PERSONDATAFORORDNINGEN

- *Et Cand.Merc.Jur.-speciale med fokus på databeskyttelsesrådgivere*

Navne / studienummer:
Alexander Høy / 25462
Emil Skov / 31431

Emne:
Persondataforordningen

Speciale afleveret:
15/05/2018

Vejledere:
Juridisk: Mette Vestergaard Huss
Økonomisk: Lasse Holt

Antal karakterer / normalsider:
260.621 / 114,56 ud af 273.000 / 120

Abstract

This master thesis is a legal analysis on whether Danish scout associations, that are subjects to the The Danish General Adult Education Act (folkeoplysningsloven), are bound to appoint a Data Protection Officer (DPO) according to the General Data Protection Regulation (GDPR) of the European Union. It is discovered in chapter 2 how the scout associations will not have to appoint a DPO, since none of the provisions are meet. There are several provisions, which are all regulated in the GDPR article. 37, sec. 1, schedule b-c) and article 37, sec. 4.

The economic focus is whether the GDPR is economically reasonable, and how the positive effects ultimately will end up surpassing the negative effects. Chapter 3 finds out the DPO is an influential game changer when the positive economic aspects of implementing the GDPR will have to exceed the negative. It is therefore concluded, that the GDPR will end up with more positive effects when the regulation is complied with possible. Game-theory including Principal/agent-theory and Theory of the Firm clarifies this.

The final part of the thesis investigates if it is possible to make the regulation more efficient by changing an article in the regulation. The legal proposal in the end is based on the knowledge from chapter 2 and 3. It is discovered, that the scout associations can have unlimited amount of personal data, but because of none of the provisions to appoint a DPO are meet, a DPO never has to be appointed according to the regulation.

Therefore is the proposal, that an organization with no personal data as a core activity, can be forced to appoint a DPO, if they have personal data in a sufficient large scale, and they meet two of the other provisions *regular and systematic monitoring* or data processing as a core activity.

Keywords: *General Data Protection Regulation (GDPR), Data Protection Officer (DPO), Game Theory, Scout associations.*

Indholdsfortegnelse

Kapitel 1

1.1 Indledning

Den 25. maj 2018 træder den nye databeskyttelsesforordning 2016/679[1] (efterfølgende nævnt som *Forordningen*) i kraft, og denne erstatter samtidigt databeskyttelsesdirektivet[2] (efterfølgende nævnt som *Direktivet*), der regulerer persondataretten frem mod Forordningens ikrafttræden.[3]

Direktivet blev taget i brug i år 1998, og efterfølgende blev det implementeret i de nationale lovtekster frem til år 2000, hvor persondataloven[4] trådte i kraft, som vi kender den i dag.

Forordningen introducerer adskillige nye forpligtelser for databehandlere og dataansvarlige[5] samt en styrkelse af de fysiske personers (herefter kaldet data-subjekternes) rettigheder.

Eksempler på disse er bl.a.:

- øget dokumentationskrav af de registrerede,
- retten til dataportabilitet[6],
- retten til at blive glemt[7] og
- hårdere sanktioner i form af høje bødetakster[8], såfremt Forordningen ikke overholdes.

Med Forordningen kommer ligeledes en forpligtigelse for offentlige myndigheder, og i nogle tilfælde private aktører, til at udpege en databeskyttelsesrådgiver (efterfølgende nævnt som *DPO*).[9] Det er udpegelsen af DPO'er, der er i betragtning i dette speciale. Mere specifikt vil specialets juridiske fokus være, at undersøge om foreninger, der modtager økonomisk støtte fra kommunen, er underlagt kravet i Forordningens artikel 37 om udpegelsen af en DPO. Et

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
[2] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
[3] Forordningens artikel 94, stk. 1.
[4] LOV nr. 429 af 31/05/2000.
[5] Disse begreber forklares nærmere på side 25 og frem.
[6] Forordningens artikel 20.
[7] Denne ret udspringer af sag C-131/12 (også kaldet Google-dommen). Retten til at blive glemt giver den/de registrerede ret til at få persondata vedrørende dem selv slettet, såfremt der ikke længere er lovhjemmel til at behandle dataen. Retten implementeres i art. 17 i Forordningen.
[8] Persondataforordningens artikel 83 og 84.
[9] Persondataforordningens artikel 37.

sådan krav kan blive skelsættende for en forening, der i forvejen er afhængig af økonomisk støtte for at fungere, da ansættelsen af en DPO kan blive meget bekostelig.

I specialets juridiske kapitel tages der udgangspunkt i (klassiske) spejderforeninger for børn og unge (herefter kaldet spejderforeningerne). Der er tale om frivillige foreninger, hvis formål er "*(...) at oplære børn og unge om selvstændighed, medansvar, demokratisk livsholdning og mellemfolkelig forståelse".*[10] Spejderforeningernes primære aktiviteter er klassiske spejderaktiviteter som arrangering af ugentlige møder, udvikling, læring, lejrture og generelle friluftsaktiviteter. Der betales et medlemskontingent, men ellers har spejderforeningerne ingen anden fast indtægt udover de bevilligede kommunale tilskud. Foreningerne er at betragte som folkeoplysende foreninger efter folkeoplysningslovens § 4, stk. 1, nr. 2,[11], og derfor kan de søge om tilskuddet.[12]

Ovenstående udgangspunkt er ikke et udtryk for, at specialets juridiske kapitel bygges op omkring en eksisterende spejderforening og dennes reelle forhold, da den nødvendige data ikke har været muligt at få adgang til ved udarbejdelsen af specialet. Udgangspunktet er udarbejdet for at beskrive den foreningstype og -struktur, der blot danner grundlag for specialet. I specialet fokuseres der således på folkeoplysende spejderforeninger efter folkeoplysningsloven § 4, stk. 1, nr. 2, og om disse er forpligtede til at udpege en DPO efter Forordningens art. 37.

Specialets økonomiske kapitel vil først udlede de negative konsekvenser ved implementeringen af Forordningens regler i det danske samfund, og derefter udledes de positive. Der vil i denne sammenhæng blive set på, hvornår Forordningen er økonomisk efficient, og hvilken rolle DPO'erne spiller i denne afvejning.

Det integrerede kapitel vurderer, om der kan foreslås en ændring af Forordningens art. 37, så den bliver mere optimal for nytteefficiensen. Dette gøres primært på baggrund af den opnåede viden fra den foregående juridiske og økonomiske analyse.

1.2 Problemstillinger

Specialet vil tage udgangspunkt i nedenstående problemstillinger:

[10] Formålet (og til dels aktiviteterne) er fra KFUM-spejderne - Se http://www.faxekommune.dk/sites/default/files/bilag/kfum_-_kongsted_-_gennemgang_af_folkeoplysende_foreninger.pdf, (tilgået 13/05/2018).
[11] Bekendtgørelse af lov om støtte til folkeoplysende voksenundervisning, frivilligt folkeoplysende foreningsarbejde og daghøjskoler samt om Folkeuniversitetet (folkeoplysningsloven) - LBK nr. 854 af 11/07/2011.
[12] Jf. folkeoplysningslovens § 2, stk. 2, nr. 2.

1.2.1 Juridisk problemstilling

Hvorvidt er folkeoplysende spejderforeninger forpligtede til at udpege en DPO efter Forordningens art. 37?

1.2.2 Økonomisk problemstilling

Hvorvidt er Forordningen økonomisk efficient ud fra en nytteteoretisk tilgang, og under hvilke omstændigheder kan DPO'en bedst påvirke den mulige efficiens?

1.2.3 Integreret problemstilling

Hvorledes er det muligt at ændre Forordningens art. 37 for at gøre Forordningens økonomiske udledninger mere efficiente?

1.3 Afgrænsning

1.3.1 Juridiske afgrænsning

Der afgrænses i specialet til folkeoplysende spejderforeninger i Danmark, og Forordningens art. 3, stk. 2, og stk. 3 (om dataansvarlige uden for EU) vil derfor ikke blive inkluderet i specialet.

1.3.2 Økonomisk afgrænsning

Kun mikroøkonomiske udregninger bliver inddraget i specialet, da der vil være fokus på parternes individuelle nytte før og under Forordningen. Makroøkonomiske udregninger havde været relevant at analysere, men har grundet opgavens omfang ikke været muligt. Derfor vil blot makroøkonomiske aspekter og argumenter indgå.

Afledte effekter ved implementeringen af Forordningen vil ligeledes ikke blive inkluderet i specialet, da dette er usikkert at konkretisere og påvise økonomisk.

1.4 Synsvinkel

Specialet er skrevet ud fra et samfundsmæssigt synspunkt. Danmark er kendt for sit mangfoldige foreningsliv - så kendt, at det bliver kaldt *foreningernes land*.[13] Foreninger spiller således en stor rolle i dagens Danmark, og de forskellige sektorer i det danske samliv

[13] Ole Hasselbalch, 2009, *Foreninger*, Nyt Juridisk Forlag, s. 9.

er tydeligt præget af de forskellige foreningsformers indflydelse. Specialets juridiske kapitel går netop ind og ser på, hvordan Forordningen påvirker de folkeoplysende foreninger, og derfor også det danske samfund. Det økonomiske kapitel ser ligeledes på de fordele og ulemper, der samfundsøkonomisk kommer til at ske ved Forordningens indtræden. Det integreret kapitel har også fokus på, hvordan Forordningen kan gøres mere samfundsefficient ud fra et retspolitisk synspunkt. Derfor har dette speciale overordnet set samfundets synspunkt.

1.5 Juridisk metode og fremgangsmåde

For at kunne foretage en fyldestgørende juridisk analyse, er det nødvendigt at forholde sig til retskildelæren og den retsdogmatiske metode.[14] I nedenstående afsnit vil begge begreber blive introduceret, da specialet er bygget op om disse.

1.5.1 Retskildelæren

Retskilderne der indgår i retskildelæren, og som er opregnet af Alf Ross[15], består henholdsvis af;

- regulering,
- retspraksis,
- sædvane og
- forholdets natur.

Efter den retsrealistiske opfattelse indgår de fire retskilder ikke i et reguleringshierarki. Dette betyder fx, at retskilden *regulering* ikke har forrang (eller en retskildemæssig større værdi) over *forholdets natur*, hvorved alle fire retskilder er lige anvendelige til løsningen af en juridisk problemstilling.[16]

Inden for retskilden *regulering*, der omfatter lovgivning, bekendtgørelse, vejledning, cirkulære o.l., findes der dog et hierarki, hvor de forskellige reguleringstyper har forrang for hinanden i kraft af *lex superior*-princippet.[17] Dette princip er et udtryk for, at lovregler af

[14] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 34.
[15] Alf Niels Christian Ross er en nu afdød jurist og retsfilosof. Efter Alf Ross' ideologi er udledelsen af gældende ret selve hjertet i retsvidenskaben. Den retsdogmatiske metode skal derfor anvendes på en måde, der skaber sikker viden for, hvad gældende ret er i den konkrete situation.
[16] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 81.
[17] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 248.

"lavere rang" må fravige, såfremt de strider imod en reguleringstype af højere rang.[18] Dermed er en almindelig lov ugyldig, hvis den strider imod grundloven, og en bekendtgørelse er ugyldig, hvis den strider imod den lov, hvorfra den er udledt af.[19]

1.5.2 Retsdogmatisk metode

I det juridiske kapitel bliver den retsdogmatiske metode anvendt. Den retsdogmatiske metode er en juridisk analytisk metode, der benyttes til at systematisere, analysere og (i sidste ende) udlede gældende ret - *de lega lata*.[20] *De lega lata* er udtryk for det resultat, som en domstol ville finde frem til ved anvendelsen af de relevante retskilder og den retsdogmatiske metode.[21]

I den retsdogmatiske metode bliver retskilderne analyserede i en bestemt rækkefølge. Den retsdogmatiske analyse vurderer og analyserer først retskilden *regulering* og derefter hhv. *retspraksis*, *retssædvane* og *forholdets natur*.[22]

Når den retsdogmatiske metode benyttes til at løse en juridisk problemstilling, ses der først på sagens faktum. Faktum skal forstås som de konkrete hændelser, der har ført til behovet for at træffe en afgørelse. Efterfølgende vurderes retsfaktum, som er de kendsgerninger, den efterfølgende afgørelse kommer til at hvile på. Retsfaktum analyseres ved hjælp af jus, som er en samlet betegnelse for de relevante retskilder, der vedrører retsfaktum. Brugen af jus og retsfaktum fører i sidste ende til retsfølgen, som er den konklusion, en domstol vil finde frem til givet de faktiske omstændigheder.[23]

1.5.3 EU-retten og dens forhold til dansk ret

Da EU-retten finder anvendelse i dette speciale, skal de retskilder, der anvendes, ligeledes inkluderes i dette kapitel. Indenfor EU-retten skelnes der mellem primær- og sekundær ret, hvorfor der findes yderligere retskilder end beskrevet i det ovenstående afsnit.[24]

Primærretten:

Primærretten udgøres af EU's traktatgrundlag, grundlæggende rettigheder og almindelige

[18] Der findes yderligere to andre lex-regler, og disse er henholdsvist *lex specialis* og *lex posterior*. Disse har været relevante at nævne da Lex superior-princippet ikke er den eneste Lex regel. De resterende to vil dog ikke blive anvendt i specialet.
[19] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 82.
[20] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 31.
[21] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 31.
[22] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 34.
[23] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 36.
[24] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 135.

retsprincipper. Traktaten om Den Europæiske Union (TEU) og Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) udgør traktatgrundlaget, og de lægger en ramme om EU-retten vedrørende EU's kompetencer og formål. Sammen med de grundlæggende rettigheder og de almindelige retsprincipper danner de EU's primære ret.[25]

Sekundærretten:
Sekundær ret eller *bindende sekundær regulering* udgøres af forordninger, direktiver og afgørelser fra EU-domstolen, der alle er afledt af primærretten.

Forordninger er almengyldige, hvilket betyder, at de ikke kun retter sig til specifikke adressater, men de finder bindende anvendelse på alle borgere, myndigheder, virksomheder og organisationer, der er underlagt forordningen i dens EU-retlige form. Når en forordning træder i kraft, skal medlemsstaternes lovtekst indrettes således, at den overholder forordningen i dens EU-retlige form.[26] Der kan dog kræves i en forordningen, at medlemsstaterne foretager visse gennemførelsesforanstaltninger. Dette er fx at ændre eller gennemføre supplerende national lov for at overholde forordningen.[27]

I modsætning til forordninger er det op til medlemsstaterne selv at beslutte, hvordan et direktiv, og dets tilsigtede mål, skal implementeres. Et direktiv er altså kun bindende i forhold til dets mål, men ikke i forhold til formen for implementeringen og hvordan målet skal nås.

Der skelnes mellem minimum og fuldkommen harmonisering ved direktiver. Ved minimumsharmonisering bliver der fastlagt minimumskrav i forbindelse med direktivets mål, som skal opfyldes af alle EU-landene. Derudover kan medlemsstaterne sætte yderligere krav end de fastlagte minimumskrav. Ved fuldkommen harmonisering fastlægges derimod et niveau, der hverken må implementeres højere eller lavere i de enkelte medlemsstater.[28]

En afgørelse fra EU-domstolen er bindende for de adressater, den er rettet imod. Både medlemsstater, borgere, virksomheder og andre organisationer (eller en kombination) kan være adressater. Afgørelser er direkte anvendelige, og der skal derfor ikke ske nogen transformation til national ret.[29]

Soft law:

[25] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 136-140.
[26] TEUF art. 288, 2. led.
[27] Neergaard, U., & Nielsen, R. (2010). EU ret (6. udg.). København: Karnov Group, s. 223.
[28] Neergaard, U., & Nielsen, R. (2010). EU ret (6. udg.). København: Karnov Group, s. 131-132.
[29] TEUF art. 288, 4. led.

Soft law, også kaldet ikke-bindende sekundærregulering, består bl.a. af Kommissionens meddelelser, henstillinger og udtalelser, og det er dermed en retskilde, der ikke er bindende for modtageren. Vejledninger tilhører også denne kategori. Det skal til gengæld bruges som fortolkningsbidrag.[30]

1.5.3.1 EU-rettens forrang og EU-konform fortolkning

EU-retten har forrang for national ret. Dette blev tydeliggjort i EU-afgørelsen *Costa mod Enel-sagen* fra 1964.[31] EU-domstolen gjorde det klart, at EU-retten hverken er en folke- eller nationalret, men den er derimod en tredje ret, der har forrang for medlemsstaternes nationale love. EU-rettens forrang gælder ligeledes for Danmark, da Danmark er en af de nuværende 28 medlemslande af EU.[32]

Medlemslandene har endvidere pligt til at foretage EU-konform fortolkning. Pligten til EU-konform fortolkning betyder, at de nationale domstole skal anvende det videst mulige fortolkningsskøn, der er at finde i national ret, for at opnå en EU-konform løsning.[33] Pligten til EU-konform fortolkning i forbindelse med implementering af direktiver udspringer af TEUF art. 288, stk. 3. Denne hjemmel er derfor kun relevant i forbindelse med fortolkning og implementering af direktiver. Dog henvises der også til TEU art. 4, stk. 3, som hjemmel til pligten til EU-konform fortolkning, og denne hjemmel (i modsætning til TEUF art. 288, stk. 3) kan benyttes på enhver retskilde.[34]

1.6 Økonomisk fremgangsmåde, metode og forudsætninger

1.6.1 Økonomisk opbygning

Det økonomiske kapitel er bygget op som følgende:

[30] TEUF art. 288, 5. led.
[31] Sag 6/64: Sagen omhandlede den italienske borger Flaminio Costa og det italienske, statsejede elselskab ENEL. Flaminio nægtede som en protest mod nationaliseringen af elværker at betale sin elregning. Han mente, at den italienske lov, der tillod nationaliseringen, stred mod EU-retten, hvilket de italienske myndigheder nægtede. EU-retten fastslog her, at for at EU-retten kan fungere, kræver det, at denne har forrang for national lov.
[32] Forrest, M. (01. januar 2018). Medlemslande i EU. Hentet fra http://www.eu.dk: http://www.eu.dk/da/fakta-om-eu/medlemslande
[33] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 226.
[34] Nielsen, R., & Tvarnø, C. (2014). *Retskilder & Retsteorier.* København: DJØF, s. 227.

Afsnit	Beskrivelse	Teorier og økonomi anvendt
Introduktion	Indledende tydeliggøres værdien af persondata, den historiske kontekst hvorfor problematikken er kommet så vidt, og hvorfor emnet er storpolitisk. Dertil tydeliggøres, hvorfor EU er vigtig overfor behandlingen af persondata, og hvad EU kan gøre for at afhjælpe misbrug af persondata.	- Argumentatorisk økonomi baseret på artikler - Algebra
Økonomisk udgangspunkt	Denne del indeholder en analyse af værdien af data, og hvad der mikroøkonomisk burde ske ved Forordningens implementering på et givent marked.	- Mikroøkonomi - HHI - Lerner - Elasticiteter - Oligopol - Algebra
Ønskelige effekter ved implementering af Forordningen	I dette afsnit vil de foregående ulemper blive opvejet af økonomiske analyser og empiriske materialer. Her inddrages den reelle værdi af Forordningen	- Argumentatorisk økonomi baseret artikler - Mikroøkonomi - Spilteori - Adfærdsøkonomi - Efficiensteori
DPO'en i økonomisk kontekst	Her inddrages DPO'er og forudsætningerne for, at Forordningen vil fungere efter hensigten. Til dette punkt bliver DPO'ens virke som arbejdstager inddraget, og hvorledes denne rolle er med til at give Forordningen værdi for samfundet.	- Spilteori
Diskussion	På baggrund af ovenstående resultater vil en yderligere dimension blive inddraget: Borgerens reelle ønske om, at alt persondata bliver kørt sammen.	- Argumentatorisk økonomi baseret på artikler - Spilteori
Delkonklusion	Delkonklusion på hele det økonomiske kapitel.	

Ovenstående teorier og metoder er (når muligt) anvendt direkte på specialets fokus.

1.6.2 Metode

Induktiv metode begynder ved en observation og ender i en teori. Deduktiv metode er det modsatte[35], hvor en teori bliver benyttet til at forklare noget om virkeligheden. Igennem specialet vil deduktiv metode primært blive benyttet. Induktiv metode benyttes indimellem ved statistisk kvantitativt materiale, der udleder en teoretisk udtagelse. Den deduktive metode anvendes primært, da økonomisk faglighed og teori bruges for at analysere, hvad der økonomisk er rationalet for EU-borgernes, virksomhederne, myndighederne og EU-Kommissionen handlinger.

[35] Kerkmeester, H. (2000). METHODOLOGY: GENERAL. Erasmus University Rotterdam, s. 391.

Der er benyttet neoinstitutionel økonomi igennem specialet, da denne metode fokuserer på spillerne og markedet, der begge er vigtige for at forstå det økonomiske system.[36] Hertil er statslig indblanding ved monopol og imperfekt information anerkendt i neoklassisk økonomi, og dette gør metoden relevant i nærværende speciale.[37] Teorien er klar over, at regulativ indblanding i markedet koster penge, og derfor skal udgiften for at korrigere markedet vurderes i forhold til de nuværende nytteværdier.[38] Med andre ord er resultatet af analysen af markedet først relevant, hvis der bestemmes en måde at løse eventuelle problemer på effektivt.[39]

1.6.3 Teoretiske forudsætninger

Samfundsøkonomiske og retsøkonomiske analyser stiler alle imod at give præcise og korrekte afspejlinger af virkeligheden for at vise den rigtig adfærd og komme med tilnærmelsesvise præcise konklusioner.[40] Samfundsøkonomiske resultater er dog umulige at gøre fejlfri, da det er en forenklet repræsentation af virkeligheden. Dermed indføres forudsætninger, der reelt er forenklinger, som gør økonomien tilnærmelsesvis rigtigt. Der er uanede variable faktorer, der spiller ind samfundsøkonomisk, og derfor viser specialet, hvad der teoretisk burde ske ved givne handlinger og markedsændringer - ikke hvad der *helt sikkert* vil ske. Da der har været svært at komme med bedre og mere præcise alternativer, er dette, hvordan økonomien er behandlet i specialet.

I det økonomiske kapitel vil ordet *handel* fremgå. Dette er ikke handel i sin sædvanlige betydning, hvor borgeren køber et produkt eller ydelse for penge, eller hvor virksomheden køber penge for en ydelse eller produkt. Handel i dette speciale betyder en elektronisk kontrakt, hvor borgeren køber en digital ydelse med betaling via sin persondata, og modsat hvor en virksomhed køber borgernes data for at give en digital ydelse retur. Når den traditionelle forståelse af ordet benyttes, vil dette fremgå. Derudover er ordet *prisen* lige så ens betegnende med den *data*, som borgerne betaler med.

[36] Kerkmeester, H. (2000). METHODOLOGY: GENERAL. Erasmus University Rotterdam, s. 384.
[37] Epstein, R. A. (2007). The Neoclassical Economics of Consumer Contracts. Minnesota Law Review, s. 804-805.
[38] Epstein, R. A. (2007). The Neoclassical Economics of Consumer Contracts. Minnesota Law Review, s. 806.
[39] Varian, H. R. (2003). Intermediate Microeconomics: A Modern Approach (6. udg.). Norton, W. W. & Company, Inc., s. 675.
[40] Eide, E., & Stavang, E. (2008). Rettsøkonomi (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 88.

1.7 Integreret metode og fremgangsmåde

Law and economics er en disciplin, der er tæt knyttet til neoinstitutionel økonomi.[41] Ronald Coase udtrykker, at økonomien er vigtig, for at man kan forstå og arbejde med juraens retsdogmatiske metode.[42] Derfor arbejder de to fag synergisk sammen ved *de lege ferenda* i kapitel 4.

1.8 Kildekritik

1.8.1 Juridisk

Forordningen og dermed artikel 37 om udpegelse af DPO'er er på nuværende tidspunkt en helt ny retsakt, der først træder i kraft d. 25. maj 2018. Den obligatoriske udpegelse af en DPO hos visse dataansvarlige er dermed et nyt juridisk område, og omfanget af anvendelige retskilder er derfor begrænset. Endvidere skal det bemærkes, at vejledningerne, der er udstedt i forbindelse med Forordningen, kun er vejledninger, og de kan fortolkes forskelligt af den enkelte. De anvendte artikler og bøger, der er blevet brugt til at udarbejde denne opgave, kan lige så være præget af forfatternes personlige fortolkninger og holdninger. Forfatterne til dette speciale har forsøgt at have en kritisk tilgang til de subjektive holdninger, der måtte være i det anvendte materiale, og derigennem udlede objektiv gældende ret.

1.8.2 Økonomisk

Som det er tydeliggjort under afsnittet *Teoretiske forudsætninger* på side 15, er det økonomiske kapitel en økonomisk gengivelse af virkelighedens teori og observationer. Dermed er grafer, matrikser, tabeller og eksempler simplificeret for at tydeliggøre de vigtige aspekter indenfor teorierne. Essensen fra artikler er udtrukket for at undgå, at subjektive holdninger påvirker analysen. Alt dette benyttes for at argumentere bedst muligt for en relevant og objektiv økonomisk konklusion.

[41] Kerkmeester, H. (2000). METHODOLOGY: GENERAL. Erasmus University Rotterdam, s. 382.
[42] Coase, R. (1994). The Firm, the market, and the Law. University of Chicago Press.

Kapitel 2 - juridisk analyse

2.1 Indledning

2.1.1 Behovet for en ny og fælles databeskyttelseslov

Behovet for den nye Forordning skyldes i høj grad den teknologiske udvikling og globaliseringen[43], der begge skaber nye problemstillinger i forbindelse med beskyttelse og behandling af persondata. Direktivet blev skabt i perioden 1990-1995, og dermed er noget så relevant som *internettet* ikke taget i betragtning, da teksten blev udformet. Yderligere er nye databehandlingsmetoder som *Big Data* og *Cloud Computing* kommet til verdenen. Disse er eksempler på databehandlingsmetoder, hvor Direktivets regler ikke er tilstrækkeligt udformet til at skabe regulering, der beskytter data-subjektet ordentligt.[44]

Både offentlige myndigheder og private virksomheder har nu om dage mulighed for at anvende personoplysninger i mere eller mindre omfang. Data-subjekterne har hermed øget mulighed for at få udspredt sin persondata på et globalt plan[45], og derfor har subjekternes tillid til det digitale miljø stor betydning for den fortsatte udvikling af EU's økonomi og innovation.

