder den også for advokater?*, Advokaten årg. 94, nr. 7 (2015), s. 41 f.,
- Jens Harkov Hansen, *Persondataforordningen rammer (også) advokatvirksomheder*, Advokaten årg. 95, nr. 7 (2016), s. 38 f.
- Carsten Munk-Hansen, *Ansvarsbegrænsning i rådgivningsaftaler*, UfR 2011B.21
- Peter Blume, *Offentlige myndigheders persondataansvar*, UfR 2014B.337
- Peter Blume, *Persondataret årgang 2018*, Revision og regnskabsvæsen, nr. 8 (2016)

Retspraksis:

- U 2005.1113 Ø (Henvisning, UfR)
- U 2005.1639 V (Henvisning, UfR)
- U 2007.1167 V (Henvisning, UfR)
- U 2008.772/2 S (Henvisning, UfR)
- U 2011.2343 H (Henvisning, UfR)

- EU-Domstolen, C-272/83, *Kommissionen mod Italien*
- EU-Domstolen, C-131/12, *Google Spain SL, Google Inc. mod AEPD (Spanien)*
- EU-Domstolen, C-362/14, *Safe Harbour*

Datatilsynets praksis:

- J.nr. 2000-219-0019 (*Inkassobureau som databehandler*)
- J.nr. 2005-632-0077 (*Videregivelse af oplysninger fra CPR til private virksomheder (I)*)
- J.nr. 2007-212-0042 (*FDB og Coop Danmark A/S' medlemsprogram*)
- J.nr. 2010-52-0138 (*Behandling af følsomme personoplysninger i Cloud-løsning*)
- J.nr. 2011-082-0216 (*Behandling af personoplysninger i cloud-løsningen Office 365*)
- J.nr. 2014-623-0025 (*Inspektion af Nyborg Kommunes brug af Skolesundhed.dk*)
- J.nr. 2015-621-0035 (*Inspektion hos Styrelsen for arbejdsmarked og Rekruttering*)

Andet materiale:

- Artikel 29-gruppen, *Udtalelse 1/2010 om begreberne "registeransvarlig" og "registerfører"*, af 16.02.2010, (00264/10/DA, WP169).
- Artikel 29-gruppen, revideret vejledning af 05.04.2017, Guidelines on Data Protection Officers (WP243)
- Artikel 29-gruppen, *FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/*EC, af 12.07.2010, (00070/2010/EN, WP 176).
- EU-Kommissionens henstilling 2008/473/EF af 08.07.2008 om revisorers erstatningsansvar.
- EU-kommissionen, *Commission Decision C(2010)593, Standard Contractual Clauses (processors)*
- EU-Kommissionen, *Fact Sheet – European Data Protection Reform*, 01/2016
- Datatilsynets årsberetning 2000
- Datatilsynets årsberetning 2001
- Datatilsynets høringsnotat af 01.06.2007, *Sikkerhed ved transmission af personoplysninger via internettet i den private sektor* (j.nr. 2005-630-0002)
- Datatilsynets anmeldelsesblanket med tilhørende vejledning, EDB-servicebureau, (2008).

- Datatilsynets vejledning, EDB-servicebureauer, af 06.05.2015 (https://www.datatilsynet.dk/erhverv/edb-servicebureau/)
- Datatilsynets vejledning af 06.05.2015, *Hvornår er man henholdsvis dataansvarlig og databehandler?* (https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/).
- Datatilsynets orienteringsbrev af 14. maj 2012 til Forsikring og Pension om nye regler om private dataansvarliges anmeldelsespligt (j.nr. 2012-213-0022)
- Information Commissioner's Office (ICO), *Data controllers and data processors: what the difference is and what the governance implications are*, 20140506 (vejledning fra tilsynsmyndigheden i Storbritannien)
- Justitsministeriets notat af 23.06.2016, *Justitsministeriets arbejde med EU's generelle databeskyttelsesforordning*, (j.nr. 2016-7910-0001)
- Justitsministeriets betænkning nr. 1565 af 24.05.2017, *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, del 1 (bind 1-2) samt del 2 (forkortet JM's bet. nr. 1565)
- Betänkande av Dataskyddsutredningen, *Ny dataskyddslag - Kompletterande bestämmelser till EU:s dataskyddsförordning*, 2017 (den svenske betænkning)
- Hunton & Williams, Privacy & Information Security Law Blog, indlæg af 22.12.05 (*Germany Adopts Law to Enable Class Actions for Data Protection Violations*) og 30.11.2016 (*France Adopts Class Action Regime for Data Protection Violations*).

Diverse:
- Gyldendals onlineleksikon, Den Store Danske
- Gyldendals Engelsk-Dansk Fagordbog, 2017

Foruden en generel tak til forfatterne bag ovennævnte litterære udgivelser, rettes en særlig tak til undertegnedes vejleder på afhandlingen, persondataspecialist (Bech-Bruun) og ph.d., Charlotte Bagger Tranberg, som tidligt i processen havde øje for den nødvendige afgrænsning og løbende har været en stor hjælp med teoretiske og praktiske vinkler.
En særlig tak rettes også til indehaver af Advokatfirmaet Lexius, advokat (H) og ph.d., Martin Gräs Lind, som i sin tid vakte min interesse for persondataretten og under arbejdet med denne afhandling har udgjort en særlig støtte og velvilligt – ligesom Charlotte – har delt ud af sin mangeårige erfaring inden for persondataretten og tilstødende retsområder.

Anvendte forkortelser af særlig karakter:

PDL	Persondataloven
RPL	Retsplejeloven
EMRK	Den Europæiske Menneskerettighedskonvention
EAL	Erstatningsansvarsloven
Jm	Justitsministeriet
Dt	Datatilsynet
J.nr.	Journalnummer
Bet.	Betænkning
Fsva.	For så vidt angår