Hvis data-subjekterne ikke har tillid til det digitale miljø, vil forbrugeren dels afholde sig fra at handle *online*, men data-subjektet vil også afholde sig fra at benytte nye digitale tjenester.[46] Dette vil have en negativ indflydelse på udviklingen af innovative anvendelser af nye teknologier, da der opstår hindringer, som begrænser grænseoverskridende datastrømme.[47]

I den forbindelse opfordrede Det Europæiske Råd Europa-Kommissionen til at evaluere de nuværende databeskyttelsesregler og (såfremt det fandtes nødvendigt) komme med

[43] Se Forordningens præambel, betragtning 7.
[44] Blume, P. (2016). Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680. København: Jurist- og Økonomforbundets Forlag, s. 15.
[45] Forslag til Europa-Parlamentet og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse), (COM/2012/011 final). http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=da, (tilgået 01.02.2018).
[46] Allerede i 2011 udtrykte EU bekymring over EU-borgeres "*lack of trust in online business*". Kilde: European Commission Staff Working Document, Bringing e-commerce benefits to consumers, SEC(2011) 1640 final, 11 January, 2012; accompanying Commission Communication, COM(2011) 942 final, 2012, s. 30.
[47] Europa-Kommissionen. (2015). Europa-Kommissionen - Pressemeddelelse. Hentet fra Aftale om Kommissionens EU-databeskyttelsesreform vil styrke det digitale indre marked: http://europa.eu/rapid/press-release_IP-15-6321_da.htm, (tilgået 14/02/2018).

initiativer til nye regler.[48] Dette var startskuddet, der førte til den nu vedtagede persondataforordning.

Beskyttelse af personoplysninger er højt prioriteret inden for Den Europæiske Union (EU), og behandlingen af oplysningerne er ligeledes karakteriseret som *grundlæggende rettigheder* i Den Europæiske Unions charter om grundlæggende rettigheder[49] artikel 8. Charteret og de indeholdende rettigheder blev efter Lissabontraktatens[50] ikrafttræden d. 1. december 2009 opløftet til traktatniveau. Charterets rettigheder skal derfor ses som primærret på samme niveau som TEUF-artiklerne.[51] Det faktum, at beskyttelsen af personoplysninger er karakteriseret som en grundlæggende rettighed, understreger, hvor højt denne beskyttelse er prioriteret inden for EU. Ligeledes understregede kommissionsformand Jean-Claude Juncker i sin tale om Unionens tilstand den 14. september 2016:

> "*At være europæer betyder, at du har ret til at få dine personoplysninger beskyttet af stærk europæisk lovgivning. (...) For privatlivets fred betyder noget i Europa. Det er et spørgsmål om menneskelig værdighed.*"[52]

Ved at der nu er tale om en forordning og ikke et direktiv, sikres der som udgangspunkt en identisk lovgivning og dermed identisk sikkerhedsniveau på tværs af medlemsstaternes grænser. Forordningen er dog ikke et udtryk for totalharmonisering af retsområdet *persondatabehandling*. Forordningen giver på flere områder medlemsstaterne mulighed for at indføre nationale love, hvorved en identisk lovgivning ikke sikres - mere om dette i afsnittet om Forordningens gennemførsel i dansk ret på side 22.

Et af Forordningens formål er bl.a. at styrke data-subjektets retssikkerhed både nationalt og på tværs af landegrænser over for institutioner, der behandler persondata. Retssikkerheden sikres bl.a. via de rettigheder, som data-subjekterne gives i kraft af Forordningen. Som

[48] Forslag til Europa-Parlamentet og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) - Bruxelles 25.01.2012, Com(2012) 11 final
[49] DEN EUROPÆISKE UNIONS CHARTER OM GRUNDLÆGGENDE RETTIGHEDER (2012/C 326/02)
[50] LISSABONTRAKTATEN OM ÆNDRING AF TRAKTATEN OM DEN EUROPÆISKE UNION OG TRAKTATEN OM OPRETTELSE AF DET EUROPÆISKE FÆLLESSKAB (2007/C 306/01).
[51] Traktaten om Den Europæiske Union (TEU) artikel 6. stk. 1.
[52] Citat: MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET om udveksling og beskyttelse af personoplysninger i en globaliseret verden, https://ec.europa.eu/transparency/regdoc/rep/1/2017/DA/COM-2017-7-F1-DA-MAIN-PART-1.PDF, (tilgået 14/02/2018).

eksempler har data-subjektet bl.a. ret til indsigt i behandlingen af dennes persondata og at gøre indsigelse mod behandlingen af dennes persondata.[53]

Forordningen har dog ikke kun til formål at sikre data-subjekternes retssikkerhed. Forordningen er ligeså en del af EU-Kommissionens strategi om det digitale indre marked. Dermed skal den bidrage til at skabe en ramme for en ordentlig udnyttelse af moderne digital økonomi. Forordningens bidrag til denne strategi er at skabe en balance, hvor udvekslingen af personoplysninger kan ske på en ordentlig måde og være med til at udvikle økonomien i EU, hvor data-subjektet fortsat har mulighed for at kontrollere sin egen persondata.[54]

Det er med den ovenstående indledning tydeliggjort, at der er et stort behov for en opdatering af Direktivets regler om databeskyttelsesret - set både fra data-subjekternes side men lige så fra et økonomisk og innovationsmæssigt synspunkt. I nedenstående afsnit vil det blive undersøgt, hvilken rolle en DPO spiller i forbindelse med opfyldelsen af de ovennævnte behov.

2.2 Databeskyttelsesrådgiveren og dennes rolle

2.2.1 Forordningens art. 24 & 37-39

Med Forordningens ikrafttræden bliver den dataansvarlige pålagt at efterleve Forordningens art. 24, der fastlægger den dataansvarlige forpligtelser i forbindelse med persondatabehandling. Den dataansvarlige skal hermed sikre sig, at alt persondatabehandling foregår i *compliance* med Forordningen. Dette kan blive en stor mundfuld alt afhængig af størrelsen på den dataansvarliges organisation og kompleksiteten af databehandlingen. En dataansvarlig kan derfor i princippet handle i strid med Forordningen uden at være klar over, at dette sker.[55]

Det er her, at DPO'en er relevant og kommer til at spille en rolle. DPO'en bliver flere gange nævnt i betragtningerne i Forordningens præambel, og rollen indgår også i Forordningens artikler. Der er dog ingen af disse, der definerer, hvad en DPO reelt er, men rollen bliver derimod beskrevet i både Artikel 29-gruppens (herefter kaldet *Gruppen*)[56] og den danske tilsynsmyndigheds (Datatilsynet) vejledninger vedrørende udpegelsen af DPO'er. Gruppens

[53] Høilund, D. (2017). Persondataret (1. ed.). Hans og Reitzels Forlag, s. 12.
[54] Høilund, D. (2017). Persondataret (1. ed.). Hans og Reitzels Forlag, s. 13.
og Europakommissionen. (u.d.). Europa-Kommissionen - Pressemeddelelse. Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_IP-15-4919_da.htm, (tilgået 03/05/2018).
[55] Blume, P. (2016). Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680. København: Jurist- og Økonomforbundets Forlag, s. 128.
[56] Se mere om Artikel 29-gruppen og Datatilsynet fra side 34.

vejledning er baseret på deres fortolkning af Forordningens præambel, betragtninger og artikler, der enten nævner eller beskriver DPO'en, og hvilken rolle denne skal spille under Forordningen.

En DPO skal efter vejledningerne forstås som en rådgiver i persondataretlige problemstillinger for den organisation, denne er tilknyttet.[57] DPO'ens overordnede opgave er at være med til at sikre, at Forordningen bliver overholdt, når organisationer behandler persondata.

Dermed er rollen som DPO en ekstra støttefunktion, der skal bidrage til ansvarligheden (*accountability*), som er et gennemløbende emne i Forordningen.[58] Dette ses i art. 24, stk. 1, der vedrører den dataansvarliges ansvar.

DPO'en anerkendes i Forordningen, som en hjørnesten i det fornyede fokus om ansvarlighed, og rollen ses som en vigtig aktør i den nye ordning, der kommer med Forordningen.[59] Det er derfor også den dataansvarliges opgave at inddrage DPO'en i alle spørgsmål vedrørende beskyttelsen af persondata jf. Forordningens art. 38, stk. 1. Den dataansvarlige skal derfor sørge for, at DPO'en bliver inddraget ved bl.a. vurderingen af om de behandlingsaktiviteter, der foretages i organisationen, er i overensstemmelse med Forordningens kapitel II om de grundlæggende behandlingsprincipper og behandlingsbetingelserne.

DPO'en har derudover yderligere opgaver. Efter Forordningens art. 39 er DPO'ens opgaver bl.a. at rådgive den dataansvarlige, databehandleren og de ansatte i organisationen, der behandler persondata, om deres ansvar og forpligtelser i forhold til overholdelse af Forordningen. Yderligere skal DPO'en overvåge overholdelsen af Forordningen og yde rådgivning, når der anmodes om denne i forbindelse med databeskyttelse og samarbejde, samt DPO'en skal fungere som kontaktperson for Datatilsynet.

Der stilles ikke nogle formelle uddannelses- eller certificeringskrav til DPO-rollen. Dog skal DPO'en efter Forordningens art. 37, stk. 5 udpeges efter sine faglige kvalifikationer - særligt dennes ekspertise og forståelse inden for både national og international databeskyttelsesret. Personens evne til at løfte DPO'ens opgaver skal ligeledes inddrages, når de faglige kvalifikationer vurderes.[60] DPO'ens opgaver er oplistet i Forordningens artikel 39. Hvorvidt

[57] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 5.
[58] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 5.
[59] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 5.
WP betyder *Working Papers,* som er, hvad Gruppens vejledninger kaldes.
[60] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 12.

en person har den nødvendige ekspertise til at agere DPO i en organisation kan variere, og vurderingen af om dette er tilfældet bør afhænge af de databehandlingsaktiviteter, der udføres i den pågældende organisation, samt det beskyttelsesniveau den behandlede persondata kræver.[61]

Der stilles ligeledes ingen krav om hvorvidt, DPO'en skal være en intern medarbejder eller en udefrakommende ekstern rådgiver jf. Forordningens art. 37, stk. 6. DPO'en kan derfor være en i forvejen eksisterende medarbejder i organisationen, såfremt denne opfylder betingelserne til at indtræde i rollen.

Efter Forordningens artikel 38, stk. 3, 1. pkt. må DPO'en ikke være underlagt instruktionsbeføjelser fra hverken den dataansvarlige eller databehandleren i organisationen, som denne er ansat i. DPO'en er som udgangspunkt kun underlagt Forordningens anvisninger, og personen skal derfor fungere som en uafhængig enhed i organisationen, når denne udfører de forpligtende opgaver efter art. 39. Dette fremgår ligeså af betragtning 97 i Forordningens præambel, og dette gælder, uanset om DPO'en er intern eller ekstern. DPO'en kan derfor hverken blive pålagt at komme frem til et bestemt resultat, der er ønsket af den dataansvarlige, eller skulle finde på en løsning, således at den dataansvarliges foretrukne databehandlingsmetode fungerer.[62] I direkte forbindelse hermed (og for at sikre DPO'ens uafhængighed) kan DPO'en ikke blive straffet eller afskediget fra sin arbejdsplads ved udførelsen af de oplistede opgaver i art. 39.

DPO'en står dog til ansvar overfor organisations øverste ledelse.[63] Artiklen om at DPO'en rent faktisk står til ansvar over for nogen i organisationen gør, at rollen ikke er *fuldt* uafhængig. Artiklen er ikke indsat i Forordningen for at give den øverste ledelse mulighed for at påvirke DPO'en i dennes arbejde, men det er gjort for at sikre, at DPO'en rent faktisk bistår ledelsen med overholdelsen af Forordningen.[64] Det skal dog bemærkes, at DPO'en kun nyder denne særlige beskyttelse, når denne udfører de i art. 39 fremsatte opgaver. En DPO kan således godt være forpligtet til at udføre andre opgaver, hvis denne fx blot er ansat som DPO på deltid, og personen derfor i den forbindelse er underlagt instruktionsbeføjelser fra sin overordnede. Det er dog den dataansvarliges opgave at sørge for, at der ikke er

[61] Jf. Forordningens præambel betragtning 97, 2. sidste punktum.
[62] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 16.
[63] Jf. Forordningens art. 38, stk. 3, 3. pkt.
[64] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 581

nogen interessekonflikt mellem de andre opgaver, og det arbejde den ansatte varetager i sin rolle som DPO.[65]

Det er bemærkelsesværdigt, at man i udarbejdelsen af Forordningen har gjort sig store anstrengelser for at sikre DPO'ens uafhængighed, når denne udfører sit arbejde, men samtidigt gør Forordningen det muligt at have en intern medarbejder ansat som DPO.

Det er med ovenstående redegjort for, hvad en DPO er, samt hvad denne kommer til at bidrage med under Forordningen. I de kommende afsnit vil der blive set på, hvordan gennemførelsen af Forordningen kommer til at påvirke dansk ret. Fokus vil særligt være på påvirkningen af den nuværende persondataret og de suppleringslove, der gennemføres i Danmark grundet Forordningens åbne artikler.

2.3 Gennemførelsen af Forordningen i dansk ret

2.3.1 En forordning i stedet for et direktiv

I modsætning til Direktivet, der blev implementeret i national lov for at finde anvendelse, kommer Forordningen til at fungere som en deciderede lov i Danmark. Dets regler skaber dermed rettigheder til data-subjekterne og forpligtelser til dataansvarlige og databehandlere, uden at den bliver inkorporeret direkte i danske lovtekster.[66]

Forordningen kommer til at være en del af dansk ret på samme måde som enhver anden dansk lov. I kraft af EU-rettens forrang vil en anden dansk lov, der enten strider imod Forordningen eller regulerer på et område, der falder ind under Forordningens anvendelsesområde, blive ugyldiggjort. Dette gøres for at minimere usikkerheden på retsområdet og sikre EU-rettens gennemslagskraft.[67] Dermed har Danmark pligt til at indrette dansk lovgivning efter Forordningens regler, således at denne bliver overholdt. Gennemførslen af Forordningen i dansk ret betyder derfor, at reglerne der finder anvendelse efter den nuværende persondatalov § 1, stk. 1[68], og som regulerer det samme som Forordningen, vil blive erstattet af Forordningens regler. Sagt på en anden måde vil størstedelen af den nuværende persondatalov ikke være gældende efter d. 25. maj 2018, hvor Forordningen erstatter Direktivet. Det vil dog være muligt, såfremt det er ønsket, at

[65] Jf. Forordningens art. 38, stk. 6.
[66] Olsen, B. E., & Sørensen, K. E. (2008). *Europæiseringen af Dansk ret* (1. udg.). Jurist- og Økonomiforbundets forlag, s. 221.
[67] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 20.
[68] Lov om behandling af personoplysninger LOV nr. 429 af 31/05/2000.

videreføre visse regler af den nuværende persondatalov, hvis bestemmelser i medfør af lovens § 1 regulerer områder, der falder uden for Forordningens anvendelsesområde.[69]

2.3.2 Åbne artikler i Forordningen med fokus på DPO'er

På trods af at Forordningen har til hensigt at sikre ens lovgivning og sikkerhed, har medlemsstaterne hjemmel i flere af Forordningens artikler til at *erstatte, komplementere* eller *præcisere* Forordningens artikler med egne nationale love. Årsagen til disse "åbne" artikler skyldes det høje ambitionsniveau, der har været fra EU-institutionernes side for at få udarbejdet og gennemført Forordningen hurtigst muligt.[70]

I Danmark vil der således være mulighed for at:

- fastsætte yderligere regler for, hvornår udpegelsen af en DPO er obligatorisk[71] og
- specificere DPO'ens minimumsopgaver.[72]

Der er dog ikke en lignende regel i de åbne artikler, som giver en medlemsstat hjemmel til at undtage en dataansvarlig for forpligtelsen til at udpege en DPO.[73]

Der vil grundet de åbne artikler ikke være en identisk databeskyttelse i de forskellige medlemslande. Foreninger, virksomheder o.l. må derfor være opmærksomme på national lovgivning, når de etablerer sig i en medlemsstat, og når de begynder at implementere deres databehandlingsprocedurer. Da hver medlemsstat kan fastsætte yderligere krav til udpegelsen af DPO'er, har denne artikel størst praktisk betydning af alle de åbne artikler i forhold til specialet.

2.3.3 Nationale suppleringslove som følge af Forordningen

For at opfylde en forordning fuldt ud er det ikke unormalt, at der er behov for at udstede supplerende lovgivning fra en medlemsstats side. Når det er nødvendigt at lave supplerende lovgivning, er medlemsstaten underlagt de samme krav til udformningen af denne, som de

[69] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565 s. 20.
[70] Se forordningens præambel, 10 betragtning samt Voigt, P., & Bussche, A. V. (2017). *The EU General Data Protection Regulation (GDPR) - A Practical Guide.* Springer International Publishing A*., s. 219*.
[71] Jf. Forordningens art. 37, stk. 4.
[72] Jf. Forordningens art. 39, stk. 1, litra a-b).
[73] For en fuld oversigt over de åbne artikler se: Voigt, P., & Bussche, A. V. (2017). *The EU General Data Protection Regulation (GDPR) - A Practical Guide.* Springer International Publishing AG*, s. 220-222.*

er ved implementeringen af direktiver.[74] Den supplerende lov skal altså dels være præcis og entydigt formuleret, og den skal derudover være egnet til at opfylde forordningen og dennes målsætning.[75] På baggrund af artiklerne, der giver medlemsstaterne mulighed (og i nogle tilfælde *pligt*) til at fastsætte særlige nationale regler, har det danske justitsministerium vurderet, at det er nødvendigt, at der laves en suppleringslov herom ved navn *lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven*).[76] Der blev derfor fremsat et lovforslag d. 25. oktober 2017, hvis formål består i at supplere Forordningen med danske nationale regler, hvor der gives råderum til dette. Såfremt der bliver udstedt nationale love for, hvornår en DPO skal udpeges, vil disse fremgå af denne lov. Dette er dog kun hvis loven går igennem 2. og 3. behandling i Folketinget.[77] Se fra side 56 for vurdering af om dette er tilfældet.

I kombination med lovforslaget om den nye databeskyttelseslov er endnu et lovforslag blevet fremsat, og den blev navngivet *Lov om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love*.[78] Behovet for et endnu et lovforslag skyldes, at adskillige danske love henviser til den udgående persondatalov. Yderligere er der andre love, der regulerer behandling af persondata, som efter Forordningens ikrafttræden vil blive underkendt. Formålet med dette ekstra lovforslag er at foretage en konsekvensændring af de berørte regler, således at de er tilpasset Forordningen og den nye databeskyttelseslov.[79] Denne

[74] Olsen, B. E., & Sørensen, K. E. (2008). *Europæiseringen af Dansk ret* (1. udg.). Jurist- og Økonomiforbundets forlag, s. 222.
[75] Sag C-119/92: Sagens parter var hhv. Kommissionen for De Europæiske Fællesskaber mod den Italienske Republik. Kommissionen gør i sagen gældende, at Italien har lavet traktatbrud ved deres gennemførelsesforanstaltninger af en forordning. Forordningen vedrører betingelserne for, hvornår en person må lave toldangivelser. De italienske myndigheder havde på baggrund af forordningen udstedt en national lov der, grundet lovens formulering, skabte en usikkerhed der forhindrede anvendelsen af den relevante forordning. Kommissionen fik i sagen medhold.
[76] Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) - 2017/1 LSF 68.
[77] På datoen for aflevering af specialet var denne suppleringslov nået til 1. behandling. Kilde: Poulsen, S. P. (2017-2018). *Folketingets hjemmeside*. Hentet fra http://www.ft.dk: http://www.ft.dk/samling/20171/lovforslag/L68/tidsplan.htm (tilgået 14/05/2018).
[78] Lov om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love - 2017/1 LSF 69.
[79] *Justitsministeriets hjemmeside*. (27. Oktober 2017). Hentet fra www.justitsministeriet.dk: http://www.justitsministeriet.dk/nyt-og-presse/nyhedsbrev/2017/nyhedsbrev-af-27-oktober-2017 (tilgået 15/02/2018).

suppleringslov forventes ligeledes først at komme i 2. og 3. behandling hhv. 15. og 17. maj 2018.[80]

2.3.4 Videreførelse af retstilstanden

På trods af det store administrative arbejde, der ligger i gennemførelsen af (og ved den generelle forberedelse til) Forordningens ikrafttræden, har Forordningen gennemgående samme opbygning som Direktivet og persondataloven.[81] Store dele af Forordningen ændres der ligeledes ikke på, og den viderefører derfor retstilstanden, som den er i dag. Dette gælder derudover også for relevant praksis fra EU-domstolen. Ligeså er de relevante begreber som *definitioner*, *anvendelsesområder* og *procedurerne for persondatabehandlingen* meget lig med den nuværende retstilstand.[82] Institutionerne, der i forvejen følger den nuværende persondatalov, er derfor allerede et godt stykke af vejen mod efterlevelse af reglerne efter Forordningen.[83]

Det er med ovenstående vist, at dansk ret skal indrettes, så denne passer til Forordningen. Den danske persondatalov, der før regulerede persondatabehandlingen i Danmark, og hvor DPO-ordningen ikke er nævnt, erstattes derfor af Forordningen og de nationale supplerende regler. I de følgende afsnit vil der derfor blive set på Forordningens anvendelsesområde. Dette gøres for at fastslå, at spejderforeningerne er underlagt Forordningen, og at de dermed potentielt skal udpege en DPO. Modsat, hvis spejderforeningerne ikke var underlagt Forordningen, vil den juridiske analyse være overstået herefter.

2.4 Forordningens anvendelsesområde

2.4.1 Forordnings territoriale anvendelsesområde (art. 3, stk. 1)

Ifølge Forordningens art. 3, stk. 1 finder Forordningen anvendelse på "*(...) behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej*".

For at forstå Forordningens territoriale område vil følgende begreber blive vurderet:

[80] Poulsen, S. P. (2017-2018). *Folketingets hjemmeside*. Hentet fra http://www.ft.dk: http://www.ft.dk/samling/20171/lovforslag/L69/tidsplan.htm (tilgået 14/05/2018).
[81] Høilund, D. (2017). Persondataret (1. ed.). Hans og Reitzels Forlag, s. 12.
[82] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 15.
[83] *justitsministeriets hjemmeside*. (24. maj 2017). Hentet fra http://justitsministeriet.dk: http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2017/nye-regler-styrker-beskyttelsen-af-persondata-i-europa (tilgået 15/02/218).

1) den dataansvarlige
2) databehandleren
3) etableringsbegrebet

Den ***dataansvarlige*** er efter Forordningens forstand den fysiske eller juridiske person eller ethvert andet organ, der har dispositionsretten over den relevante persondata. Det er ligeledes denne, der afgør, hvordan persondata indsamles, og hvordan denne skal behandles, jf. Forordningens artikel 4, stk. 1, nr. 7. Den dataansvarlige har altså ansvaret for behandlingen af dataen overfor data-subjektet. Den dataansvarlige kan (som tidligere nævnt) være ethvert organ, der har dispositionsretten over den relevante persondata, og dermed kan det også være spejderforeningerne. Da det er spejderforeningerne, der indhenter medlemmernes data, er disse at betragte som de dataansvarlige efter Forordningen.

Den dataansvarlige kan hyre ekstern hjælp, der skal assistere med databehandlingen. Det er i disse situationer, at ***databehandleren*** bliver relevant. En databehandler skal efter Forordningen forstås som en fysisk eller juridisk person, der behandler persondata på vegne af den dataansvarlige jf. Forordningens artikel 4, stk. 1, nr. 8. Dette kan være lønbureauer og leverandører af IT-systemer, hvor der behandles persondata m.fl.

I forhold til ***etableringsbegrebet*** jf. Forordningen må det antages, at dette svarer til det allerede anvendte begreb efter det udgående Direktiv. Relevant retspraksis fra Direktivet må derfor kunne anvendes til at fastsætte bredden af begrebet. Efter Direktivet skal etableringsbegrebet forstås meget bredt, og den omfatter enhver aktivitet, der bliver udført fra en permanent selskabsretlig struktur - selv hvis denne er minimal.[84] Hvorledes denne struktur er udformet, er uden betydning for Forordningens anvendelsesområdet, og dermed er alle strukturelle former underlagt Forordningen, hvad end der er tale om filialer, foreninger, moder- eller datterselskaber o.l.[85]

I sag C-230/14 ved EU-domstolen var blot tilstedeværelsen af en salgsrepræsentant i medlemsstaten Ungarn, der udførte behandling af persondata på vegne af et slovensk selskab, således tilstrækkelig til, at det slovenske selskab blev anset som værende etableret i Ungarn. Ungarns databeskyttelseslov fandt derfor anvendelse.

[84] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 35.
[85] Jf. Forordningens præambel betragtning 22.

Det er med ovenstående gennemgang klargjort, at spejderforeningerne falder ind under Forordningens territoriale anvendelsesområde, da de bliver kategoriserede som dataansvarlige, når de indsamler og behandler data om deres medlemmer. I det kommende afsnit vil der blive set på, om spejderforeningerne ligeså er underlagt Forordningens materielle anvendelsesområde.

2.4.2 Forordningens materielle anvendelsesområde (art. 2, stk. 1)

Ifølge Forordningens art. 2, stk. 1 finder Forordningen anvendelse på;

> "*(...) behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling, og på anden ikke- automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.*".

Forordningens art. 2, stk. 1 svarer stort set ordret til Direktivets artikel 3, stk. 1, hvori der står, at Direktivet finder anvendelse på;

> "*(...) behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.*".

Den største forskel er anvendelsen af ordet "*edb*", som er nævnt i Direktivet (se understregede i citatet fra Direktivet). Dette svarer til Forordningens formulering "*automatisk databehandling*"[86], og derfor er ordlyden af Forordningens materielle anvendelsesområde ens med Direktivets.

For at kunne klarlægge omfanget af Forordnings materielle anvendelsesområde, er det nødvendigt at redegøre for begreberne i art. 2, stk. 1. De relevante begreber er:

1) personoplysninger
2) behandlingsbegrebet
3) register

Forordningens definitioner på begreberne findes i Forordningens art. 4:

Det fremgår af art. 4, stk. 1, nr. 1, at der ved ***personoplysninger*** skal forstås "*(...) enhver form for information om en identificeret eller identificerbar fysisk person (...)*". Forordningens definition er yderst bred, så den inkluderer alt fra navn, adresse og fødselsdagsdato til økonomisk, kulturel eller social identitet m.m. Listen af information, der skal forstås som

[86] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, betænkning nr. 1565, s. 31.

personoplysninger efter art. 4, stk. 1, nr. 1, er ikke udtømmende, og den må benyttes som et redskab, der skal hjælpe databehandlere og dataansvarlige med at forstå, hvornår et stykke data er kategoriseret som persondata i Forordningens forstand.[87]

Behandlingsbegrebet er defineret i Forordningens art. 4, stk. 1, nr. 2. Her fremgår det, at behandling er "*(...) enhver aktivitet eller række af aktiviteter - med eller uden brug af automatisk behandling - som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering (...)*". Ligesom det var tilfældet med oplistningen af personoplysningerne i Forordningens art. 4, stk. 1, nr. 1, er oplistningen over behandlingsbegrebet heller ikke udtømmende eksempler på, hvornår et foretagende kategoriseres som "behandling" i Forordningens forstand. Kort sagt er nærmest alle aktiviteter, som personoplysninger gøres til genstand for, behandling i Forordningens forstand. Elektronisk og manuelt behandlingen skal vurderes ens, og derfor fritages manuel behandling ikke fra Forordningen.[88]

Endelig er begrebet ***register*** defineret i Forordningens art. 4, stk. 1, nr. 6. Et register er her defineret som "*(...) enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier, hvad enten denne samling er placeret centralt eller decentralt eller er fordelt på funktionsbestemt eller geografisk område".*

Som nævnt i indledningen til dette kapitel har den digitale udvikling bevirket, at både private virksomheder og offentlige institutioner kan benytte sig af data-subjekternes persondata på flere og flere måder. Subjekternes persondata er anvendelig, når den behandles på en sådan måde, at dataen er let at søge i. Hermed er der øget sandsynlighed for, at dataen bliver benyttet på en ikke-hensigtsmæssig måde til skade for data-subjektet. Dette er netop tilfældet, hvis dataen ligger digitalt eller i et fysisk register. Det er i sådanne tilfælde, at subjekternes beskyttelsesbehov aktualiseres, og derfor er Forordningens anvendelsesområde afgrænset til situationer, hvor persondatabehandlingen enten sker digitalt eller manuelt - og i et register.[89]

Ud fra ovenstående er det tydeliggjort, at Forordningens materielle anvendelsesområde er yderst bredt, og at Forordningen som udgangspunkt er gældende for alle, der behandler

[87] At listen ikke er udtømmende, kan bl.a. udledes af, at listen indledes med "*f.eks.*". Dette indikerer, at mere/anden data end de listede eksempler kan defineres som persondata.
[88] *Manuel behandling* skal dog foretages i et register for at være gældende.
[89] Blume, P. (2016). *Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680.* København: Jurist- og Økonomforbundets Forlag, s. 49.

persondata, hvad enten det er offentlige myndigheder, private virksomheder, internationale organisationer, diverse foreninger eller tilsvarende organisationer.

2.4.2.1 Undtagelse fra Forordningen anvendelsesområde (art. 2, stk. 2)

Forordningens art. 2, stk. 2 indeholder fire undtagelser til, hvornår behandlingen af persondata ikke falder ind under Forordningens anvendelsesområde. Disse undtagelser analyseres for at undersøge, om spejderforeningerne falder ind under én af disse kategorier. Hvis dette er tilfældet, vil spejderforeningerne helt være undtaget for Forordningen og ligeså pligten til at udpege en DPO.

2.4.2.1.1 Udøvelse af aktiviteter der falder udenfor EU-retten (art. 2, stk. 2, litra a) og b))

Det er ikke overraskende, at Forordningen ikke finder anvendelse på områder, der falder udenfor EU-retten, da forordninger er et reguleringsværktøj indenfor EU. EU kan kun regulere områder, hvor denne er blevet tildelt kompetence fra medlemsstaterne.[90] Denne undtagelse er relevant at analysere, da artiklen ikke specificerer hvilke aktiviteter, der falder uden for EU-retten. Spørgsmålet er derfor, hvornår en aktivitet, der vedrører persondatabehandling, falder uden for Forordningens anvendelsesområde.

Betragtning nr. 16 i Forordningens præambel tydeliggør, at Forordningen bl.a. ikke finder anvendelse på persondatabehandling, der vedrører *medlemsstaternes sikkerhed*. Med dette forstås, at Forordningen ikke finder anvendelse på medlemsstaternes efterretningstjenester - i Danmark særligt Politiets og Forsvarets efterretningstjenester.[91] Undtagelsen er dog ikke begrænset til blot disse efterretningstjenester.

Dermed er persondatabehandling, der foretages af enhver offentlig myndighed (såfremt behandlingen foretages udelukkende for at beskytte statens sikkerhed), undtaget for Forordningen.[92] Det skal i forbindelse med dette fremhæves, at Forordningen heller ikke finder anvendelse, når medlemsstaterne foretager persondatabehandling *inden for rammerne* af TEU kapitel 2, der omhandler den fælles udenrigs- og sikkerhedspolitik.[93]

[90] TEU art. 5, stk. 2.
[91] Politiets og Forsvarets efterretningstjenester kaldes henholdsvis PET og FE. Deres opgaver kan findes på: *Politiets efterretningstjenestes hjemmeside*. (u.d.). Hentet fra https://www.pet.dk/. og *Forsvarets efterretningstjenestes hjemmeside*. (u.d.). Hentet fra https://fe-ddis.dk: *https://fe-ddis.dk/Pages/default.aspx* (tilgået d. 12/05/2018).
[92] Blume, P. (2016). *Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680.* København: Jurist- og Økonomforbundets Forlag, s. 50.
[93] Blume, P. (2016). *Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680.* København: Jurist- og Økonomforbundets Forlag, s. 51.

Specialets fokuserer på spejderforeningernes persondatabehandlingsaktiviteter. Med udgangspunkt i den juridiske analyse må det konkluderes, at disse ikke er undtaget efter reglen om medlemsstaternes sikkerhed, da persondatabehandlingen, der sker i spejderforeningerne, ikke sker for at beskytte staten.

2.4.2.1.2 Personlige eller familiemæssige aktiviteter foretaget af en fysisk person (art. 2, stk. 2, litra c))

Forordningen finder ikke anvendelse på persondatabehandling, der foretages af en fysisk person, når behandlingen er en personlig eller familiemæssig aktivitet. I Forordningens præambel betragtning 18 uddybes, at der med *personlige* og *private aktiviteter* skal forstås aktiviteter, der ikke er forbundet med erhvervsmæssige eller kommercielle aktiviteter. At denne undtagelse kun gælder for fysiske personer, må antages at være fordi, det er uproportionalt at forlange, at en fysisk persons private oversigt over fx sine venner og families fødselsdage er underlagt Forordningen.

Spejderforeningerne er ikke at betragte som fysiske personer, men skal derimod betragtes som selvstændige juridiske enheder. Denne undtagelse finder derfor ikke anvendelse for spejderforeningerne.

2.4.2.1.3 Behandling foretaget af kompetente myndigheder i forbindelse med retsforfølgning m.m. (art. 2, stk. 2, litra d))

Denne undtagelse finder anvendelse, når de relevante myndigheder foretager persondatabehandling i forbindelse med bl.a. forebyggelsen af strafbare handlinger.[94] Årsagen til denne undtagelse er, at persondatabehandling inden for strafferettens områder er reguleret af en anden EU-retsakt - direktiv 2016/680. Dermed finder Forordningen ikke anvendelse i disse persondatabehandlingssituationer.[95]

Dette punkt er heller ikke en anvendelig undtagelse for spejderforeningerne. Sådanne spejderforeninger er af naturlige grunde ikke at betragte som myndigheder, der behandler persondata i forbindelse med at forebygge og retsforfølge strafbare handlinger.

Det er ud fra ovenstående analyse af Forordningens territoriale og materielle anvendelsesområde tydeliggjort, at spejderforeningerne ikke er undtaget fra Forordningens

[94] Jf. Forordningens præambel betragtning 19.
[95] EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA.

anvendelsesområder, men at de derimod er underlagt begge områder. Derfor skal kravet om udpegelse af DPO'er stadig undersøges.

I de næste afsnit er fokus, hvilke fortolkningsbidrag der findes til Forordningens art. 37 om udpegelse af DPO'er. Der vil blive set på DPO-rollens udvikling inden for EU, hvor denne er startet, til hvor den er nu som en del af Forordningen. Yderligere vil der blive set på, om der er relevant retspraksis, der kan videreføres fra Direktivet, persondataloven og eventuelle andre retskilder.

2.5 Fortolkningsbidrag til Forordningens art. 37 vedr. DPO'er

2.5.1 DPO-rollen før Direktivets ikrafttræden (Den Tyske Model)

DPO'en blev introduceret i EU ved Direktivet, men allerede før Direktivets tilblivelse havde rollen eksisteret i Tyskland i flere år. Rollen som DPO blev indført i Tyskland efter den tyske databeskyttelseslov af 1977 - på tysk navngivet *Bundesdatenschutzgesetz*.[96] Før Direktivets ikrafttræden i Tyskland var det således obligatorisk for den dataansvarlige at udpege en DPO, såfremt denne havde ni eller flere ansatte, der behandlede persondata.[97] Idéen var dengang at lave en effektiv selvmonitorering af virksomhedens egen overholdelse af landets persondatalov. Ved en sådan indførelse håbede staten at reducere de bureaukratiske vanskeligheder, der opstod ved indblanding af de relevante myndigheder. Lovgiver mente, at DPO'en ville mindske myndighedernes behov for at kontrollere virksomhedernes overholdelse af loven, samtidigt med at loven fortsat ville blive overholdt.[98]

Idéen om selvmonitorering har altså været kendt i Tyskland i mange år. Det var også de tyske EU-repræsentanter, der i Bruxelles i 1994 var med til at overbevise EU-Kommissionen om at give medlemsstaterne mulighed for at implementere den tyske DPO-model i de respektive medlemsstater.[99] EU-Kommissionen var allerede ved Direktivets

[96] Bundesdatenschutzgesetz - BDSG) of 27th of January, 1977, [*Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act -BDSG)*] kapitel 3, sektion 5, art. 1 for offentlige myndigheder og kapitel 3, sektion 38, art. 1. for private enheder. *German Law Archive*. (17. August 2017). Hentet fra https://germanlawarchive.iuscomp.org: https://germanlawarchive.iuscomp.org/?p=712 (tilgået d. 18/03/2018).

[97] *DLA Piper - Data Protection Laws Of The World*. (26. Januar 2017). Hentet fra www.dlapiperdataprotection.com: https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=DE (tilgået d. 04/04/2018).

[98] Klug, C. (2010). *The German Association for Data Protection and Data Security (GDD) .* Hentet fra https://www.gdd.de: https://www.gdd.de/international/english/DPO_Report_by_Christoph_Klug.pdf s. 2.

[99] Klug, C. (2010). *The German Association for Data Protection and Data Security (GDD) .* Hentet fra https://www.gdd.de: https://www.gdd.de/international/english/DPO_Report_by_Christoph_Klug.pdf, s. 2.

implementeringsfase positivt stemt overfor DPO'er. Kommissionen udtrykte i første statusrapport vedrørende implementeringen sin beklagelse over, at så få medlemsstater havde valgt at implementere muligheden for en DPO hidtil.[100]

Anskaffelsen af en DPO blev derudover en konkurrencefordel i Tyskland, da rollen som DPO blev et tegn på kvalitet. Med dette menes en konkurrencemæssig fordel, der viser, at virksomheden tager borgernes persondata alvorligt, og at der er en uafhængig specialist ansat, som sikrer og optimerer virksomhedens procedurer overfor lovgivningen.[101]

2.5.2 Udpegelse af DPO'er under Direktivet

2.5.2.1 Direktivets art. 18

Der er frem til 25. maj 2018 (hvor Direktivet erstattes) ikke en forpligtigelse for hverken offentlige myndigheder, private virksomheder eller foreninger til at udpege en DPO. Direktivets art. 18, stk. 2, 2. pind gav dog i implementeringsfasen af Direktivet alle medlemsstaterne mulighed for at indføre DPO-rollen, såfremt medlemsstaten ønskede dette.

Art. 18 i Direktivet vedrører anmeldelsespligten til den relevante tilsynsmyndighed. Efter artiklen skulle den registeransvarlige[102], inden denne indførte en elektronisk databehandlingsproces, anmelde dette samt anmelde behandlingsprocessen til Datatilsynet.[103] Artiklen åbner samtidigt op for muligheden for en forenklet (eller sågar en hel fritagelse for) anmeldelsespligt ved udpegelse af en person med ansvar for persondatabeskyttelsen, jf. ordlyden i hhv. artikel 18, stk. 2 og artikel 18, stk. 2, 2. pind:

> "*Medlemsstaterne må kun give mulighed for forenklet anmeldelse eller fritagelse for anmeldelse i følgende tilfælde og på følgende betingelser:*"
>
> "*- de registeransvarlige udpeger i overensstemmelse med den nationale lovgivning, som de er underlagt, en person med ansvar for beskyttelse af personoplysninger (...)*".

2.5.2.2 Implementering af Direktivets art. 18 i dansk ret

I forbindelse med implementeringen af Direktivet i dansk ret blev der nedsat et lovforberedende udvalg (kaldet *registerudvalget*), hvis opgave bestod i, at vurdere hvorledes

[100] REPORT FROM THE COMMISSION First report on the implementation of the Data Protection Directive (95/46/EC) Brussels, 15.5.2003 COM(2003) 265 final, s. 18 og 24.
[101] Meyer, D. (6. Juni 2016). What will mandatory DPOs look like under the GDPR? Germany could tell you. *The Privacy Advisor* .
[102] *Registeransvarlige* under Direktivet svarer til *Dataansvarlige* efter Forordningen.
[103] Jf. Direktivets art. 18, stk. 1.

Direktivets og dets mål bedst kunne blive implementeret i Danmark. Registerudvalget udarbejdede i den forbindelse en betænkning, hvor Direktivets artikler blev analyseret og fortolket. Her blev det gjort klart, at ordningen om en DPO efter Direktivets artikel 18, stk. 2, 2. pind ikke ville blive implementeret i dansk ret.[104] Afvisningen af ordningen i dansk ret begrundes særligt i, at 1) DPO'en efter Direktivet skal kunne fungere fuldt uafhængig, og dette ville skabe problemer mellem DPO'en og ledelsen, samt at 2) udpegelsen af en person, der har ansvaret for overholdelsen af den implementerede lov, vil skabe en stor og unødvendig byrde for virksomhederne.[105] Det er ikke specificeret i betænkningen, hvori denne byrde ligger.

Ovenstående er bemærkelsesværdigt, da Direktivet som hovedregel forpligter medlemsstaterne til at indføre en generel anmeldelsespligt efter Direktivets art. 18, stk. 1. Dette giver mulighed for en forsimplet anmeldelsespligt, såfremt virksomheden udpeger en DPO. Da udpegelsen af en DPO efter Direktivets ordlyd må forstås som et *frivilligt tilbud*, må det være op til den enkelte virksomhed at vurdere, hvorledes det er administrativt mere byrdefuldt at følge den normale anmeldelsespligt eller udpege en DPO.

Idéen om en DPO er derfor ikke en nyskabelse efter Forordningen, og rollen er ligeledes i forvejen blevet benyttet i andre EU-medlemsstater, men alligevel valgte Danmark ikke at benytte sig af muligheden. I år 2010 havde syv medlemsstater implementeret ordningen for at indføre DPO'er nationalt. Disse lande var Estland[106], Frankrig[107], Luxembourg[108], Malta[109], Holland[110], Sverige[111] og Tyskland. Det er dog kun i Tyskland, at udpegelsen af en DPO i

[104] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 336-337.
[105] Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger, s. 336-337.
[106] Jf. Estlands Databeskyttelseslov - *Personal Data Protection Act of 2007* § 30.
Riigi Teataja - Personal Data Protection Act. (3. Juli 2016). Hentet fra https://www.riigiteataja.ee: https://www.riigiteataja.ee/en/eli/ee/529012015008/consolide/current (tilgået d.18/03/2018).
[107] LOI INFORMATIQUE ET LIBERTES ACT N°78-17 OF 6 JANUARY 1978 ON INFORMATION TECHNOLOGY, DATA FILES AND CIVIL LIBERTIES art. 22, 3. pind. Loven er dog blevet ændret og opdateret flere gange - bl.a. af Direktivet.
Commission Nationale de l'Informatique et des Libertés . (u.d.). Hentet fra https://www.cnil.fr/: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf (tilgået d. 18/03/2018).
[108] Jf. Luxembourgs Databeskyttelseslov - *Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data* art. 12, stk. 2, litra a).
National Commission For Data Protection. (u.d.). Hentet fra https://cnpd.public.lu/en.html: https://cnpd.public.lu/content/dam/cnpd/en/legislation/droit-lux/doc_loi02082002mod_en.pdf (tilgået d. 18/03/2018).
[109] Jf. Maltas' Databeskyttelseslov - *Data Protection act of 2001* § 30, stk. 1
The Laws of Malta website. (4. May 2018). Hentet fra http://www.justiceservices.gov.mt/: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8906&l=1 (tilgået d. 18/03/2018).
[110] Jf. Holland's Databeskyttelseslov - Personal Data Protection Act of 2001 art. 62. https://rm.coe.int/16806af297 (tilgået d. 18/03/2018) (uofficiel oversættelse af den Hollandske lov). Se

visse situationer er obligatorisk efter national lov. I de andre seks lande er udpegelsen frivillig efter Direktivet fremgangsmåde.[112]

Det er med ovenstående gjort klart, at der på EU-niveau ikke har været et obligatorisk krav ved udpegelsen af DPO'en[113] efter de kriterier, der er opstillet i Forordningens art. 37. Der er således ikke noget relevant praksis at videreføre fra Direktivet, der kan bidrage til fortolkningen af Forordningens artikel 37.

I nedenstående afsnit vil andre fortolkningsmuligheder blive vurderet.

2.5.3 Artikel 29-gruppens vejledning

Forordningens art. 37 regulerer de situationer, hvor der skal udpeges en DPO hos en dataansvarlig/databehandler. Hverken denne artikel eller Forordningens præambel (med undtagelse af betragtning 97) uddyber mere specifikt, hvornår artiklens betingelser er opfyldt. Til hjælp for dette har *Gruppen* (Artikel 29-gruppen) udstedt en vejledning, der skal hjælpe adressaterne med at fastslå, hvornår de skal udpege en DPO.

Gruppen er det populære navn for den samling, der er nedsat med hjemmel i Direktivets artikel 29. Ifølge Direktivets art. 29, stk. 1's formulering skal der nedsættes "*(...) en gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger*". Gruppen består af en repræsentant fra hver medlemsstats tilsynsmyndighed og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne samt af en repræsentant fra Kommissionen.[114] Det nuværende danske medlem af Gruppen er direktøren for det danske datatilsyn Cristina Angela Gulisano. Gruppen er efter art. 29, stk. 1 uafhængig, og den skal kun fungere som en rådgivende instans.

Gruppen har siden sin oprettelse udstedt flere vejledninger, der skal hjælpe medlemsstaterne og adressaterne med at forstå, hvordan Direktivets artikler korrekt skal anvendes. Disse vejledninger bliver kaldt *working papers*, men de vil fortsat blive kaldt

---

også guidelines fra det Hollandske justitsministerium vedrørende samme lov på side 44. https://www.privacy.nl/uploads/guide_for_controller_ministry_justice.pdf (tilgået d. 18/03/2018).

[111] Jf. Sveriges *The personal data protection act (1998:204)* sektion 36 http://www.wipo.int/edocs/lexdocs/laws/en/se/se097en.pdf (tilgået d. 18/03/2018).

[112] Christoph Klug, *Improving self-regulation through (law-based) Corporate Data Protection Officials, 2010,* The German Association for Data Protection and Data Security (GDD), s. 1.

[113] Med undtagelsen af Tysklands nationale lov der ikke kan finde anvendelse, da en medlemsstats national lov ikke binder andre medlemsstater.

[114] Direktivets art. 29, stk. 2.

vejledninger i dette speciale.[115] Ligeså har Gruppen været aktiv med sin udstedelse af vejledninger i forbindelse med overholdelsen af Forordningen, da den indtil videre har offentliggjort 15 vejledninger.[116] Der er ligeså udstedt en vejledning specifik til udpegelsen af DPO'er.[117] Gruppens vejledning til udpegelse af DPO'er er dermed et redskab, der kan benyttes til at fastslå, om spejderforeningerne er forpligtede til at udpege en DPO.

2.5.3.1 Vejledningernes retskildemæssige værdi

2.5.3.1.1 TEUF art. 288

Gruppens udtalelser og henstillinger karakteriseres som værende *soft law*, hvilket vil sige ikke-bindende sekundær regulering jf. TEUF art. 288 (dette blev beskrevet på side 11). *Soft law* er dermed ikke bindende for dennes adressater, og de omtalte vejledninger kan som udgangspunkt udelukkende benyttes som fortolkningsbidrag til den konkrete problemstilling. Det er vist, at der ikke er noget retspraksis at videreføre fra Direktivet vedrørende udpegelsen af DPO'er. Gruppens vejledning vil derfor fungere som det primære fortolkningsbidrag til afgørelsen af, hvorvidt spejderforeningerne er forpligtede til at udpege DPO'er. Der er derfor først værd at vurdere, hvilken retskildemæssig værdi Gruppens vejledninger egentlig har.

2.5.3.1.2 EU-domstolens praksis vedrørende anvendelsen af soft law

Det skal først og fremmest næves, at når EU-domstolen afsiger domme for at løse konflikter, bliver både bindende og ikke-bindende regulering fortolket, og soft law bliver således inddraget ved afgørelser.[118] Udover dette har domstolen i sin hidtidige praksis henvist til ikke-bindende regulering i selve afgørelsen, såfremt der var relevant soft law at inddrage.[119]

---

[115] *European Commission's website.* (12. December 2017). Hentet fra http://ec.europa.eu/: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=59485 (tilgået d. 20/03/2018).

[116] En oversigt over de udstedte vejledninger i forbindelse med Forordningen kan findes på *Datatilsynets hjemmeside.* (20. April 2018). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/ (tilgået d. 22/04/2018).

[117] Guidelines on Data Protection Officers (*DPOs*) WP 243 rev. 01.

[118] Sag C-113/75: Dommens parter er Giordano Frecassett mod den Italienske finansforvaltning. Sagen omhandler fortolkningen af begrebet *indførselsdagen,* og det er relevant i forhold til den toldafgift, der på dette tidspunkt blev pålagt majs. Der bliver i sagen stillet tre spørgsmål, hvor der til spørgsmål to bliver anmodet om en fortolkning af Kommissionens henstilling (*soft law*) vedrørende begrebet indførselsdagen.

[119] Sag C-222/84: Dommens parter var Marguerite Johnston mod politidirektøren for det nordirske politi. Sagen vedrørte en afskedigelse af Marguerite, der arbejdede som reservebetjent. Det hævdes i sagen, at afskedigelsesgrundlaget strider imod ligebehandlingsdirektivet, men at nationale love forhindrede en effektiv domstolsprøvelse. Domstolen blev derfor spurgt, om en sådan foranstaltning stred imod fællesskabsretten. Her nævner domstolen i præmis 18, at en ret til effektiv domstolsprøve er et retsprincip, der også nævnes i Konventionen for beskyttelse af menneskerettighederne.

Soft law kan derfor ikke umiddelbart negligeres som retskilde, og har om ikke andet betydning for selve fortolkningen af de retskilder, der reelt er bindende - i dette tilfælde Forordningens art. 37.

EU-domstolen har i sag C-322/88 (også kendt som *Grilmaldi-sagen*) givet udtryk for, at ikke-bindende regulering ikke er uden retsvirkning. Her sagde domstolen, at "*(...) de omhandlede henstillinger ikke kan anses for at være ganske uden retsvirkninger. De nationale retsinstanser skal således ved afgørelsen af tvister, der indbringes for dem, tage hensyn til henstillinger, navnlig når disse kan bidrage til fortolkningen af nationale bestemmelser udstedt til gennemførelse heraf, eller når der er tale om henstillinger, som har til formål at udfylde bindende fællesskabsretlige bestemmelser.*". Vejledningen om udpegelse af DPO'er har netop til formål at hjælpe med at udfylde en bindende fællesskabsretlig bestemmelse, nemlig den obligatoriske forpligtelse til at udpege en DPO.

Kommissionen udtrykker lige så om Gruppens vejledninger i sin meddelelse vedrørende anvendelsen af Forordningen[120], at "*(...) databeskyttelsesmyndighederne vil henvise til dem ved håndhævelsen af forordningen".*[121]

Det er med ovenstående gjort klart, at Gruppens vejledninger kan bruges til udledningen af gældende ret. Dette kan gøres på trods af, at en vejledning fra Gruppen er karakteriseret som *soft law*.

2.5.3.2 Vejledningernes anvendelse når Direktivet erstattes

Gruppen er oprettet med hjemmel i Direktivets artikel 29, som erstattes af Forordningen, når denne træder i kraft.[122] Det er derfor relevant at undersøge, hvad dette kommer til at betyde for de nuværende og eventuelle fremtidige vejledninger fra Gruppen, og om disse fortsat er gældende, efter Direktivets er blevet erstattet.

Ved Forordningens ikrafttræden introduceres Gruppens efterfølger[123] - Det Europæiske Databeskyttelsesråd (herefter kaldet *Rådet*).[124] Rådets medlemmer kommer til at være

---

Principper, der fremgår i konventionen, bliver af EU-kommissionens henstilling (*soft law*) fra 5. april 1977 (EFT C 103, s. 1) fastslået som værende gældende i fællesskabsretten.

[120] MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET - Stærkere beskyttelse, nye muligheder – Kommissionens vejledning om den direkte anvendelse af den generelle forordning om databeskyttelse fra den 25. maj 2018 - COM(2018) 43 final.

[121] Danmark er undtaget for dette, men efter Forordningen er det de lokale tilsynsmyndigheder, der har beføjelse til at udstede administrative bøder efter art. 83, såfremt de områder af Forordningen, der vedrører artikel 83, ikke overholdes. jf. Forordningens præambel betragtning 151.

[122] Forordningens artikel 94, stk. 1.

[123] Jf. Forordningens præambel, betragtning 139.

[124] Det Europæiske Databeskyttelsesråd er reguleret i Forordningens art. 68-76.

chefen for de enkelte medlemsstaters tilsynsråd samt Den Europæiske Tilsynsførende for Databeskyttelse.[125] I Danmark betyder det, at det nuværende medlem af Artikel 29-gruppen, Cristina Angela Gulisano, vil være Danmarks repræsentant, da hun er den nuværende direktør for Datatilsynet.[126] Rådets opgaver er oplistet i Forordningens art. 70, stk. 1, litra a-y), og de er som udgangspunkt ganske omfattende. Særligt at bemærke er litra e), der omhandler Rådets forpligtelse til at udstede retningslinjer/vejledninger for at fremme en ensartet anvendelse af Forordningen. Rådet kommer altså til at overtage/fortsætte Gruppens funktion med udarbejdelse af vejledninger.[127]

I forbindelse med dette nævner Kommissionen i sin meddelelse vedrørende anvendelsen af Forordningen, at den har "*(...) støttet arbejdet i Artikel 29-Gruppen, også med henblik på at sikre en gnidningsløs overgang til Det Europæiske Databeskyttelsesråd*".[128]

Det må ud fra det ovenstående forstås, at Gruppen som sådan ikke ophører med at eksistere. Gruppen bliver i stedet omdannet til Rådet. Dermed må vejledningerne, som er udstedt af Gruppen med hjemmel i Direktivet, fortsat være gældende, når Direktivet udgår, og Rådet tager over.

2.5.4 Nationale vejledninger

2.5.4.1 Forordningens art. 47

Ligesom det var tilfældet under Direktivet[129], skal der efter Forordningen udpeges en kompetent tilsynsmyndighed i hver medlemsstat. Denne skal sørge for, at Forordningen bliver korrekt anvendt i medlemsstaten.[130] Tilsynene i de forskellige medlemsstater skal både individuelt og ved samarbejde sikre en ensartet anvendelse af Forordningen i EU. Tilsynene er i denne forbindelse blevet pålagt en række opgaver, kompetencer og undersøgelsesbeføjelser.[131] Opgaverne er oplistet i Forordningens art. 47, litra a-v), hvoraf de væsentligste er at sørge for 1) håndhævelsen af Forordningen, 2) at behandle klager indsendt af krænkede data-subjekter, 3) at rådgive Regeringen og Folketinget vedrørende

[125] Jf. Forordningens art. 68, stk. 3.
[126] *Datatilsynets hjemmeside.* (28. Marts 2018). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/om-datatilsynet/medarbejdere/ (tilgået d. 20/03/2018).
[127] Forordningens art. 70, stk. 1, litra f-k), handler ligeså om udstedelse af diverse vejledninger. Disse vejledninger skal alle udstedes i overensstemmelse med litra e).
[128] MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET - Stærkere beskyttelse, nye muligheder – Kommissionens vejledning om den direkte anvendelse af den generelle forordning om databeskyttelse fra den 25. maj 2018 - COM(2018) 43 final.
[129] Jf. Direktivets art. 28.
[130] Jf. Forordningens art. 51, stk. 1.
[131] Se Forordningens art. 56 for kompetencerne, art. 57 for opgaverne og art. 58 for beføjelserne.

Forordningens anvendelse og 4) at udstede vejledninger, der skal fremme de dataansvarliges forståelse af deres pligter.[132] Ligesom det er tilfældet med Rådet, har Datatilsynet hjemmel i Forordningen til at udstede vejledninger, som de dataansvarlige og databehandlerne, der hører under Datatilsynets jurisdiktion, kan forholde sig til. Datatilsynet har ligeså udstedt en national vejledning vedrørende udpegelsen af DPO'er.[133]

På trods af at medlemsstaternes tilsyn har hjemmel til at udstede nationale vejledninger, må disse ikke stride imod de vejledninger, der er blevet udarbejdet af Gruppen eller vil blive udstedt af Rådet (medmindre det er en vejledning vedrørende de åbne artikler i Forordningen). Kommissionen gør dette klart i sin meddelelse vedrørende anvendelse af Forordningen, at nationale retningslinjer skal "*(...) enten ophæves eller bringes i overensstemmelse med dem, der er vedtaget af Artikel 29-Gruppen/Det Europæiske Databeskyttelsesråd om samme emne".*[134] Dette er dog ikke ensbetydende med, at de nationale vejledninger ikke har nogen fortolkningsmæssig værdi.

De nationale vejledninger går mere i dybden vedrørende de nationale forhold. Vejledningen fra Gruppen fortæller fx, at medlemsstaterne blot selv har mulighed for at definere begreberne *offentlig myndighed* og *offentligt organ*, hvorimod vejledningen fra Datatilsynet netop specificerer, hvad der i Danmark skal forstås med disse begreber. Dermed kommer de nationale vejledninger til at bidrage til fortolkningen af, hvornår en dataansvarlig (og spejderforeningerne) i Danmark er forpligtet til at udpege en DPO.

2.5.5 Betænkningen til Forordningen

Da dansk lovgivning skal indrettes efter Forordningen, blev det i Justitsministeriet besluttet, at der skulle udarbejdes en betænkning, der skal indeholde en analyse af Forordningens regler med henblik på bl.a. vejledning.[135] Sædvanligvis indeholder en betænkning en redegørelse for den nuværende retstilstand, samt en vidtgående analyse af de lovmæssige ændringer der er nødvendige at foretage for at gennemføre den lov, som betænkningen

[132] Dall, N. P., Langemark, J., & Langebæk, A. (2016). *Persondataforordningen - en håndbog for praktikere* (1 udg.). Ex Tuto Publishing, s. 133.
[133] *Datatilsynets hjemmeside.* (December 2017). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf (tilgået d. 19/04/2018).
[134] MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET - Stærkere beskyttelse, nye muligheder – Kommissionens vejledning om den direkte anvendelse af den generelle forordning om databeskyttelse fra den 25. maj 2018 - COM(2018) 43 final.
[135] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 10.

bygger på.[136] I dette tilfælde er betænkningen baseret på Forordningen, og hvilke nyskabelser denne bringer til området for databeskyttelse. Betænkningen indeholder derfor en analyse af den nuværende retstilstand under den danske persondatalov og Direktivet samt en analyse af de enkelte artikler i Forordningen.

Analyserne der er foretaget i betænkningen, er baseret på de i forvejen eksisterende retskilder som f.eks. afsagt retspraksis. Dermed er betænkningen ikke blot analytikernes subjektive holdning. De steder i betænkningen hvor retstilstanden ikke er klar og entydig, indeholder betænkningen et bud på, hvordan retstilstanden kommer til at være baseret på de eksisterende retskilder.[137] I forbindelse med dette speciale vil betænkningen dermed kunne bidrage til fortolkningen af, om hvorvidt spejderforeningerne skal udpege en DPO efter Forordningens art. 37.

Det er med de ovenstående afsnit gjort klart, at spejderforeningerne er underlagt Forordningen, samt hvilke retskilder der er tilgængelige og anvendelige ved fortolkningen af, om disse skal udpege en DPO. I de kommende afsnit vil Forordningens art. 37, stk. 1, litra a-c) samt art. 37, stk. 4 blive analyseret. Dette gøres for at udlede, om spejderforeningerne skal udpege en DPO efter disse.

2.6 Udpegelse af DPO efter Forordningens art. 37

2.6.1 Forordningens art. 37, stk. 1, litra a)

Efter art. 37, stk. 1 litra a) skal alle offentlige myndigheder og organer udpege en DPO. Den eneste undtagelse er domstolen, når denne behandler persondata i forbindelse med sit hverv som domstol.

For at se om spejderforeningerne skal udpege en DPO efter denne bestemmelse, skal det undersøges, hvad der efter Forordningen menes med en *offentlig myndighed* eller et *offentligt organ*.

Forordningen definerer ikke nogle af de to begreber. Betragtning 45's sidste punktum i Forordningens præambel fortæller dog, at "*(...) det bør henhøre under EU-retten eller medlemsstaternes nationale ret at afgøre, om den dataansvarlige, der udfører en opgave i samfundets interesse eller i forbindelse med offentlig myndighedsudøvelse, skal være en*

[136] Nielsen, R., & Tvarnø, C. (2014). Retskilder & Retsteorier. København: DJØF, s. 90
[137] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 16.

offentlig myndighed eller en anden fysisk eller juridisk person, der er omfattet af offentlig ret (...)". Med ovenstående må det fortolkes, at medlemsstaterne har hjemmel til at beslutte, om opgaver i samfundets interesse skal udføres af offentlige myndigheder eller offentlige organer. Dermed må det også være op til medlemsstaterne at definere disse. Det er ligeledes Gruppens opfattelse, at medlemsstaterne selv skal have ret til at udarbejde definitionen.[138]

2.6.1.1 National ret om offentlige myndigheder og organer

Efter dansk ret er alle organer, der henregnes under den offentlige forvaltning efter forvaltningslovens § 1, stk. 1-2[139], at betegne som offentlige myndigheder eller organer. Derfor skal disse udpege en DPO efter Forordningens art. 37, stk. 1, litra a).[140]

Efter forvaltningsloven § 1, stk. 2, nr. 1-2 er følgende omfattet af loven: "*(...) al virksomhed, der udøves af 1) selvejende institutioner, foreninger, fonde m.v., der er oprettet ved lov eller i henhold til lov, og 2) selvejende institutioner, foreninger, fonde m.v., der er oprettet på privatretligt grundlag, og som udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentlig tilsyn og intensiv offentlig kontrol*".

Der er i specialet fokus på spejderforeninger, der er oprettet på et frivilligt grundlag, hvorefter forvaltningslovens § 1, stk. 2, nr. 1 ikke er relevant. Denne lov finder netop anvendelse på institutioner o.l., der er oprettet ved lov, og dermed ikke blot kan lukke/opløses på frivillig basis.

Efter ordlyden af forvaltningslovens § 1, stk. 2, nr. 2 vil visse foreninger være forpligtet til at udpege en DPO, mens andre ikke vil være det. Det vil afhænge af de opgaver, som foreningen udfører, og hvor meget kontrol det offentlige har over foreningen. Begrebet *offentlig virksomhed* er ikke defineret i nogen dansk lov eller i retspraksis. Det følger dog af betænkningen til offentlighedsloven, at offentlig virksomhed i hvert fald dækker over udfærdigelsen af retsakter, samt anden virksomhedsudøvelse der normaltvist anses for decideret forvaltningsvirksomhed (såsom sygepleje og undervisning).[141] Betænkningens

[138] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 570.
[139] Bekendtgørelse af forvaltningsloven LBK nr 433 af 22/04/2014.
[140] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn s. 14.
[141] Betænkning om offentlighedsloven (1510/2209), s. 272.

opfattelse, af hvad offentlig virksomhed er, stemmer til dels overens med Gruppens opfattelse jf. deres vejledning.[142]

Der er i specialet taget udgangspunkt i spejderforeninger, hvis formål og aktiviteter ikke falder ind under begrebet om offentlig virksomhed. Dette gælder hverken efter betænkningen til offentlighedsloven eller efter Gruppens vejledning.

Da betingelserne for at være omfattet af forvaltningslovens § 1, stk. 2, nr. 2 må fortolkes at være kumulative ud fra deres ordlyd, er spejderforeningerne ikke forpligtet til at udpege en DPO efter Forordningens art. 37, stk. 1, litra a).

2.6.2 Forordningens art. 37, stk. 1, litra b)

2.6.2.1 De kumulative betingelser

Efter Forordningens art. 37, stk. 1, litra b) skal en dataansvarlig udpege en DPO, når "*(...) den dataansvarlige eller databehandlerens kerneaktiviteter består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang.*"

Baseret på artiklens udformning har Gruppen i sin vejledning delt artiklen op i tre kumulative betingelser.[143] Disse betingelser er i vejledningen fra Datatilsynet udtrykt som følgende:

1) "*Behandling af personoplysninger skal være virksomhedens kerneaktivitet*,
2) *Behandlingsaktiviteten består af regelmæssig og systematisk overvågning af personer* og
3) *der skal behandles data i et stort omfang".*[144]

De kumulative betingelsers betydning vil blive forklaret i de følgende afsnit - startende med begrebet *kerneaktivitet.* Når alle tre begreber er blevet analyseret, vil de derefter blive sat op imod de databehandlingsaktiviteter, der sker i spejderforeningerne.

2.6.2.1.1. Begrebet 1) *kerneaktivitet*

Definitionen på en dataansvarlig og en databehandler er nævnt i afsnittet om Forordningens anvendelsesområde på side 25. Det er ud fra denne definition klart, at spejderforeningerne opfylder kravet til en dataansvarlig. For at udlede om spejderforeningerne som dataansvarlige er omfattet af Forordningens art. 37, stk. 1, litra b), kræver det altså bl.a., at

[142] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 6.
[143] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 7-9.
[144] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 6.

foreningernes kerneaktivitet er persondatabehandling. Der vil i de følgende afsnit blive udledt, hvad der efter vejledningerne menes med en *kerneaktivitet*.

Kerneaktivitet er ikke defineret i Forordningen, selvom begrebet fremgår af både Forordningens art. 37, stk. 1, litra b) og c) (se nedenfor på side 55 for litra c)). Betragtning 97 i Forordningens præambel specificerer dog begrebet en smule. Efter betragtning 97 skal den dataansvarliges kerneaktiviteter forstås som dennes *hovedaktiviteter*. Der skal med denne nærmest synonyme begrebsforklaring forstås, at persondatabehandlingen, som foretages af den dataansvarlige, ikke blot skal være en *biaktivitet* som følge af hovedaktiviteten.[145]

Gruppen kommer yderligere med en fortolkning af begrebet i deres vejledning. Ifølge Gruppen skal *kerne-/hovedaktiviteterne*, som foretages af den dataansvarlige, forstås som "*(...) de centrale aktiviteter, der er nødvendige for at opnå den dataansvarlige eller databehandlerens mål*".[146] For at persondatabehandling kan kvalificeres som en kerneaktivitet, skal denne altså være en *nødvendig* aktivitet, for at den dataansvarlige kan opnå sit mål. Hvad der menes med den dataansvarliges mål uddybes ikke i vejledningen, men det må antages at være individuelt for den enkelte dataansvarlige.

For en privat virksomhed vil målet/formålet som regel være at udbyde et produkt eller tjenesteydelse for at opnå en profit. En privat virksomhed der fx producerer og sælger færdigvarer, vil derfor have som mål at opnå en fortjeneste via denne aktivitet. Virksomhedens kerneaktivitet vil være de specifikke aktiviteter, der er nødvendige for, at virksomheden kan opnå denne profit. Altså vil produktionen og salget af produktet være at betragte som kerneaktiviteten.

I dette speciale fokuseres der på spejderforeninger, der ikke har sine medlemmers økonomiske interesse for øje. Disse foreningers "mål" er ikke at optjene en egentlig profit til medlemmerne/ejerne, men derimod at sørge for at selve foreningens formål bliver opnået. Kerneaktiviteterne for spejderforeningerne må derfor være de aktiviteter, der er nødvendige for, at foreningernes medlemmer kommer til at lære om demokrati, selvstændighed og medansvar.[147]

Det er med ovenstående gjort klart, hvad der efter Forordningen skal forstås ved en kerneaktivitet. I analysen er spejderforeningernes kerneaktivitet indtil videre ikke behandling

[145] Jf. Forordningens præambel betragtning 97, 2. pkt.
[146] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev. 01 (Dansk version) s. 7.
[147] Dette blev forklaret i indledningen til specialet side 7.

af persondata. Der vil derfor i nedenstående afsnit blive set på, i hvilke situationer persondata udgør en faktisk kerneaktivitet for spejderforeningerne.

2.6.2.1.1.1 Persondatabehandling som en kerneaktivitet

Ifølge vejledningen fra Datatilsynet er persondatabehandling omfattet af begrebet *kerneaktiviteter* i to tilfælde:

Det første og mest oplagte tilfælde er, når den ydelse eller det produkt, der udbydes, decideret består af persondatabehandling. Dette er fx tilfældet, når en virksomhed, der som sin kerneaktivitet tilbyder lagring af persondata via en *cloud*-løsning, eller når der fx udbydes markedsundersøgelser baseret på persondata.[148] I tilfældet med *cloud*-løsningen er kerneaktiviteten selve opbevaringen af dataen. Lagring af data er omfattet af behandlingsbegrebet, se side 27, og persondatabehandling er dermed en kerneaktivitet. Det er også tilfældet med markedsundersøgelser, der er baseret på persondata. En virksomhed bestiller således ikke en markedsundersøgelse om fx forbrugernes spisevaner for at få en liste over de enkelte personers vaner. De bestiller derimod rapporten for at få en overskuelig oversigt over fx forbrugernes madbudgetter eller forbrug. Rapporten er baseret på den bagvedliggende, indsamlede persondata, og derfor er den behandlede data at betragte som kerneaktiviteten.[149]

Persondatabehandlingen er i det andet tilfælde omfattet af kerneaktivitetsbegrebet, når persondatabehandlingen udgør en ***uundgåelig*** del af selve kerneaktiviteten.[150] Denne betingelse skaber i sin udformning stor usikkerhed for, hvornår betingelsen om *uundgåelighed* er opfyldt. Betingelsen kan fortolkes på mange måder, og Gruppens vejledning oplister derfor nogle situationer, hvor persondatabehandling udgør en uundgåelig del af kerneaktiviteten. Disse vil blive gennemgået i de følgende afsnit.

Et eksempel på en situation, hvor behandling af persondata er uundgåeligt forbundet med virksomhedens kerneaktivitet, er fx i forbindelse med et privat vagtselskab, der har til opgave at overvåge offentlige eller private områder for at øge sikkerheden. Virksomhedens kerneaktivitet er i dette tilfælde selve overvågningen af de områder, firmaet er hyret til at dække. Her er det netop umuligt for vagtfirmaet ikke at behandle persondata, da data-subjekterne, der befinder sig på de overvågede områder, bliver optaget og lagret i overvågningssystemet. Persondataen, der bliver lagret som følge af overvågningen, vil

[148] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 8.
[149] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 8.
[150] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 8.

derfor skulle behandles efter Forordningens regler. Dermed er persondatabehandling en uundgåelig del af vagtfirmaets kerneaktivitet.[151]

Et andet eksempel er *privathospitaler*, hvor persondatabehandlingen er mere indirekte en uundgåelig del af virksomhedens kerneaktivitet. Kerneaktiviteten er i sin natur selve sundhedsplejen til hospitalets patienter. Selvom et hospital i princippet godt kan yde sundhedspleje uden behandling af persondata, er et hospital nødt til behandle persondata som en uundgåelig del af kerneaktiviteten, da ydelsen ikke ville kunne ydes på et sikkert grundlag uden at behandle patientens persondata.[152] For at få et indblik i patientens generelle helbred vil hospitalet være nødsaget til at se patientens lægejournal. Dette gøres bl.a. for at finde ud af, om patienten er allergisk overfor specifikt bedøvelse eller medicin. Den udførte sygepleje vil således være baseret på patientens persondata. Dermed er udførelsen af den korrekte og sikre sundhedspleje, som er hospitalets kerneaktivitet, afhængig af persondatabehandling i en sådan grad, at denne udgør en uundgåelig del af kerneaktiviteten.

Vejledningen specificerer dog ikke, i hvor høj grad udførslen af kerneaktiviteten skal være baseret på behandlet persondata, før at behandlingen er en uundgåelig del af kerneaktiviteten. Ifølge betænkningen til Forordningen er dette tilfældet, når "*(...) det pågældende produkt er baseret på behandling af personoplysninger i så høj grad, at der er tale om en kerneaktivitet*".[153] Sagt på en anden måde skal kerneaktiviteten ikke kunne udføres, uden at der foretages en høj grad af persondatabehandling i forbindelse med udførelsen.

2.6.2.1.1.2 Persondatabehandling som biaktivitet er ikke en uundgåelig del kerneaktiviteten

På trods af kriteriet om uundgåelighed har alle organisationer brug for at behandle en vis form for persondatabehandling, for at kerneaktiviteten kan udføres. Fx er det nødvendigt for en virksomhed at betale sine ansatte, og derfor behandles deres persondata. Ligeså sker der behandling af personoplysninger i forbindelse med kundekontakt og *support*-funktioner, der udføres som en service til (eller for at understøtte) selve kerneaktiviteten.[154] Set i perspektiv til dette speciale har spejderforeningerne ligeledes brug for persondata om sine medlemmer, for at disse fx kan betale medlemskontingent. Persondatabehandling, der

[151] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 7.
[152] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 7.
[153] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, betænkning nr. 1565, s. 563.
[154] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 7.

udføres som en forudsætning for, at kerneaktiviteten kan udføres, skal ikke forstås som persondatabehandling, der er uundgåeligt forbundet til organisationens kerneaktivitet, eller som en kerneaktivitet overhoved.[155] Disse skal i stedet betragtes som en biaktivitet, der ikke forpligter en dataansvarlig til at udpege en DPO. Hvis dette var tilfældet, ville stort set alle organisationer i den private sektor være forpligtede til at udpege en DPO.[156]

Det er med de ovenstående afsnit klargjort, hvad der skal forstås med en kerneaktivitet, og hvornår persondatabehandling er at betragte som en kerneaktivitet. I de følgende afsnit vil de to resterende betingelser blive gennemgået. Efterfølgende vil de kumulative betingelser fra Forordningens art. 37, stk. 1, litra b) blive sat op imod de databehandlingsaktiviteter, der sker i spejderforeningerne. Dette sker på side 47.

2.6.2.1.2 Begreberne 2) *regelmæssig og systematisk overvågning*

Den anden betingelse for at skulle udpege en DPO kræver, at "*(...) den dataansvarliges eller databehandlerens kerneaktiviteter består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede (...)".*[157]

2.6.2.1.2.1 Regelmæssig og systematisk overvågning

Betragtning 24 til Forordningens præambel tydeliggør, at formålet for dataindsamlingen skal være at træffe beslutninger om data-subjektet, for at den dataansvarlige skal kunne analysere eller forudsige den pågældendes præferencer, adfærd og holdninger. Umiddelbart virker dette ikke til at være tilfældet med spejderforeningerne, men hvis Gruppens fortolkninger til de to begreber benyttes, kan det ikke udelukkes, at det inkluderer spejderforeningers behandling af persondata. Nedenfor er der beskrevet, hvad Gruppen mener, at begreberne *regelmæssig og systematisk* skal forstås som. Ligeså er der understreget, hvad der er relevant at inddrage fra Gruppens vejledning i forhold til spejderforeningerne:[158]

[155] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 7.
[156] Forudsat at de resterende betingelser for udpegelsen af en DPO efter Forordningens art. 37, stk. 1, litra b) er opfyldt.
[157] Jf. Forordningen art. 37, stk. 1, litra b).
[158] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 9.

Regelmæssig

1. *vedvarende eller forekommende persondatabehandling med bestemte intervaller i en bestemt periode*
2. *tilbagevendende eller gentaget på faste tidspunkter*
3. *konstant eller periodisk forekommende.*

Systematisk

1. *forekommer ifølge et system*
2. *forudarrangeret, organiseret eller metodisk*
3. *finder sted som led i en generel plan for dataindsamling*
4. *udføres som en del af en strategi.*

Når spejderforeningerne varetager deres medlemmers persondata, må dette (fx ved ind- og udmelding) klassificeres som "konstant eller periodisk forekommende", og derfor foretages den regelmæssigt. Derudover vurderes det, at alle fire punkter vedr. "systematisk" er opfyldt, da foreningerne behandler medlemmernes data på sådan en måde ved medlemskab, kommunalt tilskud[159] o.l.

Gruppen kommer afslutningsvist med eksempler på, hvornår de to begreber *systematisk* og *regelmæssig* forekommer.[160] Da der her nævnes aktiviteter som drift af telekommunikationsnet- og tjenester, e-mail-retargeting, kreditvurdering, risikovurdering, sporing af opholdssted, overvågning af sundhedsdata o.l., vurderes spejderforeningerne ikke som udgangspunkt at være omfattet af disse begreber. En dybere juridisk analyse af de faktiske forhold i spejderforeningerne vil være nødvendig for at afgøre dette med sikkerhed.

2.6.2.1.3 Begrebet 3) *stort omfang*

Den tredje betingelse for at skulle udpege en DPO er, at "*(...) den dataansvarliges eller databehandlerens kerneaktiviteter består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang (...)*"[161].

2.6.2.1.3.1 Databehandlingen foretaget i "stort omfang"

Begrebet "stort omfang" benyttes både i Forordningen art. 37, stk. 1, litra b) og c), men der defineres ikke, hvordan det skal forstås. Betragtning 91 giver i stedet en fortolkning: "*(...)*

[159] Se mere om dette i afsnit X vedr. kommunalt tilskud.
[160] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 9.
[161] Jf. Forordningen art. 37, stk. 1, litra b).

omfattende behandlingsaktiviteter til behandling af meget store mængder personoplysninger på regionalt, nationalt eller overnationalt plan, der kan berøre mange registrerede, og som sandsynligvis vil indebære en høj risiko, f.eks. på grund af behandlingsaktiviteternes følsomhed (...)". Artikel 29-gruppen tydeliggør, det ikke er muligt at fremsætte et præcist tal for, hvornår *stort omfang* er opnået, men følgende bør af den dataansvarlige tages i betragtning:[162]

1) *"Antallet af registrerede som behandles – enten som specifikt tal eller som en procentdel af den relevante befolkningsgruppe*
2) *mængden af data og/eller omfanget af forskellige datatyper,som behandles*
3) *databehandlingsaktivitetens varighed eller permanens*
4) *databehandlingsaktivitetens geografiske udstrækning"*

Persondataen på medlemmer ved spejderrelaterede aktiviteter kan som udgangspunkt godt blive inkluderet under denne betingelse, men Gruppens egne eksempler på *stort omfang* inkluderer ikke specifikke spejderrelaterede aktiviteter.[163] Derfor skal der foretages en yderligere juridisk udledning af punkterne, før der kan vurderes, om denne type folkeoplysende foreninger er omfattet af punkterne.

2.6.2.2 Persondatabehandling som kerneaktivitet i spejderforeningerne

Ovenfor ved betingelse 1-3 er det forklaret, hvordan begreberne i art. 37, stk. 1, litra b) skal forstås. Det er obligatorisk at udpege en DPO, hvis alle tre begreber vurderes at være opfyldt.

Der vil i de følgende afsnit blive set på situationer, hvor spejderforeningerne (og foreninger generelt) behandler persondata i forbindelse med deres virke, og om denne persondatabehandling kan kvalificeres som de ovenstående begreber.

Der vil blive set på følgende behandlingssituationer:

1) persondatabehandling i forbindelse med driften af en forening
2) persondatabehandling i forbindelse med ansøgning af kommunale tilskud
3) persondatabehandling i forbindelse med de udførte aktiviteter i spejderforeningerne

2.6.2.2.1 Persondatabehandling påkrævet for at drive en forening

Foreningsretten er ikke materialiseret i dansk lov, og foreningsretten reguleres derfor primært efter foreningernes egne vedtægter. Der er dermed ikke en officiel reguleringsform,

[162] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 8.
[163] Fx forretningsgangen på et hospital, rejsedata i det offentlige transportsystem, geolokaliseringer, kundeinformationer i banker o.l.

der fortæller, hvilken eller hvornår persondata skal indsamles af spejderforeningerne. Foreninger kan dog være i en situation, hvor de er tvunget til at følge bestemte regelsæt.[164]

Således er foreninger underlagt persondataloven (der erstattes af Forordningen d. 25. maj 2018), når disse indsamler og behandler medlemmernes persondata. Dette er også tilfældet, når spejderforeningerne bliver tildelt økonomisk støtte fra det offentlige. Den økonomiske støtte kan tildeles direkte i form af midler fra kommunen eller staten eller mere indirekte i form af en skattebegunstigelse (foreninger kan slippe for at betale skat af de bidrag, der frivilligt bliver givet til foreningen, for at denne nemmere kan opnå sit formål).[165]

For at opnå den kommunale støtte er spejderforeningerne nødt til at opfylde kravene i de relevante love, også hvis dette omfatter behandling af persondata. Der er ligeledes retspraksis, der regulerer foreningsretten for, hvornår disse skal behandle persondata.

I modsætning til fx kapitalselskaber gælder der ingen formelle formkrav for selve *stiftelsen* af en forening. En forening stiftes derfor ved den blotte aftale mellem to eller flere personer, som ønsker at opnå et fælles mål gennem en forening. Der er end ikke krav om, at stiftelsen skal ske på et skriftlige grundlag.[166]

Når foreningen først er stiftet, er der alligevel nogle krav, der skal overholdes, for at denne bliver betragtet som en forening udadtil, så den får status som juridisk person. Der er i alt fire krav, men kun det persondataretlige krav nævnes her. For at blive betragtet som en forening kræves det, at foreningen har flere medlemmer, og at disse til et vist punkt kan identificeres.[167] De resterende tre antages at være opfyldt.[168]

2.6.2.2.1.1 Krav om identifikation af medlemmerne

Medlemmerne skal altså til en vis grad kunne *identificeres*. Der er derfor et persondataretligt krav, før at foreninger overhoved kan bestå. Der er efterfølgende af henviste domsafsigelse

[164] Hansen, S. F., & Krenchel, J. V. (2017). *Introduktion til dansk selskabsret II personselskaber, foreninger og fonde* (3 udg.). Karnov Group, s. 195.
[165] Hasselbalch, O. (2011). *Foreningsret* (4 udg.). Jurist- og Økonomforbundets forlag, s. 42.
[166] Hansen, S. F., & Krenchel, J. V. (2017). *Introduktion til dansk selskabsret II personselskaber, foreninger og fonde* (3 udg.). Karnov Group, s. 202.
[167] Se bl.a. UfR 1969.898V: I sagen fandtes der to medlemslister for en forening der var stiftet i 1904. Den ene liste blev lavet da foreningen blev stiftet, og den efterfølgende i år 1932. Da foreningens formand på vegne af foreningen optrådte i retten vedrørende en ejendomstvist, var formanden ikke i stand til at oplyse hvor mange medlemmer foreningen havde eller identiteten på disse. Dermed kunne foreningen ikke optræde som juridisk enhed i retten.
[168] 1) en del af foreningens formue skal være adskilt fra medlemmernes,
2) der skal være en ledelse, og
3) foreningen skal have en vis kompetence til at handle på fællesskabets vegne. Kilde: U.1997B.273, Jens Valdemar Krenchel, Søren Friis Hansen: Refleksioner over foreningsbegrebet.

(UfR 1969.898V) ikke blevet opstillet nogle krav eller definitioner, der nærmere beskriver, hvad der menes med *identificeres*. Det må antages ved tidspunktet for dommen, at der er tale om minimum medlemmets *navn* og *kontaktoplysninger*.

Udover det lovmæssige krav kan der opstå mange situationer, hvor det er nødvendigt at have indsamlet persondata om medlemmerne. Såfremt der skal indbetales kontingent, skal foreningerne have navn og adresse på den/de relevante personer. Ifølge Center for Frivilligt Socialt Arbejde (CFSA) skal der ved "almindelige medlemsoplysninger" (i frivillige foreninger), forstås information som *navn*, *adresse*, *indmeldelsesdato*, *telefonnummer*, *fødselsdato*, *mailadresse* mv.[169]

Der skal altså behandles persondata i en forening til en vis grad. Dette må således også være tilfældet for spejderforeningerne i dette speciale. Inden det afgøres, om denne databehandling er at betragte som spejderforeningernes kerneaktivitet, vil der først blive udledt, om der sker persondatabehandling i forbindelse med ansøgningen om kommunale tilskud i spejderforeningerne. Hvis dette er tilfældet, vil det blive analyseret om en eller begge af disse databehandlingsaktiviteter, er at betragte som spejderforeningernes kerneaktivitet.

2.6.2.2.2 Kommunale tilskud til foreninger

Spejderforeningerne blev i indledningen til dette speciale klassificeret som folkeoplysende foreninger med ret til kommunale tilskud. Det blev dog ikke uddybet, hvorfor disse foreninger er berettiget til kommunale tilskud, og hvilke krav til der stilles til foreningerne for at blive betragtet som en folkeoplysende forening. Danske kommuner er forpligtet til at støtte visse typer af foreninger efter serviceloven, og der afsættes derfor et beløb i alle kommuner til dette formål. Efter serviceloven § 18, stk. 1[170] er kommunerne forpligtet til at "*(...) samarbejde med frivillige sociale organisationer og foreninger (...)*", og efter servicelovens § 18, stk. 2 er kommunalbestyrelsen ligeså forpligtet til "*(...) årligt at afsætte et beløb til støtte af frivilligt socialt arbejde*".[171] Det er dette beløb, spejderforeningerne kan ansøge om tilskud fra.

[169] Center for Frivilligt Socialt Arbejde (CFSA) er det landsdækkende udviklings-, kompetence- og videnscenter på velfærdsområdet i Danmark.
Center for Frivilligt Socialt Arbejde. (29. November 2017). Hentet fra https://frivillighed.dk: https://frivillighed.dk/guides/regler-for-foreningers-brug-og-behandling-af-personoplysninger (tilgået 24/04/2018).
[170] Bekendtgørelse af lov om social service (LBK nr. 102 af 29/01/2018).
[171] Bekendtgørelse af lov om social service (LBK nr. 102 af 29/01/2018).

2.6.2.2.2.1 Krav til foreninger der ansøger om kommunale tilskud

For at spejderforeningerne kan komme i betragtning til de kommunale tilskud, kræves det, at de er klassificeret som folkeoplysende foreninger.[172] Dette afhænger af *strukturen* og *aktiviteten* i den relevante forening.[173] Kravene til selve foreningsstrukturen er ikke relevante for dette speciale, og de antages at være opfyldte. Derimod er kravene til hvilke aktiviteter, der skal udføres af foreningen, for at denne er at betragte som en folkeoplysende forening, relevante at tydeliggøre. Hvis aktiviteterne, der skal udføres for at være en folkeoplysende forening, indebærer persondatabehandling, vil dette hjælpe med at tydeliggøre, om spejderforeningerne skal have en DPO baseret på de udførte aktiviteter.

Efter folkeoplysningslovens § 4, stk. 1 er en forening at betragte som en folkeoplysende forening, når den 1) "*(...) tilbyder folkeoplysende voksenundervisning",* eller når den 2) "*(...) tilbyder frivilligt folkeoplysende foreningsarbejde.*"

Der er i specialet fokus på foreninger efter folkeoplysningslovens § 4, stk. 1, nr. 2, og der skal derfor undersøges, hvad der menes med folkeoplysende foreningsarbejde efter denne paragraf.

Efter folkeoplysningslovens § 14, stk. 2 rummer det frivillige folkeoplysende foreningsarbejde "*(...) idræt og idébestemt og samfundsengagerende børne- og ungdomsarbejde, hvortil der er knyttet deltagerbetaling.*".

Spejderforeningerne i dette speciale er netop frivillige foreninger, der tilbyder samfundsengagerende børne- og ungdomsarbejde, idet spejderforeningernes formål er at *"(...) oplære børn og unge om selvstændighed, medansvar, demokratisk livsholdning og mellemfolkelig forståelse".*[174] Dermed opfylder spejderforeningerne kravet til at være folkeoplysende foreninger, og de er dermed kvalificeret til at få kommunale tilskud. Der vil i det nedenstående afsnit blive set på, om der kræves persondatabehandling i forbindelse med ansøgningen om tilskud, og om denne databehandling kan betragtes som spejderforeningernes kerneaktivitet.

[172] Jf. § 1 og § 3 i Bekendtgørelse af lov om støtte til folkeoplysende voksenundervisning, frivilligt folkeoplysende foreningsarbejde og daghøjskoler samt om Folkeuniversitetet (folkeoplysningsloven) - LBK nr. 854 af 11/07/2011.
[173] Jf. folkeoplysningslovens § 4, stk. 1-3.
[174] Som set i indledningen til specialet.

2.6.2.2.2.2 Persondataretlige krav for at få kommunale tilskud

De økonomiske tilskud, som spejderforeningernes er berettiget til, kan være signifikante. For at spejderforeningernes kan fungere økonomisk, spiller tilskuddene derfor en væsentlig rolle. Beløbsstørrelsen afhænger af foreningens medlemstal. Det er kommunen, som den enkelte spejderforening er tilknyttet, der bestemmer beløbet, hvilket derfor kan variere.[175] Efter tilskudstaksterne fra år 2018 for Københavns Kommune kan en folkeoplysende forening få op til 1.400 kr. pr. foreningsmedlem under 25 år som tilskud til lokaleomkostninger. Yderligere kan den folkeoplysende forening få op til 290 kr. pr. foreningsmedlem under 25 år i almindeligt medlemstilskud.[176] Folkeoplysningsloven kræver dog, at spejderforeningerne udfører en vis form for persondatabehandling, for at de er berettiget til tilskuddet. Efter folkeoplysningsloven § 4, stk. 4 skal spejderforeningerne løbende indhente børneattester på alle individer, der enten direkte eller indirekte kommer i kontakt med børn under 15 år som led i deres aktivitet i foreningen. Børneattesterne skal ikke indsendes til kommunen, men foreningen er ikke desto mindre forpligtet til at indsamle og opbevare denne data alligevel.[177]

Det skal i forbindelse med børneattester nævnes, at disse er omfattet af Forordningens art. 9, stk. 1 om særlige kategorier af personoplysninger. Denne type af persondata må som udgangspunkt slet ikke behandles af en dataansvarlig, medmindre en af undtagelserne i Forordningens art. 9, stk. 2 finder anvendelse. Da der her er tale om folkeoplysende spejderforeninger uden gevinst for øje, må det antages, at Forordningens art. 9, stk. 2, litra d) finder anvendelse. Spejderforeningerne kan således indsamle og behandle børneattester på de beskæftigede i den relevante forening.

For at modtage selve tilskuddet skal der lige så sendes en ansøgning til kommunen med følgende persondataretligt materiale inkluderet:[178]

Navn, *adresse*, *e-mail*, *telefonnummer*, *postadresse* og *by* skal oplyses om følgende foreningspersoner:

- Revisoren,
- formanden,
- kassereren og
- øvrige bestyrelsesmedlemmer.

[175] Folkeoplysningslovens § 4, stk. 3, nr. 7.
[176] Se https://www.kk.dk/sites/default/files/uploaded-files/bilag_1_ansoegningsfrister_og_takster_2018.docx, (tilgået 13/05/2018)..
[177] *Københavns kommunes hjemmeside*. (u.d.). Hentet fra www.kk.dk: https://www.kk.dk/artikel/folkeoplysende-foreninger (tilgået 11/03/2018).
[178] Ansøgningen her, er den ansøgning der skal sendes hvis man som folkeoplysende forening i Københavns kommune, søger om tilskud.

Navn, *adresse* og *fødselsdato* skal ligeledes oplyses for:

- Alle aktive- og eller kontingentbetalende medlemmer af foreningen.[179]

Mængden af persondata der skal behandles, afhænger naturligvis af foreningens medlemstal. Det har ikke været muligt at finde en oversigt, der viser medlemstallene for samtlige danske spejderforeninger - store som små. Det har derimod været muligt at finde medlemsopgørelsen for henholdsvist KFUM-spejderne, og spejderforeninger der er tilknyttet Det Danske Spejderkorps. Hos KFUM-spejderne var der således 28.940 medlemmer fordelt ud på 494 individuelle grupper[180] og Det Danske Spejderkorps havde 35.872 medlemmer i 2017[181] fordelt ud på omkring 400 selvkørende foreninger.

I forbindelse med ansøgning af kommunale tilskud kan der altså behandles en betydelig mængde persondata fra spejderforeningerne side afhængig af deres størrelse.

I de ovenstående afsnit er der blevet set på to situationer, hvor spejderforeningerne er nødsagede til at behandle persondata som følge af deres virke.

Foreningerne skal således 1) kunne identificere sine medlemmer for at have status som juridisk enhed og 2) indsende oplysninger om samtlige foreningsmedlemmer, og indhente børneattester på visse ansatte i foreningen for at få kommunale tilskud.

Det skal derfor undersøges, hvorvidt disse to former for persondatabehandling er at betragte som spejderforeningernes kerneaktivitet. Definitionen på en kerneaktivitet efter Forordningen skal ifølge Gruppens vejledning forstås som "*(...) de centrale aktiviteter, der er nødvendige for at opnå den dataansvarlige eller databehandlerens mål*".[182]

Som udgangspunkt må begge aktiviteter kategoriseres som kerneaktiviteter efter ovenstående fortolkning. Begge aktiviteter er nødvendige for, at spejderforeningerne kan udføre deres egentlige kerneaktivitet og dermed opnå deres mål. Spejderforeningerne ville ikke kunne udføre deres kerneaktiviteter, hvis ikke disse havde status som juridisk enhed og dermed selvstændige foreninger. Ligeledes søges der om kommunale tilskud, for at få de nødvendige midler til at udføre kerneaktiviteterne.

[179] Se https://www.kk.dk/sites/default/files/uploaded-files/ansoegningsskema_om_godkendelse_lokaler_og_tilskud.docx, (tilgået 13/05/2018).
[180] Se medlemsopgørelsen fra 2017 hos KFUM spejderne.
[181] *Det Danske Spejderkorps hjemmeside. (u.d.). Hentet fra https://dds.dk/: https://dds.dk/om-det-danske-spejderkorps,* (tilgået 03/05/2018).
[182] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev. 01 (Dansk version) s. 7.

Det er dog ens for begge situationer, at de ikke udføres som en del af kerneaktiviteten, men derimod udføres den som en forudsætning for, at spejderforeningernes kerneaktiviteter kan udføres. Persondatabehandling der udføres på dette grundlag, er at betragte som biaktiviteter (se side 44) og ikke kerneaktiviteter. Dermed er databehandlingen, der sker for at en forening kan have status som juridisk person og for at få kommunale tilskud, ikke at betragte som egentlige kerneaktiviteter efter Forordningens forstand.

Formålet med spejderforeningerne blev i indledningen til dette speciale fastslået, og ligeledes hvilke aktiviteter spejderforeningerne udfører for at opnå deres mål. Disse aktiviteter vil blive oplistet og sat op imod kerneaktivitetsbegrebet i nedenstående afsnit. Dermed vil det være muligt at fastslå, om persondatabehandling kan betragtes som spejderforeningernes kerneaktivitet. Såfremt dette ikke er tilfældet, vil spejderforeningerne ikke behandle persondata som deres kerneaktivitet, og vil ikke skulle udpege en DPO efter Forordningens art. 37, stk. 1, litra b).

2.6.2.2.3 Udførte aktiviteter i spejderforeningerne

Det blev konstateret tidligere i dette kapitel, at spejderforeningerne i dette speciale er at betragte som folkeoplysende foreninger efter folkeoplysningslovens § 4, stk. 1, nr. 2, da foreningernes udbudte aktiviteter lever op til kravene i denne lov.

Formålet med disse aktiviteter er efter folkeoplysningslovens § 14 "*(...) at fremme demokratiforståelse og aktivt medborgerskab og med udgangspunkt i aktiviteten og det forpligtende fællesskab at styrke folkeoplysningen. Sigtet er at styrke medlemmernes evne og lyst til at tage ansvar for eget liv og til at deltage aktivt og engageret i samfundslivet".*

Spejderforeningernes formål er at udvikle og oplære børn og unge i områder som bl.a. medansvar og demokratisk forståelse.[183] For at opnå disse mål udbyder foreningerne spejderaktiviteter som lejrture, frilufts- og færdighedsaktiviteter for også at styrke medlemmernes sammenhold. Dermed er det lejrturene, frilufts- og færdighedsaktiviteterne, der udgør spejderforeningerne kerneaktiviteter.

Med udgangspunkt i de ovenstående betragtninger skal der udledes, hvorvidt persondatabehandling kan betragtes som kerneaktiviteten i spejderforeningerne. Som nævnt udgør kerneaktiviteten efter Gruppens vejledning "*(...) de centrale aktiviteter, der er nødvendige for at opnå den dataansvarlige eller databehandlerens mål*".[184]

[183] Dette blev nævnt i indledningen til specialet.
[184] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 7.

Det blev udledt på side 43, at persondatabehandling er at betragte som den dataansvarliges kerneaktivitet i to situationer. Nemlig når;

1) det udbudte produkt eller tjenesteydelse består af databehandling, eller
2) databehandlingen er en uundgåelig del af kerneaktiviteten.

Der skal således ses på, om persondatabehandling er at betragte som enten spejderforeningernes *udbudte aktiviteter* eller som en *uundgåelig del* af disse.

I forbindelse med det første tilfælde kan det konkluderes, at persondatabehandling ikke udgør spejderforeningernes udbudte aktiviteter, da disse omfatter lejrturene, frilufts- og færdighedsaktiviteterne. Persondatabehandling kan således ikke udgøre disse ydelser efter Gruppens eller Forordningens forstand.

I det andet tilfælde skal der ses på, om persondatabehandling udgør en uundgåelig del af kerneaktiviteterne. Her kan der argumenteres for, at dette er tilfældet, idet spejderforeningerne må forventes at indsamle persondata om medlemmerne i forbindelse med udførelsen af disse aktiviteter. Dette kunne fx være i forhold til allergier overfor insektstik eller i forhold til mad og kontaktinfo på forældre ved nødstilfælde. Dette må være nødvendigt for, at kerneaktiviteterne kan udføres på et sikkert grundlag. Efter Gruppes vejledning skal persondatabehandling i dette tilfælde betragtes som en uundgåelig del af kerneaktiviteterne jf. hospitalseksemplet på side 43.[185]

Omvendt må der ud fra hospitalseksemplet forstås, at kerneaktiviteten skal være baseret på den behandlede persondata i en sådan grad, at udførslen af kerneaktiviteten varieres på baggrund af persondataen, og derfor er den uundgåelig.[186] Den individuelle sygepleje af et hospitals patienter er netop baseret på den enkelte patients persondata, og sygeplejen er derfor skræddersyet efter den enkelte patients persondata. Derfor er persondatabehandlingen uundgåelig på hospitaler.

Friluftsaktiviteter, lejrture og færdighedsaktiviteter kan ikke på samme måde betragtes som værende skræddersyede efter det enkelte spejdermedlems persondata. Selve udførelsen af friluftsaktiviteter eller lejrture vil i store træk forblive den samme på trods af den indsamlede persondata. Dermed vurderes det at udførslen af kerneaktiviteten ikke baseret på

[185] Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version), s. 7.
[186] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 563.

persondataen, der gør persondataen til en uundgåelig del af kerneaktiviteten efter Forordningens forstand.

Det må derfor konkluderes, at spejderforeningernes kerneaktiviteter ikke består af persondatabehandling. Da betingelserne i Forordningens art. 37, stk. 1, litra b) er kumulative, findes det ikke nødvendigt at analysere de resterende to betingelser om *regelmæssig og systematisk* overvågning, samt databehandling *i stort omfang*. Spejderforeningerne skal således ikke udpege en DPO efter Forordningens art. 37, stk. 1, litra b).

I de kommende afsnit vil der blive set på, om spejderforeningerne i stedet skal udpege en DPO efter Forordningens art. 37, stk. 1, litra c) eller Forordningens art. 37, stk. 4.

2.6.3 Forordningens art. 37, stk. 1, litra c)

2.6.3.1 Behandling af følsomme oplysninger eller oplysninger om strafbare forhold

Efter Forordningens art. 37, stk. 1, litra c) skal den dataansvarlige udpege en DPO når "*(...) den dataansvarliges eller databehandleres kerneaktiviteter, består af behandling i stort omfang af særlige kategorier af oplysninger jf. artikel 9, og personoplysninger vedrørende straffedomme og lovovertrædelser jf. artikel 10.*"

Ifølge Datatilsynets vejledning skal art. 37, stk. 1, litra c) opdeles i de næsten tre samme kumulative betingelser, som art. 37, stk. 1, litra b) - dog med en enkelt ændring.[187] De kumulative betingelser er således efter litra c):

1) *Behandlingen af persondata skal være kerneaktiviteten,*
2) *der skal behandles persondata i et stort omfang, og*
3) *behandlingen skal vedrøre følsomme oplysninger eller oplysninger om strafbare forhold*

Det er udledt i afsnittet om art. 37, stk. 1, litra b) på side 53, at spejderforeningernes kerneaktivitet ikke består af persondatabehandling, og de kumulative betingelser er således ikke opfyldt i hverken art. 37, stk. 1, litra b) eller litra c).

[187] Vejledning om databeskyttelsesrådgivere, December 2017, Det Danske Datatilsyn, s. 10.

2.6.4 Forordningens art. 37, stk. 4

2.6.4.1 Nationale love for udpegelsen af en DPO

Efter Forordningens art. 37, stk. 4 kan medlemsstaterne i deres nationale ret lave flere betingelser for, hvornår en dataansvarlig skal udpege en DPO. I Tyskland er denne mulighed blevet anvendt, og efter tysk ret skal der derfor også udpeges en DPO, såfremt den dataansvarlige har 10 eller flere ansatte, der arbejder med behandling af persondata.[188]

Betænkningen til Forordningen nævner ikke, om Folketinget i Danmark har besluttet at gøre brug af denne mulighed, men den fortæller, at muligheden er tilgængelig.[189] Der er udarbejdet to lovforslag til suppleringslove i forbindelse med gennemførelsen af Forordningen i dansk ret. DPO'en er nævnt i lovforslag - 2017/1 LSF 68 (databeskyttelsesloven). Det nævnes dog blot, at DPO'en er underlagt tavshedspligt, når denne modtager personoplysninger i forbindelse med udførelsen af sit job som DPO.[190] DPO'en efter Forordningen nævnes heller ikke i den anden suppleringslov.[191]

Det må ud fra dette antages, at spejderforeningerne ikke bliver forpligtet til at udpege en DPO efter nogen national lov, der er udstedt med hjemmel i Forordningens art. 37, stk. 4.

2.7 Diskussion

Spejderforeningerne, der blev undersøgt under den retsdogmatiske analyse, er ikke forpligtet til at udpege en DPO i Forordningens forstand. Folkeoplysningslovens § 4, stk. 1, nr. 2 og § 14 er dog bredde, og de åbner dermed op for mange muligheder for, hvornår en forenings formål gør, at den er kvalificeret som en folkeoplysende forening. Alene i Frederiksberg Kommune findes der over 100 forskellige folkeoplysende foreninger - alle med hvert deres formål inden for lovens rammer.[192] Foreningerne udbyder mange aktiviteter, der varierer fra alt mellem basketball- til spejderforeninger og teater- og musikforeninger. Ud fra den ovenstående retsdogmatiske analyse, må det forventes, at langt de fleste folkeoplysende foreninger efter lovens § 4, stk. 1, nr. 2 ligeledes ikke vil være forpligtet til at udpege en DPO efter Forordningens art. 37. Som det blev udledt med spejderforeningerne,

[188] https://www.hldataprotection.com/2017/08/articles/international-eu-privacy/germany-publishes-english-version-of-its-national-gdpr-implementation-act/ (tilgået d. 13/05/2018).
[189] Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565, s. 573.
[190] 2017/1 LSF 68, §24.
[191] 2017/1 LSF 69.
[192] *Frederiksberg kommunes hjemmeside*. (u.d.). Hentet fra https://www.frederiksberg.dk: https://www.frederiksberg.dk/borger/fritid-og-oplevelser/foreninger/foreninger-pa-frederiksberg (tilgået d. 01/05/2018).

vil persondataen i nogle af disse folkeoplysende foreninger spille en rolle, men ikke på et niveau der gør, at behandlingen betragtes som del af foreningernes kerneaktiviteter. Ligesom med spejderforeningerne er argumentet, at udførelsen af kerneaktiviteterne ikke er baseret på den behandlede persondata på et tilstrækkeligt niveau, der gør, at persondataen er en uundgåelig del af kerneaktiviteten i Forordningens forstand.

2.8 Delkonklusion

Delspørgsmål: Hvorvidt er folkeoplysende spejderforeninger forpligtede til at udpege en DPO efter Forordningens art. 37?

Det er i den juridiske analyse udledt, at spejderforeningerne er underlagt både Forordningens materielle og territoriale anvendelsesområde. Spejderforeningerne skal derfor overholde Forordningens regler i det fulde omfang, når denne træder i kraft d. 25. maj 2018. Spejderforeningerne er dog ikke forpligtet til at udpege en DPO efter nogen af bestemmelserne i Forordningens art. 37, da ingen af betingelser er opfyldt i deres fulde omfang. Ligeledes er der ingen af de potentielle nationale love, der er udarbejdet på baggrund af de åbne artikler i Forordningen, der forpligter spejderforeningerne til at udpege en DPO. Hvis foreningerne finder dette nødvendigt, kan de dog stadig udpege en DPO på frivillig basis.

Kapitel 3 - økonomisk analyse

3.1 Introduktion til det økonomiske kapitel

Kapitlet indledes med en økonomisk grundviden, der underbygger det resterende økonomiske kapitel. Dette bliver hovedsageligt gjort ved matematisk argumentationsanalyse, der vurderer, hvorfor persondata har værdi, og hvilken værdi denne data har. Herefter vurderes det økonomiske rationale, hvorfor EU har valgt at udarbejde en persondataforordning. Disse emner benyttes som et springbræt til at forstå grundlaget for specialets økonomiske kapitel. Herefter analyseres det negative *mikroøkonomiske udgangspunkt* ved implementeringen af Forordningen, mens næste del analyserer de *ønskelige effekter ved Forordningen*. Dette omhandler, hvorfor de negative konsekvenser reelt overgås af økonomisk positive faktorer. I afsnittet *DPO'en i økonomisk kontekst*, bliver det analyseret, hvorfor DPO'en er en spiller, der vil få organisationer til at overholde Forordningen bedst muligt. Herefter diskuteres, om det reelt er i borgernes interesse at få implementeret Forordningen. Denne del vurderer, under hvilke forudsætninger borgerne støtter op om deling af deres persondata. Til sidst bliver det hele konkluderet, hvor den økonomiske problemstilling besvares.

3.1.1 Dataens værdi for virksomheder

Stort set alle virksomheder der arbejder med indsamling og behandling af persondata, erkender, at de skal bruge den data, de har til rådighed så effektivt som muligt, hvis de skal kunne følge med den teknologiske udvikling. Det skyldes bl.a., at virksomheder mister kunder til konkurrenter, hvis det ikke lykkes at effektivisere, udvikle, forudsige og ramme borgeren direkte, og ved persondata kan dette opnås.

Et konkret bud på virksomheders nytte af hele en borgers dataprofil er vurderet til mellem 90 og 242 kr.[193] Dette var baseret på platforme som *Minecraft*, *Instagram* og *WhatsApp*. I den lavere ende er information om blot alder og køn blevet solgt på databørser ned til 0,0042 kr. (0,0007$) pr. bruger.[194]

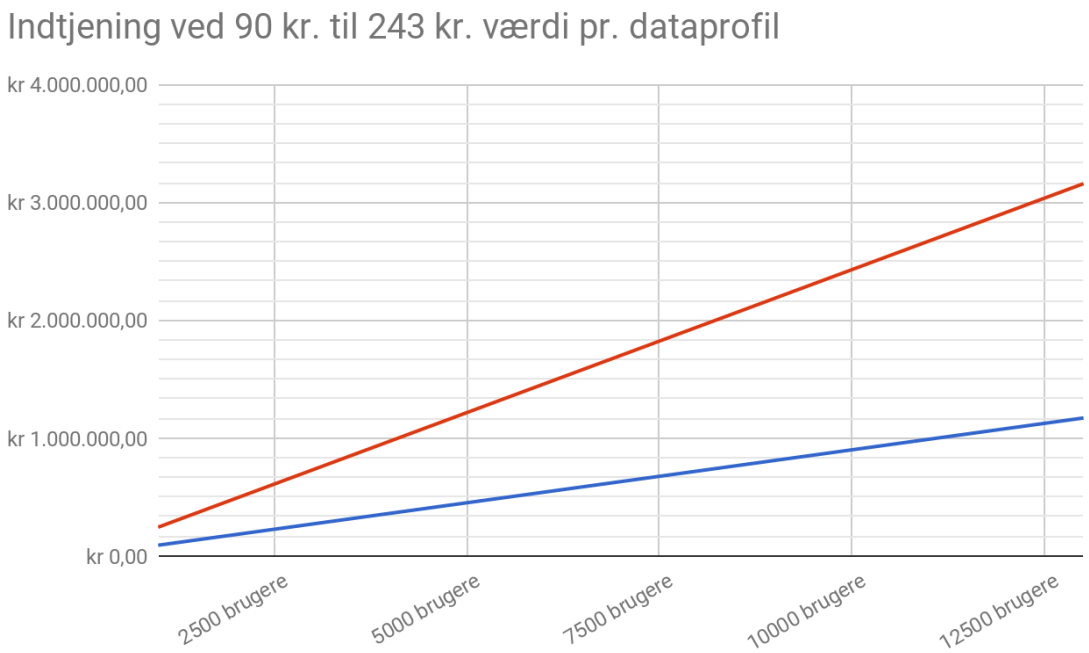
Ud fra en forventning om at tjene mellem 90 og 243 kr. pr. brugerprofil skal der være adgang og ejerskab over mellem 4.115 og 11.111 personlige dataprofiler, før udgiften er indhentet.

[193] Det er fx information som adresse, navn, e-mail, alder, køn, *likes*, billeder, venner, familie o.l., der blev vurderet til mellem 15$ og 40$.
[194] Kugler, L. (Februar 2018). The War Over the Value of Personal Data. *Communications of the ACM, 2* (61), s. 18.

Dette er, hvis det har kostet 1.000.000 kr.[195] at implementere Forordningen. Det er for overblikkets skyld tydeliggjort i nedenstående formler og graf.

$$Rød\ graf: 1.000.000\ kr./\ 90\ kr.pr.bruger\ \approx 11.111\ brugere$$

$$Blå\ graf: 1.000.000\ kr./\ 243\ kr.pr.bruger\ \approx 4.115\ brugere$$



196

Hvis indtjeningen er 0,0042 kr. pr. bruger, skal der være adgang til oplysninger fra *235.568.572 personer*[197], før udgiften på 1.000.000 kr. er tjent ind.

Det er tydeliggjort, at det ikke er den individuelle data, der har nogen værdi, men det er selve aggregeringen, der skaber værdien. Ovenstående lineære kurver er sandsynligvis i virkeligheden eksponentielt stigende. Der er derfor behov for store mængder persondata, før borgeres data kan benyttes i erhvervsøjemed.

Store platforme som *Facebook* og *Google* har hurtig og kontinuerligt adgang til flere zettabytes[198] persondata. Denne viden er andre virksomheder meget interesserede i at købe og benytte sig af. Derfor er persondataen en profitabel forretning for store digitale

[195] Beløbet 1.000.000 kr. er et tænkt eksempel, som fx indeholder udgifter til: forarbejde, kurser, advokater, DPO, ændring af interne processer, og varetagelse af datasubjekternes efterfølgende rettigheder.
[196] Graf tilegnet af forfatterne.
[197] 1.000.000 kr. / 0,00424504845 kr. pr. bruger ≈ 235.568.572 brugere.
[198] 1 zettabyte = 1.000 exabytes = 1.000.000 petabytes = 1.000.000.000 terabytes = 1.000.000.000.000 gigabytes.

tjenester[199], hvor persondata er uundgåeligt "*den nye olie*" i et øget digitalt marked. Dette skyldes, at de store internationale selskaber har stor viden om EU-borgerne, og derfor har de et højt niveau af kontrol og magt. I bund og grund kunne medlemsstaterne i EU allerede under Direktivet sanktionere selskaber og myndigheder, der udnytter eller misbruger borgernes persondata. Det er dog sket uligeligt mellem medlemsstaterne, og det er samtidigt ikke sket i særligt stort omfang. Dette ses fx ved, at den højeste bøde i Danmark for brud på persondataloven (under Direktivet) var 25.000 kr. Sanktionen blev givet i godtgørelse pga. videregivelse af persondata mellem to kommuner.[200] Rundt om i Europa har *UK Information Commissioner's Office* i Storbritannien i 2015 givet teleselskabet *TalkTalk* en bøde på 3,5 mio. kr.[201], og *Garante per la protezione dei dati personali* i Italien har givet fem selskaber sanktioner for i alt på 82 mio kr. i 2017.[202] Begge for brud på deres respektive persondatalove. Danmark har derfor tradition for at straffe brud på persondataloven mildere end andre medlemsstater.

Både Direktivet og Forordningen har til formål at øge innovationen og økonomien i EU ved at skabe øget tillid mellem borgeren og den dataansvarlige virksomhed eller myndighed. Derfor er der som udgangspunkt ikke store forskelle mellem Direktivet og Forordningen.[203]

---

[199] Afsnit er skrevet på baggrund af artiklerne:
- Kugler, L. (Februar 2018). The War Over the Value of Personal Data. *Communications of the ACM, 2* (61).
- Andrejevic, M. (Januar/Februar 2017). Personal Data: Blind Spot of the "Affective Law of Value"? *Information Society , 1* (31), s. 5-12.
- Flint, D. (Februar 2016). Computers and Internet What Is the Value of Personal Data? *Business Law Review , 1* (37), s. 38-39.

og websiderne:
- *Styrelsen for Dataforsyning og Effektiviseringens hjemmeside*. (u.d.). Hentet fra http://sdfe.dk: http://sdfe.dk/data-skaber-vaerdi/en-bedre-og-hurtigere-offentlig-sektor/
- *Energi-, Forsynings og klimaministeriets hjemmeside*. (21. Marts 2017). Hentet fra http://efkm.dk: http://efkm.dk/aktuelt/nyheder/nyheder-2017/marts-2017/frie-geodata-har-en-vaerdi-paa-3-5-mia-kr/
- Bækby, R. (2. Februar 2017). *Alexandra Instituttets hjemmeside*. Hentet fra https://www.alexandra.dk: https://www.alexandra.dk/dk/aktuelt/nyheder/2017/studie-hjaelper-danske-virksomheder-udnytte-data

alle websider tilgået 28/02/2018.

[200] Se U.2011.2343.H.

[201] *Information Commissioners office's website*. (5. Oktober 2016). Hentet fra https://ico.org.uk: https://ico.org.uk/action-weve-taken/enforcement/talktalk-telecom-group-plc-mpn/, (tilgået 21/04/2018). Citat: "*The attacker accessed the personal data of 156,959 customers including their **names**, **addresses**, **dates of birth**, **phone numbers** and **email addresses**. In 15,656 cases, the attacker also had access to **bank account details** and **sort codes**.*"

[202] Kroman Reuters: https://www.kromannreumert.com/Nyheder/2017/04/Stoerste-boede-nogensinde tilgået (13/05/2018).

[203] COMMISSION OF THE EUROPEAN COMMUNITIES COM(92) 422 final - SYN 287 Brussels, 15 October 1992, Amended proposal for a COUNCIL DIRECTIVE on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Tilgået ved http://aei.pitt.edu/10375/1/10375.pdf, s. 128.

I Danmark har det været ambivalent at give bøder til offentlige organer. Dette ses fx ved hospitaler, hvor en høj bøde for at bryde persondataloven blot vil nedsætte kvaliteten på stuegangene. Der var derfor tendens til, at virksomheder og myndigheder i Danmark ikke behandlede persondata seriøst under Direktivet.

Pga. en uforsvarlig omgang med persondata under Direktivet har borgerne i EU overordnet set mistet troen på, at virksomheder og myndigheder forsvarligt kan håndtere og anvende den data, som de opsamler.[204] Derfor er en af de største nye tiltag i Forordningen de store bødetakster[205], som skal sikre, at Forordningen reelt overholdes ligeligt af alle.

Umiddelbart kan store selskaber udnytte deres markedsmagt på monopollignende måder, som gør, at det er meget svært for små og mellemstore virksomheder at komme ind eller vækste på et marked. Dette scenarie kan analogt betragtes som *misbrug af dominerende stilling*, hvor *Google Inc*. blev idømt at betale 18 mia. kr. i sanktion i 2017 for søgeordsoptimering af egne produkter.[206] Bødeniveauet skyldes netop, at Google havde misbrugt sin position, og dermed havde de skævvredet markedet til egen fordel.

En neoøkonomisk *cost-benefit*-analyse[207] understøtter, at virksomheder og aktører handler efter, hvor der findes mest værdi. Dvs. at Google i denne sag havde vurderet, at misbruget gav en større total fordel, end hvad sanktionen for overtrædelsen ville føre til. Teoretisk burde Google have fået mere end 18 mia. kr. ud af at misbruge sin dominerende stilling, ellers ville misbruget ikke være sket.[208] Dette betyder, at:

$$Straffen\ for\ at\ blive\ dømt\ *\ sandsynligheden\ for\ at\ blive\ opdaget < fortjenesten\ ved\ at\ bryde\ lovgivningen$$

I relation til dette speciale kan der argumenteres for, at en lignende situation kan opstå med misbrug af persondata. Derfor vil virksomheder *ikke* misbruge borgeres data, hvis:

$$Straffen\ for\ at\ blive\ dømt\ *\ sandsynligheden\ for\ at\ blive\ opdaget > fortjenesten\ ved\ at\ bryde\ lovgivningen$$

[204] Clausen, N. J., Kronborg, A., & Mortensen, B. O. (2017). *Festskrift til Hans Viggo Godsk Pedersen* (1 udg.). Jurist- og Økonomforbundets Forlag, s. 598.
[205] Op til EUR 20.000.000 eller 4% af den årlige globale koncernomsætning, jf. art. 83 og 84 i Forordningen.
[206] *Europa Kommissionens hjemmeside*. (27. Juni 2017). Hentet fra https://ec.europa.eu: https://ec.europa.eu/denmark/news/google-160627_da (tilgået 28/02/2018).
[207] Viscusi, W. K., Harrington, J. E., & Vernon, J. M. (2005). Economics of Regulation and Antitrust (4. udg.). Mit Press Ltd., s. 30-31.
[208] *Google Inc*. havde et overskud på 662,24 mia. kr. i 2017, så det er ikke urealistisk, at misbruget af dominerende stilling var risikoen værd. Kilde: *Statista*. (u.d.). Hentet fra https://www.statista.com: https://www.statista.com/statistics/266206/googles-annual-global-revenue/ (tilgået 15/04/2018).

Overordnet set har der været tendens til, at store virksomheder og myndigheder vurderede sanktionen som førstnævnte ligning, hvorimod ønsket med Forordningen er, at spillerne forventer nederste ligning som værende en realitet. Se mere om dette på side 98 bøder.

3.1.2 EU's rolle ved håndhævelse af misbrug af persondata

EU-Kommissionen er anerkendt som den eneste instans, der globalt kan nedtrappe de dominerende virksomheders position.[209] Overordnet set beskrives, at de europæiske samfundsmodeller har dårlige tider, da USA, Rusland og Nordkorea styres af ledere, som hhv. betragtes som konservativ liberal og som diktatorer, og de går alle langt for at opretholde deres magt. Det amerikanske styre kontrolleres af ønsket om et frit *liberalt marked*, mens de østlige lande styres af ønsket om at give *staten* monopolistisk magt. Begge yderpunkter ender med at øge monopolismen, og dette minimerer den fuldkomne konkurrence, da scenarierne er politiske ideologier, som risikerer tab i markedet. Dette skyldes, at dødvægtstabet øges betydeligt, som det vises på side 73 i nærværende speciale og i følgende citat vedr. det frie liberale marked i USA:

> "*The rise and monopolistic behaviour of the giant American internet platform companies is contributing mightily to the US government's impotence. These companies have often played an innovative and liberating role. But as Facebook and Google have grown ever more powerful, they have become obstacles to innovation, and have caused a variety of problems of which we are only now beginning to become aware.*"[210].

Sidste del af citatet tydeliggøres navnlig i de verserende sager om *Cambridge Analyticas*[211] indflydelse på det amerikanske præsidentvalg i 2016[212] og Brexit i 2016[213], hvor millioner af Facebook-profiler blev udnyttet til at påvirke vælgerne.[214] På nuværende tidspunkt overholder Facebook ikke Forordningen[215], men på baggrund af høringen af Mark

[209] Soros, G. (15. Februar 2018). Only the EU can break Facebook and Google's dominance. *The Guardian* (tilgået 07/03/2018).
[210] Citat fra: Soros, G. (15. Februar 2018). Only the EU can break Facebook and Google's dominance. *The Guardian,* (tilgået 20/04/2018).
[211] Cadwalladr, C., & Graham-Harrison, E. (17. Marts 2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian* (tilgået 13/04/2018).
[212] Rosenberg, M., Confessore, N., & Cadwalladr, C. (17. Marts 2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times* (tilgået 13/04/2018).
[213] MacAskill, A. (21. Marts 2018). What are the links between Cambridge Analytica and a Brexit campaign group? *Reuters* (tilgået 13/04/2018).
[214] Cadwalladr, C., & Graham-Harrison, E. (17. Marts 2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian* (tilgået 13/04/2018).
[215] Ghosh, S. (11. April 2018). Mark Zuckerberg's personal notes hint that Facebook isn't ready for GDPR. *Business Insider Nordic* (tilgået 13/04/2018).

Zuckerberg d. 10.-11. april 2018 i Den Amerikanske Kongres virkede stifteren af Facebook positivt indstillet på at implementere Forordningens regler globalt, så den ikke kun omfatter europæere. Dette er et skridt mod at undgå udnyttelse af persondata, som det skete ved *Cambridge Analytica.*[216] I bund og grund er EU-Kommissionens opfattelse, at konsekvensen ved at udnytte persondata skader mere, end hvad værdien af at udnytte dataen tilfører. EU ønsker det bedste for innovationen og den teknologiske udvikling - og ikke nødvendigvis det bedste for de store virksomheder. Derfor går EU ind og rammer selve *overudnyttelsen* af data.

EU blevet den eneste instans, som reelt kan gå ind og gøre noget ved de dominerende spilleres udnyttelse af deres magt. George Soros[217] anerkender Europas forståelse af behovet for tillid mellem borger og virksomhed:

> *"The European Union, and particularly the Nordic countries, are much more farsighted than the US in their social policies. They protect the workers* [EU-borgere red.]*, not the jobs* [virksomhederne red.]*. (...) This gives workers in Nordic countries a greater sense of security and makes them more supportive of technological innovations than workers in the US."*

Derfor tilskyndes idéen om at give mindre magt til dominerende spillere, da det vil øge innovationen.

Andre artikler går endnu længere.[218] Der beskrives at Larry Page, medstifter af Google, reelt ikke er interesseret i penge, men at interessen består i at ændre ideologien om den europæiske samfundsmodel. Han er erklæret *libertarianer*, som ønsker totalt privatejede bystater, der ledes af frie markedskræfter uden nogen form for statslig indblanding. Kritikerne siger yderligere, at det ikke handler om at vinde markedsandele for *tech*-giganter som Facebook og Google, men derimod om at vinde hele markedet og *monopolets tronstol*, da dette kan ændre samfundsideologier. Forslaget om 3% skat på *tech*-giganters

[216] Jeong, S. (11. April 2018). Zuckerberg says Facebook will extend European data protections worldwide — kind of. *The Verg* (tilgået 13/04/2018).
Jaffe , J. (11. April 2018). How Facebook is responding to Europe's new GDPR privacy rules. *Cnet* (tilgået 13/04/2018).

[217] George Soros er bestyrelsesmedlem i *Soros Fund Management* og *Open Society Foundations*, som hhv. er et investeringsfirma og en NGO, som støtter lighed, uddannelse, helbred og selvstændige medier. Kilde: Harvey, Kerric (2013), *Encyclopedia of Social Media and Politics*, SAGE Publications, s. 919.

[218] Jensen, C. (25. Marts 2018). Hvor længe vil vi passivt se til, mens tech-giganter undergraver samfundet? *Politiken* (tilgået 10/04/2018).

omsætning[219] er pludselig en form for nødret for at forsvare den europæiske samfundsmodel, der har taget 100 år at bygge op.

3.1.2.1 Europa-Kommissionens erkendelse af dominerende spillere

Det skal understreges, at Europa-Kommissionen ikke har interesse i, at store selskaber som Facebook og Google lukker ned. Kommissionen er interesseret i at nedjustere deres potentielle overudnyttelse af persondata, da det påvirker negativt den samlede markedsøkonomi. Et eksempel på dette er fx Kommissionens anerkendelse af *Social Media Marketing.* EU har initieret flere webinarer, som sætter fokus på, hvordan store sociale medier kan benyttes bedst muligt for det indre europæiske marked.[220]

EU erkender, at de store *tech*-virksomheder er med til at skabe innovation, og de store udbydere af digitale platforme er ofte de førende aktører, når nytænkende systemer skal udvikles. Det er disse selskaber, der har arbejdskraften, kapaciteten, erfaringen og viden til at foretage store investeringer, som kommer små og mellemstore virksomheder til gode, og dette kommer også forbrugeren til gode i sidste ende. Når stor kapacitet og stor datamængde sættes sammen, opstår synergien ved at udvikleren, markedsspillere og slutbrugeren alle påvirkes positivt. Derfor er de store innovative selskaber med til at starte innovationsprocessen, som reelt er en spiral, der udvikler alle involverede parter.

3.2 Økonomisk udgangspunkt

3.2.1 Mikroøkonomisk forståelse af markedstilstanden

En mikroøkonomisk udvikling af markedet er vigtig at analysere, før yderligere økonomiske faktorer inkluderes. Der tages udgangspunkt i de største *tech*-giganter i EU, som har store mængder af personlig data, der understøtter deres forretning. Dette er fx multinationale selskaber som Google og Facebook. Disse spillere har de største markedsandele indenfor sociale medier og digitale søgninger, og dermed har de den største private markedsmagt over EU-borgernes persondata. Da selskaberne har stor markedsmagt, har de også mulighed for at kræve mere fra deres brugere, og dette øger deres samlede overskud. Virksomhederne bliver derfor betragtet som dominerende på markedet, som det ligeledes tydeliggøres i nedenstående statistik:

[219] Bloomberg. (17. Marts 2018). Tech Giants Set to Face 3% Tax on Revenue Under New EU Plan. *The Fortune* (tilgået 15/04/2018).
[220] *European Commission's website*. (16. Februar 2018). Hentet fra https://ec.europa.eu: https://ec.europa.eu/growth/sectors/tourism/business-portal/webinars/social-media-marketing-facebook_en (tilgået 07/03/2018).

Mellem 90-97 % af online søgninger foretages ved Google i Europa, og 75% af alle smartphones bliver styret af Googles Androit i Europa.[221] *I Europa logger 46,6% af alle EU-borgere ind på deres Facebook-profil hver dag.*[222] *Udover Google er Facebooks tætteste konkurrent Twitter, som har omkring 5% af markedet.*

3.2.2 Herfindahl–Hirschman Index - HHI

Både indenfor[223] og udenfor[224] EU er intensiteten af konkurrencen på et marked blevet anerkendt ved HHI-udregninger.[225] EU-Kommissionen anerkender og forklarer indekset ved følgende citat:

> "*For at måle koncentrationsgraden anvender Kommissionen ofte Herfindahl-Hirschman-indekset. HHI beregnes som summen af kvadraterne på alle virksomhedernes individuelle markedsandele*"[226].[227]

Det er vigtigt at understrege, at indekset er *suggestivt*. Dette betyder, at det ikke kun er resultatet af indekset, som beskriver markedskoncentrationen, det gør elementer som *adfærd* og *ydeevne* ligeledes.[228] Fx foreskriver HHI-indekset, at et marked med to lige store spillere udtrykkes i et HHI på 0,5. Dette betyder *høj konkurrence*, men i realiteten kan fem spillere med hver 20% af markedet være mindre konkurrencepræget end førstnævnte. På trods af HHI-indekset foreskriver det modsatte. Se HHI-tabellerne på senere i dette afsnit.

---

[221] Meyer, R. (15. April 2015). Europeans Use Google Way, Way More Than Americans Do. *The Atlantic* (tilgået 07/03/2018).
European Commission's website. (25. April 2013). Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_MEMO-13-383_da.htm, tilgået 07/03/2018.

[222] *Statista*. (u.d.). Hentet fra https://www.statista.com: https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/ (tilgået 07/03/2018).
360 mio. EU-borgere (ud af 822,710,362) tilgår Facebook dagligt.

[223] Den Europæiske Union, *Retningslinjer for vurdering af horisontale fusioner efter Rådets forordning om kontrol med fusioner og virksomhedsovertagelser*, Den Europæiske Union, Luxembourg, 2004.

[224] U.S. Department of Justice and Federal Trade Commission, *Horizontal Merger Guidelines*, U.S. Department of Justice and the Federal Trade Commission, Washington DC, 1997 [1992].

[225] Djolov, G. (2013). The Herfindahl-Hirschman Index as a decision guide to business concentration: A statistical exploration. *Journal of Economic and Social Measurement*, s. 201.

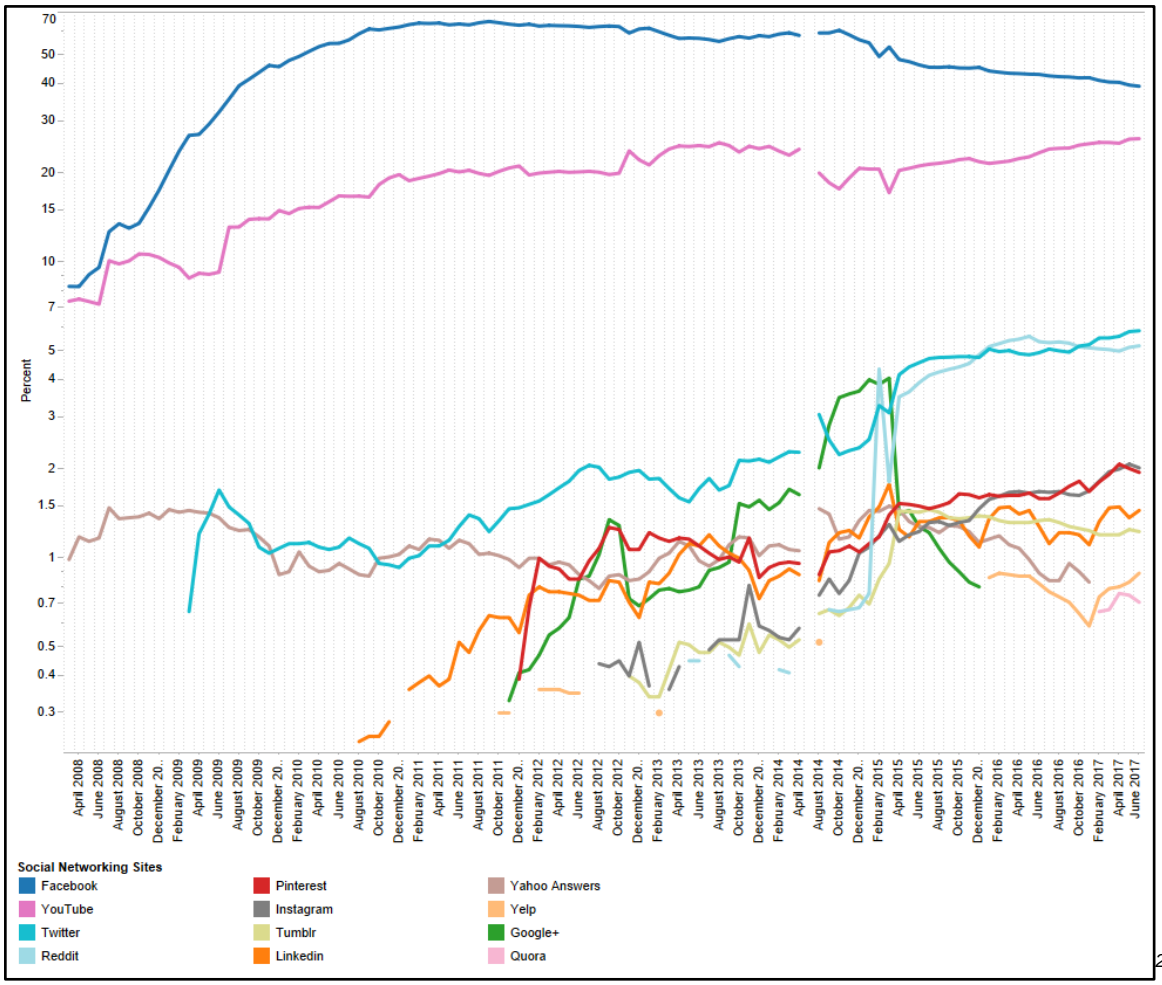
[226] Citat: Europa-Kommissionen. (2004). EUR-Lex Access to European Union law. Hentet fra http://eur-lex.europa.eu: http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:52004XC0205(02), (tilgået 13/03/2018).

[227] For eksempel har et marked bestående af fem virksomheder med markedsandele på henholdsvis 40%, 20%, 15%, 15% og 10% et HHI på 2.550 (402 + 202 + 152 + 152 + 102 = 2.550).
HHI varierer fra et tal, der nærmer sig nul (i tilfælde af et atomistisk marked) til 10.000 (når der er tale om et rent monopol).
Kilde: Retningslinjer for vurdering af horisontale fusioner efter Rådets forordning om kontrol med fusioner og virksomhedsovertagelser - *EU-Tidende nr. C 031 af 05/02/2004 s. 0005 - 0018* (tilgået 13/03/2018).

[228] Besonko, D., Dranove, D., Shanley, M., & Schaefer, S. (2013). *Economics of Strategy* (6. udg.). Singapore: John Wiley & Sons, s. 172.

HHI-indekset har fået yderligere kritik end førnævnte.[229] Indekset vil alligevel blive inddraget i specialet, da det giver en indikation af, hvordan markedet ændrer sig, når de spillere med størst markedsandel får det sværere, samtidigt med at mindre markedsspillere får det nemmere. Derudover (som tidligere nævnt) har europæiske og amerikanske myndigheder anerkendt indekset.

Nedenfor er indsat en grafisk oversigt, der viser sociale mediers markedsandelene på baggrund af antal besøgende - udtrykt i procent fra 2008 til 2017. Grafen vil være udgangspunkt for efterfølgende HHI-udregning.



230

[229] Mandelbrot, B. (1997). *Fractals and Scaling in Finance - Discontinuity, Concentration, Risk.* New york: Springer Publishing, s. 215-216.

[230] Kilde: Kallas, P. (4. December 2017). *Dreamgrow*. Hentet fra https://www.dreamgrow.com: https://www.dreamgrow.com/top-10-social-networking-sites-market-share-of-visits/ (tilgået 14/03/2018).

De største 8 markedsandele ud fra ovenstående graf:

Facebook	YouTube (Google)	Twitter	Reddit	Instagram	Pinterest	Linked In	Tumblr
40%	26%	5,8%	5%	2%	1,9%	1,5%	1,2%

Når konkurrencen udregnes ved HHI-indekset (på baggrund af ovenstående tal), bliver resultatet:

$$\underline{HHI =}$$
$$((0{,}4^2) + (0{,}26^2) + (0{,}058^2) + (0{,}05^2) + (0{,}02^2) +$$
$$(0{,}019^2) + (0{,}015^2) + (0{,}012^2) + (0{,}0\ldots^2)) * 10.000 \approx$$
$$\underline{2.345}$$

Ud fra nedenstående HHI-tabeller bliver koncentrationen på markedet for sociale medier beskrevet til at være dels *monopolistisk* og *oligopolistisk*, afhængigt af om HHI betragtes fra et økonomisk eller et juridisk synspunkt. Den præcise definition er mindre vigtig, da 2.345 under alle omstændigheder er langt fra fuldkommen konkurrence.

Tabel om økonomisk opfattelse af HHI-værdi og dennes betydning.

HHI-værdier i %-point	HHI-koncentration	Markedsstruktur	Priskonkurrence
$0{,}00 \leq HHI \leq 0{,}20$	*Lav koncentration*	*Perfekt konkurrence*	*Høj priskonkurrence*
$0{,}20 < HHI \leq 0{,}40$	Middel koncentration	Monopolistisk konkurrence	Let eller høj priskonkurrence - afhængigt af produktdifferentiation.
$0{,}40 < HHI \leq 0{,}70$	*Opløftet koncentration*	*Oligopol*	*Let eller høj priskonkurrence - afhængigt af rivalisering mellem konkurrenter.*
$0{,}70 < HHI \leq 1{,}00$	*Høj koncentration*	*Monopol*	*Let priskonkurrence - med mindre der er nye spiller på vej ind*

Tabel om juridisk opfattelse af HHI-værdi og dennes betydning.

HHI-værdier i %-point	HHI-koncentration	Markedsstruktur	Priskonkurrence
$0{,}00 \leq HHI \leq 0{,}10$	*Lav koncentration*	*Perfekt konkurrence*	*Høj priskonkurrence*
$0{,}10 < HHI \leq 0{,}18$	*Moderat koncentration*	*Monopolistisk konkurrence*	*Let eller høj priskonkurrence - afhængigt af produktdifferentiation.*
$0{,}18 < HHI \leq 1{,}00$	Høj koncentration	Oligopol på vej til monopol	Let eller høj priskonkurrence - afhængigt af rivalisering mellem konkurrenter eller nye spillere.

[231]

På baggrund af officielle HHI-tabeller er det vist, at markedet er oligopolistisk mod monopolistisk. For at komme sådanne markedskoncentrationer til livs, har Europa-Kommissionen skabt strategien for det indre marked[232], som består af en række initiativer. Persondataforordningen er et led i denne strategi, og ligeledes er ønsket om at få flere mindre spillere ind på markederne. Dette vil blive inddraget yderligere i afsnittet *Ønskelige effekter ved Forordningen* på side 79.

Grundet Europa-Kommissionens ønske om mere fuldkommen konkurrence vil der efterfølgende blive udregnet et tænkt eksempel, hvor 20 spillere hver har 5% af markedet. Dette gøres for at vise, hvordan HHI ændres, når markedet bliver mere konkurrencedygtigt:

$$\underline{HHI =}$$

$$\sum_{i=1}^{N} * s_i^2 = \sum_{i=1}^{20} * 0{,}05^2$$

$$\underline{500}$$

Med andre ord går HHI fra at være *monopolistisk* og *oligopolistisk* $(HHI \approx 2.345)$ til *perfekt konkurrence* $(HHI \approx 500)$, når magten deles mellem flere spillere. Det er yderst ønskeligt at

[231] Tabeller udformet af forfatterne på baggrund af:
Ertl, H., & McCarrell, H. (2002). *The State of Telecommunications Services.* Science, Innovation and Electronic Information, s. 9, og
Djolov, G. (2013). The Herfindahl-Hirschman Index as a decision guide to business concentration: A statistical exploration. *Journal of Economic and Social Measurement*, s. 202.
Nærværende speciales udregninger er multipliceret med 10.000, hvor der i tabellerne ikke er gjort dette.

[232] *Europa Kommissionens hjemmeside*. (u.d.). Hentet fra https://ec.europa.eu: https://ec.europa.eu/commission/priorities/digital-single-market_da (tilgået 07/04/2018).

opnå for EU, da det giver værdi og bedre konkurrence overordnet set. Dette uddybes yderligere i næste afsnit.

3.2.3 Statisk konkurrence

Jo flere spillere der er på et marked, jo mere fri konkurrence opstår der. Når ydelsen, der tilbydes på markedet, er den samme, og aktørene konkurrerer på prisen, er det *statisk konkurrence*, hvor "*(...) ingen kjøber eller selger kan stille avtalebetingelser uten å ta hensyn til at motparten kan velge en annen avtaaalepartner.*"[233]. Dette betyder, at den statiske konkurrence undergraver den aktør, der stiller højere krav til sine kunder. I forhold til specialet: *Hvis en udbyder af applikationer kræver mere ejerskab over brugernes data end andre*.[234]

Udbyderen undergraver sig selv ved at kræve mere data fra brugerne, da der er mange andre applikationsudbydere i *frikonkurrence-modellen*, som borgerne kan skifte over til. Det er markedsbetingelserne, der styrer markedet, modsat ved monopolisme hvor én aktør styrer markedet. Det er derfor mere økonomisk efficiens ved statisk konkurrence.

[235]

Forfatterne Eide og Stavang argumenterer modsætningsvist for, at markedet selv vil kunne gå imod monopolisten, når denne udnytter sin position tilstrækkeligt.[236] I forhold til dette speciale, går Forordningen reelt ind og påvirker markedet i den retning, som EU mener, det er mest gavnligt, da markedet ikke har tilpasset sig efficient på nuværende tidspunkt.

3.2.4 Konsekvens af markedsmagt

Specialet har indtil videre konkluderet, at oligopol og monopol påvirker økonomien negativt. Hvordan og hvad der sker for borgerne under disse tilstande, vil efterfølgende blive analyseret.

[233] Citat fra: Eide, E., & Stavang, E. (2008). *Rettsøkonomi* (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 63.
[234] Læseren bedes huske fra kapitel 1, at data er betalingsmidlet.
[235] Figuren er udarbejdet af forfatterne på baggrund af Eide, E., & Stavang, E. (2008). *Rettsøkonomi* (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 63-66.
[236] Eide, E., & Stavang, E. (2008). *Rettsøkonomi* (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG s. 64.

For at forstå prisreaktionen for dominerende spillere bestemmes det, hvad der mikroøkonomisk menes med *markedsmagt*. Det er elementerne 1) *antal købere*[237], 2) *antal udbydere*[238] og 3) *borgernes præferencegrad*[239], som afgør, hvilken magt spillerne har på markedet.

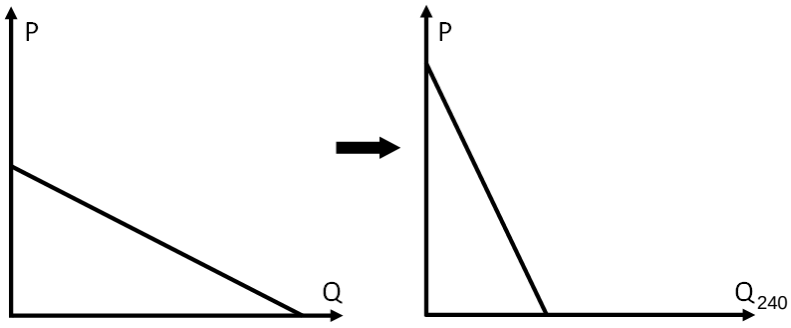
Det blev konstateret på side 65 og frem, at der på nuværende tidspunkt er meget få spillere på markedet for sociale medier og søgninger. Det betyder, at de(n) spiller(e) med magten styrer hvilke produkter og ydelser, der er tilgængeligt for forbrugerne på markedet. Dette er, hvad EU lægger op til at ændre. Nytten opstår ved, at borgerne har adgang til alternative ydelser og tjenester, som differentierer udbyderne fra hinanden. Dette øger dels konkurrencen, og det minimerer ligeledes risikoen for, at de største spillere kan udnytte deres magt.

3.2.4.1 Lerner-indekset

Mikroøkonomisk set betyder ovenstående, at de store spillere har markedsmagt til at hæve betalingskravet, og dette skaber mere egenværdi for selskabet end for borgerne. Borgerne falder ikke fra ved prisstigninger, grundet der ikke er nogle alternativer. Markedet beskrives nedenfor algebraisk og grafisk:

Nedenstående formler og grafer viser høj konkurrence på venstre side grundet fx mange spillere og alternativer, hvorimod højre side viser et marked få spillere og mindre omfang af alternativer:

$\Delta P < \Delta Q \quad \Rightarrow \quad \Delta P > \Delta Q$, hvor Δ er ændringen



[237] Der forudsættes, at der er tilstrækkelig med købere, og derfor vi dette punkt ikke blive inddraget i speciale.
[238] Som begrebet fuldkommen konkurrence antyder, jo færre udbydere, der er på markedet, jo mindre konkurrence er der. Dette vises i dette afsnit.
[239] Hvis udbydernes udbud minder om hinanden, opstår der ligeledes mere konkurrence på markedet for ydelsen/produktet. Se mere om dette i afsnittet om dynamisk konkurrence på side X.
[240] Figurer er udarbejdet af forfatterne. P = pris og Q = mængde.

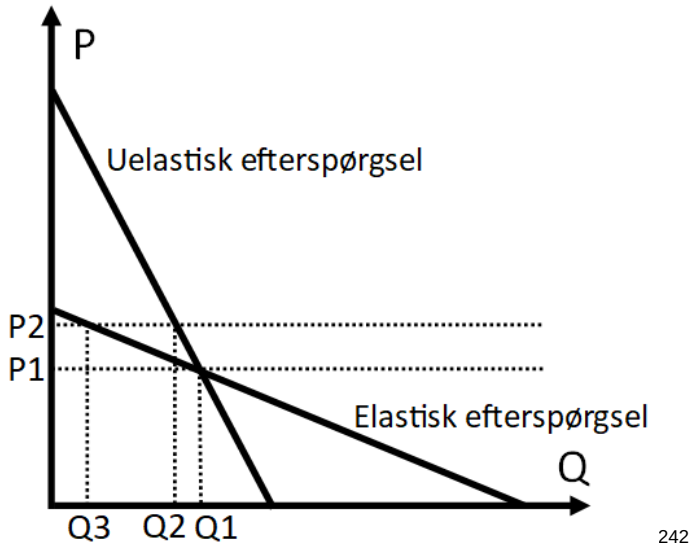
Markedsmagten måles ved Lerner-indekset (*The Lerner Index*).[241] Beskrevet ved Lerner betyder ovenstående, at priselasticiteten som udgangspunkt er mellem -1 og 0 (uelastisk), når spillerne i oligopolet kan optimere ved at kræve mere af borgerne for ydelserne. Med dette menes, at spillerne kan hæve prisen med 1%, hvor afsætningen derefter falder med mindre end 1%, og derfor skaber prishævningen værdi for virksomheden ($\Delta P > \Delta Q$).

Lerner (L) udregnes på følgende måde i nærværende speciale:

$$L = \frac{-1}{E_d}, \text{ hvor } E_d \text{ er hældningen i virksomhedernes efterspørgselskurve.}$$

Når Lerner går mod 0, skyldes det, at E_d bliver større. En prisændring medfører derfor en større ændring i, hvor meget borgerne vil handle:

$$\Delta P < \Delta Q \quad \Rightarrow \quad mere\ fuldkommen\ konkurrence\ i\ punkt\ (P1, Q1): uelastiskt$$
$$\Delta P > \Delta Q \quad \Rightarrow \quad mere\ monopolistisk\ tilstand\ i\ punkt\ (P1, Q1): elastiskt$$



[242]

Jo fladere efterspørgselskurven er, jo mere vil borgerne være tilbøjelige til at skifte ydelse/produkt, hvis prisen stiger (uelastisk). Dette ses ved:

$$Når\ P1 \rightarrow P2, går\ Q1 \rightarrow Q3, og\ \Delta P < \Delta Q\ , og\ dette\ giver\ tab\ for\ virksomheden.$$

Modsat vis jo stejlere efterspørgselskurven er, jo mindre kan/vil borgerne skifte ydelse/produkt, hvis der sker prisstigninger (elastisk). Dette ses ved:

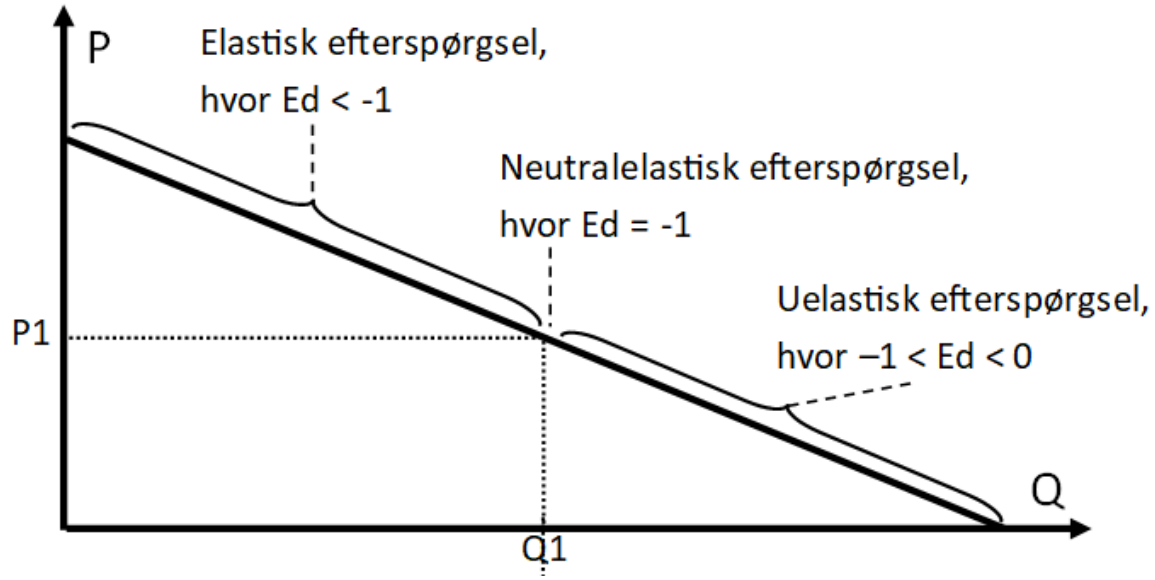
$$Når\ P1 \rightarrow P2, går\ Q1 \rightarrow Q2, og\ \Delta P > \Delta Q\ , og\ dette\ giver\ gevinst\ for\ virksomheden.$$

[241] Cabral, L. M. (2000). *Introduction to Industrial Organization.* MIT Press, s. 154.
[242] Figuren er udarbejdet af forfatterne. P = pris og Q = mængde.

I relation til strategien for det indre marked vil et ønsket marked med mere fuldkommen konkurrence blive beskrevet ved et lavt Lerner og elastisk efterspørgsel ved situationen:

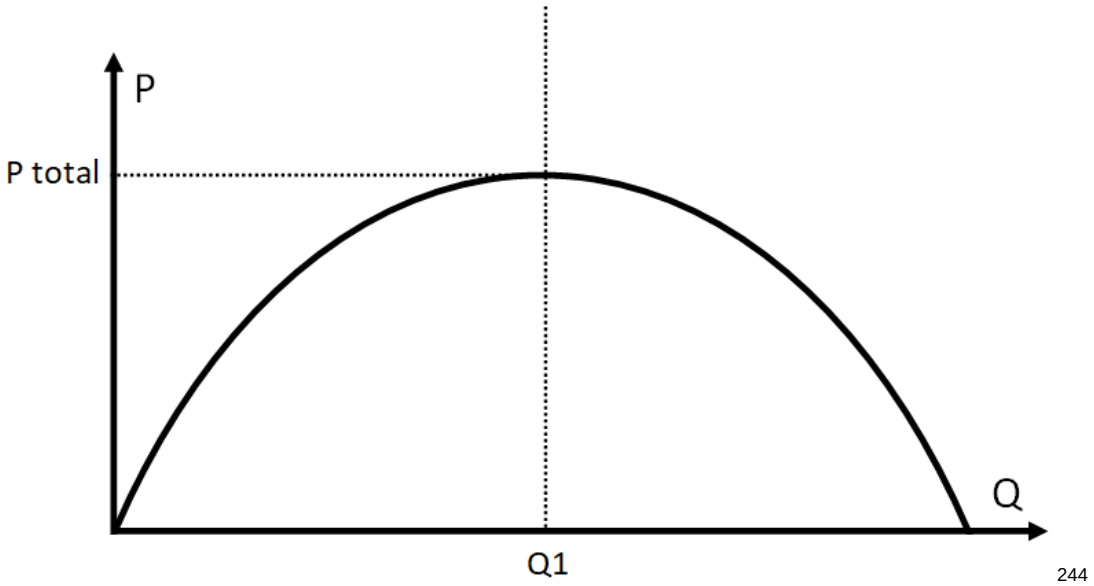
$\Delta P < \Delta Q$.

Nedenfor vises elasticiteterne grafisk:



[243]

I punktet hvor $E_d = -1$, opstår nytteoptimering for de markedsspillere, som har høj markedsmagt (oligopolistisk/monopolistisk), da det er her, omsætningen er størst. Dette vises nedenfor:



[244]

[243] Figur udarbejdet af forfatterne.
[244] Figur udarbejdet af forfatterne.

Punktet $(Q1, P\ total)$ er hvor virksomheden prisoptimerer (og ikke borgeren), da $Q * P$ maksimeres. Algebraisk udtrykkes dette ved funktionen for Q, som efterfølgende differentieres og sættes lig med 0:

$$F(Q) = -Q^2 + a * Q$$

$$F'(Q) = -2Q + a \rightarrow -2Q + a = 0 \rightarrow a = \frac{Q}{2} \rightarrow Q = \frac{a}{2}$$

Ovenstående algebraiske udregning vil finde sted med rigtige talværdier på side 76 og frem.

I punktet $(Q1, P\ total)$ sker der ligeledes dødvægtstab i samfundet, og det er grunden til, at monopolisme typisk påvirker et marked negativt. Dette vises i næste afsnit.

3.2.4.2 Dødvægtstab - Dead Weight Loss

Dødvægtstabet (DWL) opstår, når monopolister overudnytter et marked. Hvis der var fuldkommen konkurrence, ville $DWL = 0$ - svarende til (P3,Q3) på nedenstående graf.

Når markedet udnyttes mere (prisen stiger til P2), er $DWL = arealet\ F$ - svarende til ligevægt i (P2,Q2).

Når markedet udnyttes meget (prisen stiger til P3), er $DWL = arealet\ C + E + F$ - svarende til ligevægt i (P1,Q1).

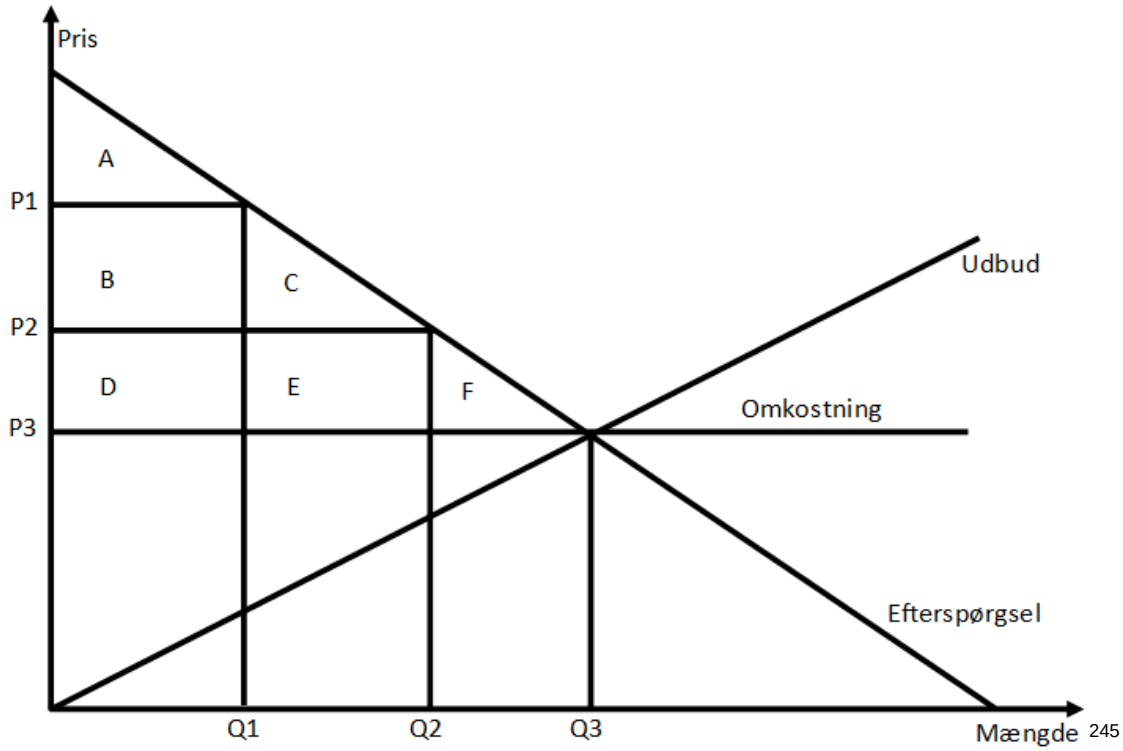
Modsat går forbrugernytten (*Consumer Surplus* - CS) fra arealet:

$A \rightarrow (A + B + C) \rightarrow (A + B + C + D + E + F)$,

når prisen falder fra:

$P1 \rightarrow P2 \rightarrow P3$.

Dette vises grafisk nedenfor:



[245]

Når prisen er P3, er CS størst muligt ($A + B + C + D + E + F$), da dette er laveste pris, som udbyderen kan tilbyde borgerne, mens den stadig kan drive forretning. Dette minimerer DWL (0). Derfor er dette scenarie ønskeligt for det totale marked (*Total Surplus* - TS).

For at relatere ovenstående teori til virkeligheden vil spillernes prisreaktioner før og under Forordningen blive analyseret i efterfølgende afsnit.

3.2.5 Spilleres prisreaktion på monopollignende marked

Det er ovenfor blevet bestemt ved HHI-indekset, at markedet for sociale medier på nuværende tidspunkt er domineret af Facebook (og til dels Google ved *Youtube.com*). Dertil er det analyseret ved Lerner, hvordan efterspørgselskurven ser ud, når dominerende spillere styrer markedet, og hvilken konsekvens dette har for borgerne.

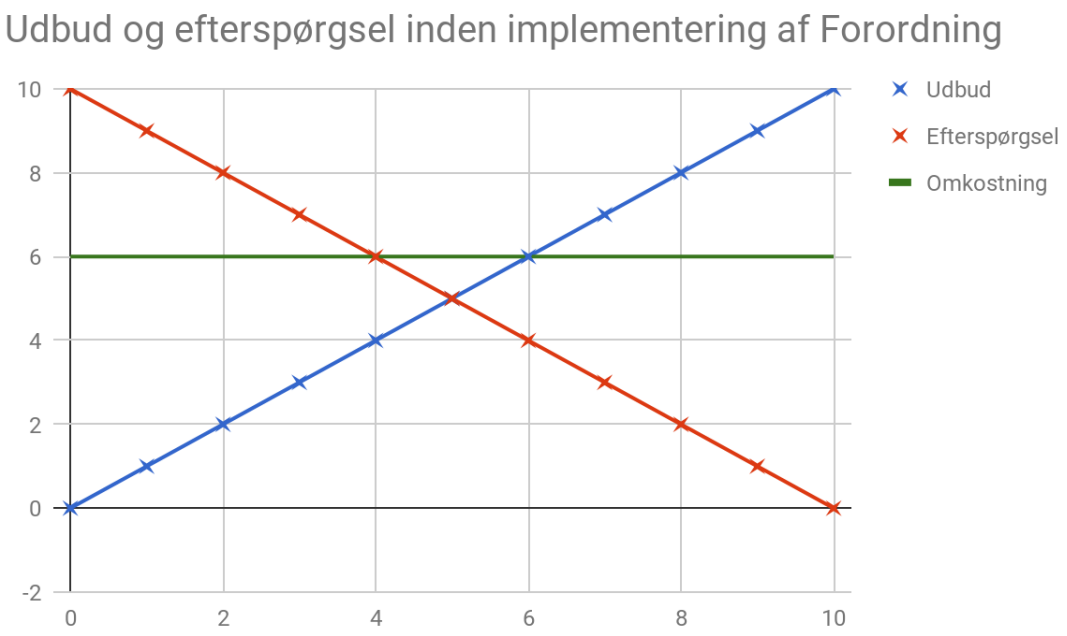
Nedenfor vil der blive vist, hvordan dominerende spillere på et marked reagerer, når de ved lovgivning påkræves at afholde yderligere omkostninger.[246] Udover selve udgiften for

[245] Graf udarbejdet af forfatterne.
[246] Som eksempel på de øgede omkostninger er de forventede 75.000 nye DPO-stillinger, som der globalt efterspørges frem mod 2019. Hvis disse skal have en "advokatløn", skal der globalt udbetales op mod 5 mia. dkk om måneden til de 75.000 nyansatte DPO'er. Kilde:
Study: 75,000 Data Protection Officers Needed by 2019, Information Management Journal. Jan/Feb 2017, Vol. 51 Issue 1, s. 6.

implementering af Forordningen[247] forventes det også, at de efterfølgende afledte effekter vil nedsætte de dominerende selskabers omsætning, men dette vil ikke blive taget med i afsnittet grundet specialets omfang.[248]

Antageligvis er den ideelle markedsligevægt placeret i det punkt, hvor udbuddet og efterspørgslen er lig hinanden. I dette punkt opstår der mindst muligt tab, da flest mulige borgere køber en given ydelse/vare hos flest mulige virksomheder.

Når omkostningerne for at drive en forretning antages at være højere end ligevægten ((5,5) i nedenstående graf), skubbes ligevægten længere op af efterspørgselskurven, da prisen for udbuddet stiger. Hvis omkostningerne antages at være 6, ender ligevægten nu i (6,4) på grafen. Den nye ligevægt repræsenterer en ny og mere realistisk ligevægt på markedet, da virksomheder har omkostninger ved at drive forretning. X-aksen er *antal enheder*, og y-aksen er *prisen* (persondataen).



Beregningen er sket på baggrund af en månedsløn på 75.000 dkk: 75.000 dkk * 75.000 DPO'er = 5.628.000.000 kr.

[247] Google har været nødt til at oprette en Forordningshjemmeside (https://privacy.google.com/businesses/) og forholde sig til cloud services, Gmail og Search, reklamer, og målingservices, som DoubleClick, AdSense og AdWords, som der opbevares på Googles servere. Kilde: Vijayan, J. (10. August 2017). Google launches new website to help explain its gdpr controls. *Eweek* (tilgået 07/03/2018).

[248] Deutche Bank forventer, at Googles omsætningen falder med 2% som følge af Forordningen. Kilde: Edwards, J. (31. Januar 2018). GDPR could wipe 2% from Google's revenues, according to Deutsche Bank. *Business Insider Nordic* (tilgået 07/03/2018).

Uden omkostninger på 6 er ligevægten i (5,5), hvor udbud og efterspørgsel rammer hinanden, og den forventede samfundsnytte $(5 * 5 =)$*25. Ved en omkostning og prissætning til 6 er ligevægten i* $(6 * 4 =)$*24.*

Det forventes, at virksomhederne prisfastsætter til 8, da deres forhold mellem salg og pris er optimeret i dette punkt. I dette scenarie vil der kun blive solgt 2 enheder til en pris af 8.

Algebraisk ser det således ud, hvor Q er mængde:

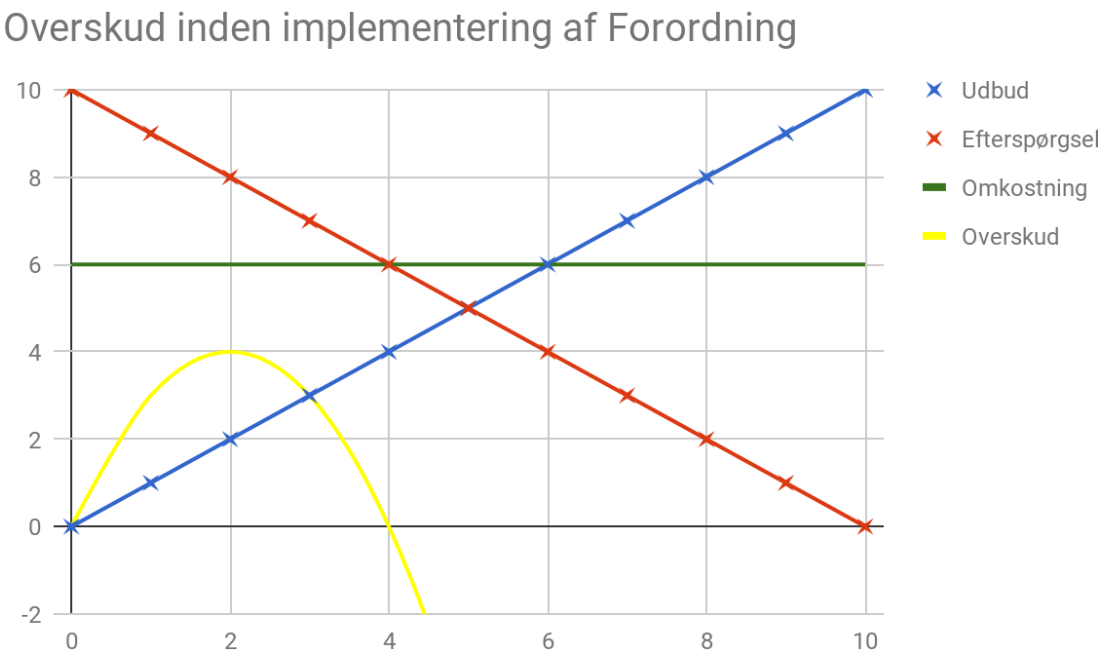
$$F(Q) = -Q^2 + 4 * Q$$

$$F'(Q) = -2Q + 4$$

$$\rightarrow -2Q + 4 = 0 \rightarrow 4 = \frac{Q}{2} \rightarrow$$

$$\underline{Q = 4/2 = 2}$$

$Q = 2$ betyder, at spilleren med høj markedsmagt har maksimeret profitten, når der sælges 2 enheder til en pris på 8[249]. Se ovenstående tekst og algebraiske udregning visuelt i nedenstående graf - se toppunktet på linjen "overskud":



Det antages herefter, at omkostningerne stiger for virksomheden grundet implementeringen af Forordningen. Monopolisten vil prisfastsætte højere, da dette maksimerer overskuddet. Hvis implementeringen af Forordningen tvinger virksomhedens omkostning op til 7, vil prisen

[249] Efterspørgslen som funktion er defineret som F(Q) = 10 - P, som viser: F(2) = 10 - P, hvor P = 8. Derfor er makspunktet (2,8).

på et produkt eller ydelse ligeledes stige, og dette minimerer antallet af borgere, der vil erhverve ydelsen. Det er visualiseret i grafen nedenfor, at overskuddet bliver mindre for både virksomheden og forbrugerne. Prissætningen vil i dette tilfælde være på 8,5, da der her opnås det maksimale overskud på 2,25 for virksomhederne, og borgerne vil købe 1,5 enheder i denne markedstilstand.

Algebraisk ser det således ud, hvor Q er mængde:

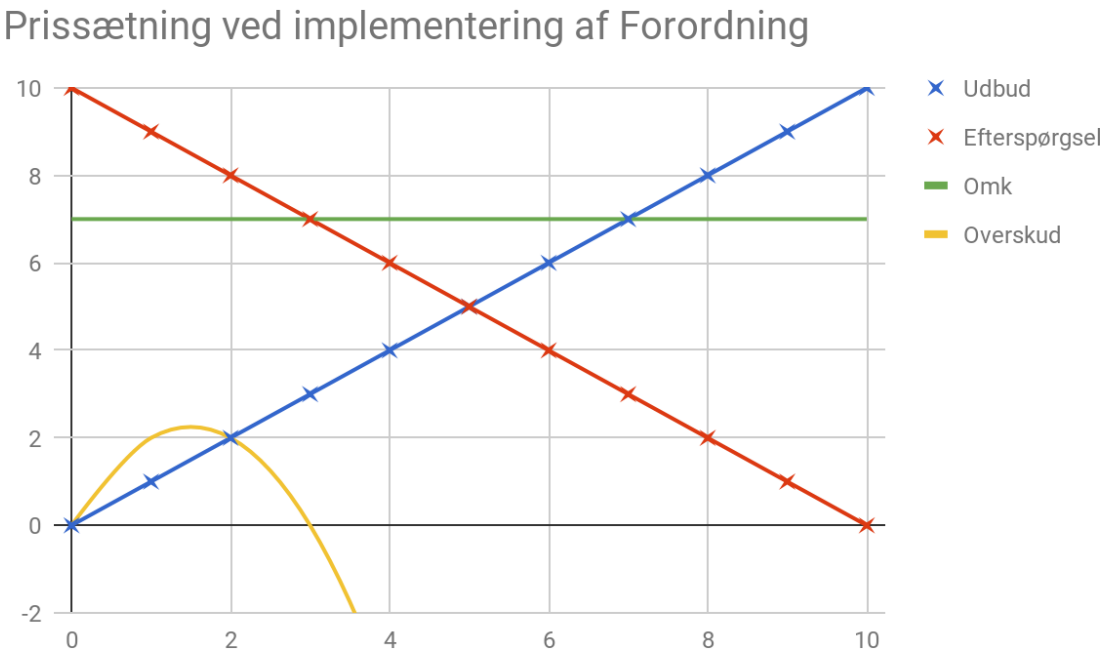
$$F(Q) = -Q^2 + 3 * Q$$

$$F'(Q) = -2Q + 3$$

$$\rightarrow -2Q + 3 = 0 \rightarrow 3 = \frac{Q}{2} \rightarrow$$

$$\underline{Q = 3/2 = 1{,}5}$$

$Q = 1{,}5$ betyder, at spilleren med høj markedsmagt har maksimeret profitten, når der sælges 1,5 enheder til en pris på 8,5[250]. Se ovenstående tekst og algebraiske udregning visuelt i nedenstående graf:



Det kan dermed konkluderes, at når omkostningerne stiger for en monopolist, stiger priserne i markedet og efterspørgslen falder:

[250] Efterspørgslen som funktion er defineret som F(Q) = 10 - P, som viser: F(1,5) = 10 - P, hvor P = 8,5. Derfor er makspunktet (1,5 ; 8,5).

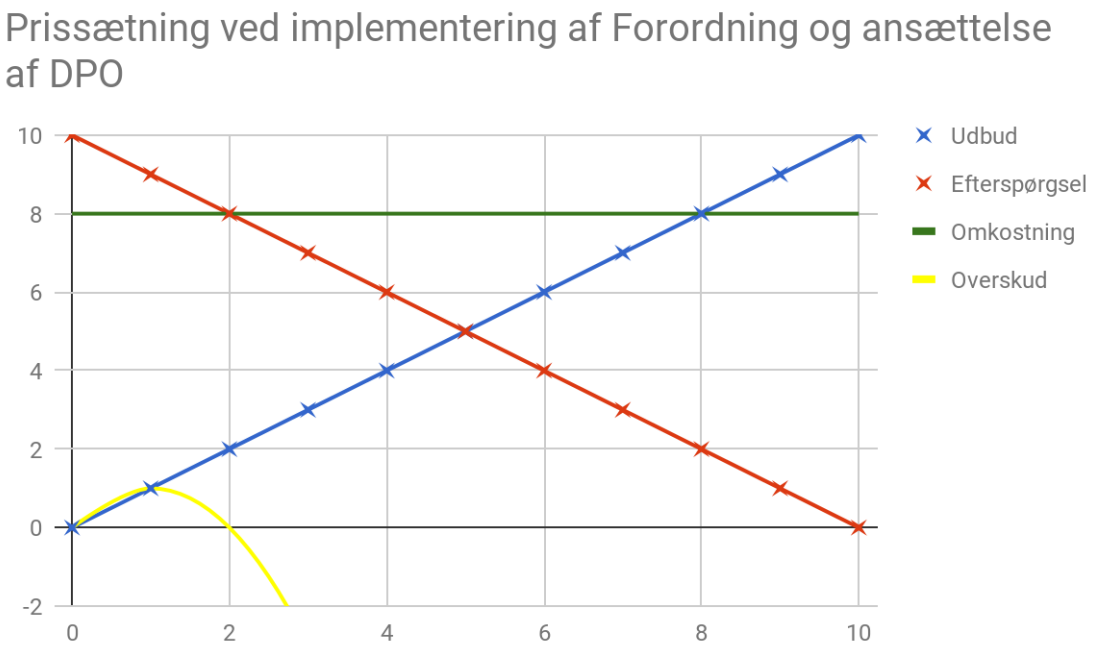
$$Omkostning \uparrow \Rightarrow \ prissætning \uparrow \Rightarrow \ efterspørgslen \downarrow \ \Rightarrow \ \ totalt\ salg \downarrow$$

Vist ved benyttede værdier:

$$\mathbf{6} \rightarrow \mathbf{7} \ \ \Rightarrow \ \ \mathbf{8} \rightarrow \mathbf{8,5} \ \ \Rightarrow \ \ \mathbf{2} \rightarrow \mathbf{1,5} \ \ \Rightarrow \ \ (2 * 8 =)\mathbf{16} \rightarrow (1{,}5 * 8{,}5 =)\mathbf{12,75}$$

Det er blevet vist algebraisk og grafisk, at købelysten bliver mindre for forbrugeren, da prisstigningen påvirker nogle forbrugere til ikke at købe ydelsen alligevel.

Når omkostningerne stiger, bliver forbrugernes nytte minimeret. Der kan ligeledes forventes, at denne tendens fortsætter, hvis yderligere omkostninger ved implementeringen af Forordningen fortsætter. Dette kan ske ved, at der ansættes en DPO i virksomheden. Det er vist grafisk nedenfor, når omkostningerne antages at stige til 8.



Hermed ender der med at blive solgt 1 enhed for prisen 9.

Det konkluderes, at de umiddelbare udgifter ved at implementere Forordningen betragtes som væsentlige, og udviklingen afskærer potentielle forbrugere fra muligheden for at købe den givne ydelse. Samtidigt giver det et mindre overskud til virksomheden, som heriblandt ikke får samme midler til at innovere for.

I næste afsnit vil det blive analyseret, hvorfor der er behov for en Forordning, når det netop er bevist, at implementeringen får en negativ indflydelse på den europæiske økonomi.

3.3 Ønskelige effekter ved Forordningen

Dette speciale har indtil nu kun analyseret de negative økonomiske konsekvenser, ved at Forordningen implementeres. Det analyseres i dette afsnit, hvordan Forordningen alligevel kan være økonomisk forsvarlig.

3.3.1 Opvejning af forbrugernes nyttetab

Som det vil blive analyseret i afsnittet 3.3.4 Efficiensteori - Pareto og Kaldor-Hicks, implementerer EU forordninger på baggrund af et ønske om nytte-forbedringer. Under denne forudsætning vil nærværende speciale analysere, om denne umiddelbare tabte nytte for borgerne ved prisstigninger kan blive opvejet af andre positive effekter. Først oplistes argumenter for og imod implementeringen af Forordningen:

	For implementering	**Imod implementering**
Forbrugerens synspunkt	- Øget datasikkerhed - Mere gennemsigtighed - Flere rettigheder som borger - Mere tillid til selskaber, som tilmed ansætter en DPO	- Højere priser - Virksomheder risikere store bøder, og regningen kan ende med at gå videre til forbrugeren
Samfundets synspunkt	- Ligestilling mellem store selskaber, som nemmere dominerer mindre virksomheder - Øget kontrol af virksomheder	- Mere bureaukrati - Virksomheder risikerer store bøder, hvor risikoen for konkurs øges

3.3.2 Det Digitale Indre Marked

Grundet de øgede omkostninger vil virksomhederne som udgangspunkt videreføre udgiften til forbrugerne.[251] Derfor må det umiddelbart ikke være i borgerens interesse, at Forordningen implementeres. Der må derfor antageligvis blive skabt positive effekter, før det økonomisk kan betale sig for EU at implementere Forordningen.

EU har anerkendt, at der ligger flere betydelige hindringer i vejen, før det fremtidige digitale marked kan blomstre optimalt. Overordnet set beskriver følgende citat, hvordan EU vil optimere den europæiske økonomi:

> *"Internettet og de digitale teknologier forandrer verden. Men de hindringer, der ligger i vejen for onlinehandel, betyder, at forbrugerne går glip af muligheden for at købe varer og tjenesteydelser, at internetfirmaer og nystartede virksomheder har begrænset*

[251] Dette blev vist i afsnittet *Økonomisk udgangspunkt* på side 64.

> *aktionsradius, og at erhvervslivet og de offentlige myndigheder ikke kan drage fuld nytte af de digitale værktøjer. Det er på tide (...), at EU's indre marked bliver tilpasset de digitale muligheder, og det vil sige, at vi skal fjerne lovgivningsmæssige barrierer og omstille 28 nationale markeder til ét enkelt. Det vil kunne bidrage med 415 mia. euro om året til vores økonomi og skabe hundredtusindvis af nye job."*[252]

Derudover nævner Dansk Industri, at "*[f]uldbyrdelse af det digitale indre marked kan øge væksten i EU med €340 milliarder og skabe 3,8 millioner jobs*".[253]

Ovenstående positive effekter skal ses i samspil med de mange negative lækager af persondata, som både er sket nationalt (Rigspolitiet i 2012, CPR-kontoret i 2014, Statens Serum Institut i 2015 og Digital Pladsanvisning i 2017)[254] - men også internationalt ved fx. Snowden-affæren i 2013, hvor der blev lækket mange tusinde top fortrolige og personlige dokumenter. Antonio Tajani, formand for Europa-Parlamentet, udtrykker, at "*(...) påstandene om misbrug af Facebook-brugerdata er en uacceptabel krænkelse af vores borgeres privatlivsrettigheder*".[255] Ovenstående påstande underbygges ved Facebooks faldende aktiekurs under *Cambridge Analytica*-affæren, som reelt afspejler borgernes mistillid og tiltro.[256] Aktiekursen gik fra 185,02 $ d. 16. marts 2018 til 162,8 $ d. 20. marts 2018, hvilket svarer til 60 mia. dollars (365 mia. kroner) på de to dage. Mistilliden understreger behovet for Forordningen, da den skal (gen)etablere tilliden mellem borgerne og virksomhederne. Under høringen af Mark Zuckerberg d. 10.-11. april 2018 i Den Amerikanske Kongres steg aktiekursen steg igen rundt regnet 4,5%, og dette viser ligeledes en forventning om tillid til Facebook.

Allerede i 2011 offentliggjorde EU en publikation, omhandlende hvorfor der var behov for en databeskyttelsesreform. Opsummeret var argumenterne, at;

- lidt over en fjerdedel af brugerne af sociale netværk (26%) og endnu færre, der køber varer og tjenester online (18%), føler, at de har fuld kontrol over deres personoplysninger,

[252] Citat: Europa Kommissionens hjemmeside. (u.d.). Hentet fra https://ec.europa.eu: https://ec.europa.eu/commission/priorities/digital-single-market_da (tilgået 28/02/2018).
[253] Dansk Industri. (u.d.). Dansk Industris hjemmeside. Hentet fra https://digital.di.dk: https://digital.di.dk/SiteCollectionDocuments/Publikationer/Faktaark%20om%20strategi%20for%20EUs%20digitale%20indre%20marked.pdf, s. 1, (tilgået 15/04/2018).
[254] Politiken, Jakob Sorgenfri Kjær, *I dag slipper myndigheder med kritik*, fredag d. 13. okt. 2017, s. 4.
[255] Thomsen, P. B. (19. Marts 2018). *Danmarks Radios hjemmeside*. Hentet fra https://www.dr.dk: *https://www.dr.dk/nyheder/udland/eu-fordoemmer-paastaaet-tyveri-af-facebook-brugerdata* (tilgået 21/03/2018).
[256] Kilde: *Yahoo Finance*. (u.d.). Hentet fra https://finance.yahoo.com: https://finance.yahoo.com/quote/FB/?guccounter=1 (tilgået 21/03/2018).

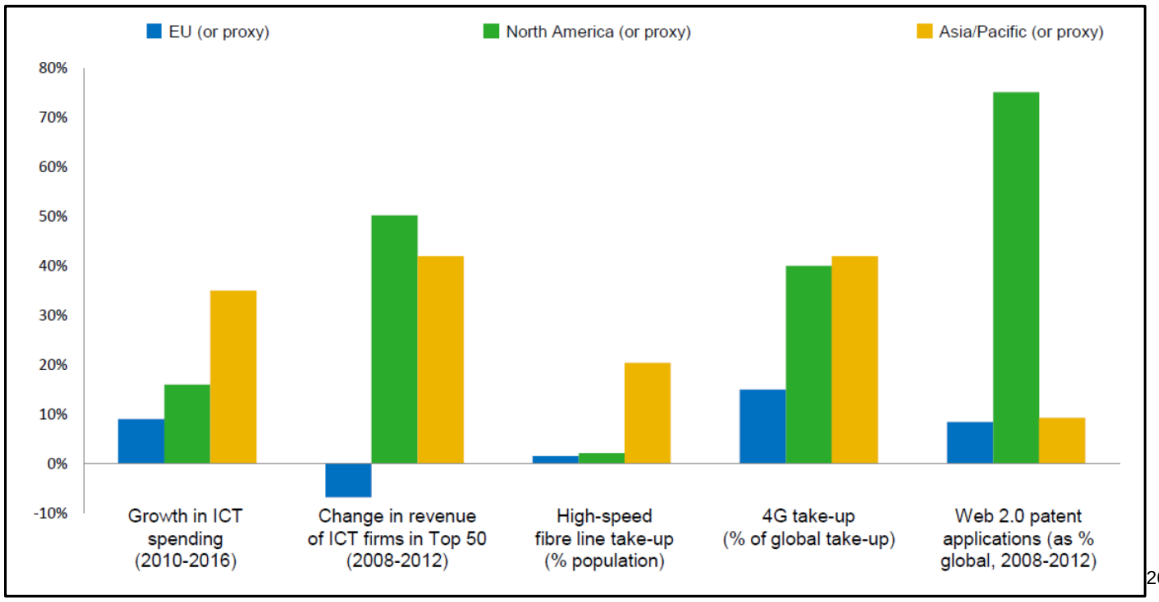
- 74% af europæerne opfatter offentliggørelse af personoplysninger som en stadig større del af den moderne tilværelse,
- 43% af internetbrugerne siger, at de er blevet anmodet om at opgive flere personoplysninger end nødvendigt,
- 33% af europæerne er klar over, at der findes en national offentlig myndighed, der er ansvarlig for databeskyttelse, og
- 90% af europæerne ønsker de samme databeskyttelsesrettigheder over hele EU.[257]

Dertil blev det vurderet i 2014, at "*(...) the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020 (...)*"[258], hvis alle borgere stoler på de dataansvarlige.

Dansk Industri har citeret og kommenteret J.M. Barrosos præsentation til Det Europæiske Råd.[259] Denne inkluderer vigtig statistisk data på området. Nedenstående søjlediagram fra kilden viser, at EU er bagud på alle 5 målte parametre indenfor *ICT*[260], 4G-netværk og applikationspatenter i forhold til Asien og Nordamerika:

"*Manglende investeringer i IKT* [ICT red.]*, faldende omsætning på det digitale område og utilstrækkelig digital infrastruktur udgør tydelige tegn på, at Europa har meget at indhente.*".

[257] Communication, D.-G. (2011). Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. Hentet fra http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf (tilgået 12/05/2018).
[258] Citat: Commission, E. (2014). Progress on EU data protection reform now irreversible following European Parliament vote. Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_MEMO-14-186_da.htm (tilgået 10/04/2018).
[259] Dansk Industri. (u.d.). *Dansk Industris hjemmeside.* Hentet fra https://digital.di.dk: https://digital.di.dk/SiteCollectionDocuments/Publikationer/Faktaark%20om%20strategi%20for%20EUs%20digitale%20indre%20marked.pdf (tilgået 15/04/2018).
[260] Information and Communications Technology.



[261]

Som J.M. Barroso netop antyder i materialet, er tilliden og sikkerheden på internettet en stor udfordring for det digitale indre marked. Dette skyldes især, at risikoen for misbrug og cyberkriminelt adfærd med EU-borgeres data stiger. Ligeledes har IBM udgivet resultaterne fra en amerikansk undersøgelse, hvor 75% af de 10.000 adspurgte tydeliggjorde, at de aldrig ville købe et produkt online, uanset hvor godt tilbuddet var, hvis borgeren ikke stoler på selskabets håndtering af persondata.[262]

Ved ovenstående argumenter er det vist, at EU havde incitament til at skabe et nyt regelsæt baseret på en ny europæisk strategi for det digitale marked.

3.3.2.1 Forsvarlig persondata og gunstigere betingelser og konkurrencevilkår for digitale net og innovative tjenester

På baggrund af ovenstående har EU analyseret sig frem til en række tiltag, som bygger på tre søjler, der i alt indeholder 16 punkter.[263] Alle blev gennemført ved udgangen af 2016. Tiltagene ændrer den traditionelle måde at drive forsvarlig storøkonomi på til en ny, bæredygtig, sikker og moderne måde, som kan følge med de andre storøkonomier globalt. Søjle nr. 2 omhandler *gunstigere betingelser og lige konkurrencevilkår for digitale net og innovative tjenester*. Søjlens pkt. 12 forventer, at tiltagene vil "*(...) styrke tilliden til og*

[261] Dansk Industri. (u.d.). *Dansk Industris hjemmeside.* Hentet fra https://digital.di.dk: https://digital.di.dk/SiteCollectionDocuments/Publikationer/Faktaark%20om%20strategi%20for%20EUs%20digitale%20indre%20marked.pdf, s. 2 (tilgået 21/04/2018).
[262] *IBM New Room*. (16. April 2018). Hentet fra http://newsroom.ibm.com: http://newsroom.ibm.com/2018-04-16-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacy-and-Security (tilgået 19/04/2018).
[263] Europakommissionen. (u.d.). Europa-Kommissionen - Pressemeddelelse. Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_IP-15-4919_da.htm (tilgået 28/02/2018).

sikkerheden i digitale tjenester, især for så vidt angår håndtering af personoplysninger. På grundlag af EU's nye databeskyttelsesregler, som forventes vedtaget inden udgangen af 2015, vil Kommissionen revidere e-datadirektivet."[264] De omtalte databeskyttelsesregler og e-datadirektivet er efterfølgende mundet ud i den forordning, som dette speciale behandler.

3.3.2.2 Parternes incitament for implementering

Ovenstående argumenter for og imod Forordningen er benyttet. Nedenstående to tabeller er udarbejdet for at vise, hvordan værdierne til den efterfølgende spilmatriks er fundet. Først vurderes 1) parternes nytte ved en implementering af Forordningen, og derefter 2) parternes nytte ved at Forordningen ikke implementeres.

1) Tabel ved implementering af Forordningen:

Parterne og nytten	**Implementerings-udgifter**	**Sikkerhed**	**Mere fuldkommen konkurrence**	**Handel**	**I alt**
Borger	-	+	+	+	2
Små og MS[265] *virksomheder*	-	+	+	++	3
Store virksomheder	-	+	-	-	-2
Markedet	-	+	+	+	3

2) Tabel uden implementering af Forordningen:

Parterne og nytten	**Implementerings-udgifter**	**Sikkerhed**	**Mindre fuldkommen konkurrence**	**Handel**	**I alt**
Borger	0	-	-	-	-3
Små og MS virksomheder	0	0	-	-	-2
Store virksomheder	0	0	+	+	2
Markedet	0	-	-	-	-3

[264] Citat: Europakommissionen. (u.d.). Europa-Kommissionen - Pressemeddelelse. Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_IP-15-4919_da.htm (tilgået 28/02/2018).
[265] "*MS*" = mellemstor. Tabeller er udarbejdet af forfatterne.

Ovenstående tabeller er benyttet til at udarbejde nedenstående opsamlende spil-matriks. Denne viser, at der opstår *nash*- og *kaldor-hicks-ligevægt* i punktet *Handle / Forordning* (2,2). Denne ligevægt skaber den højeste nytte for alle parter inkl. markedet - dog ikke de *store virksomheder*. Hvis de store virksomheder også fik noget ud af Forordningen, ville Forordningen blive paretooptimal. Se mere om pareto på side 88.

Matriks over ligevægten i markedet ved hhv. implementering af Forordningen og ingen implementering af Forordningen:

Forbruger/virksomhed	Forordning	Ikke Forordning
Handle	**2,2**	-3,1
Ikke handle	0,-1	0,0

Der konkluderes i forhold til ovenstående, at både borgerne og virksomhederne (som helhed) har incitament til at implementere Forordningen. Dette skyldes primært, at EU-Kommissionen forventer, at:

1. borgerne vil købe mere,
2. flere kommer i arbejde,
3. markedet bliver mere fair overfor små og mellemstore virksomheder, og
4. innovationen øges.

3.3.2.3 Persondata i økonomisk kontekst

Eftersom borgerne i et anseeligt omfang har mistet troen på, at dataansvarlige kan behandle dataen forsvarligt, er der ved Forordningen en øget forventning om, at virksomheder og myndigheder reelt overholder Forordningen. Den væsentligste håndhævelse ved dette fremgår i de høje krav til politikker, procedurer og især det nye skærpede bødeniveau for overtrædelse af Forordningen.

Derfor opstår der uundgåeligt signifikante omkostninger og transaktionsomkostninger ved selve implementering af Forordningen fra virksomhedernes synspunkt. Det væsentlige spørgsmål er herefter, om udgifterne, som virksomhederne er tvunget til at afholde, er proportionelle med formålet for Forordningen. Ligeledes stilles spørgsmålet om borgerne, økonomien og det digitale indre marked bliver tilsvarende bedre efter implementeringen af Forordningen d. 25. maj 2018.

Det fremgår i det forberedende arbejde til Forordningens, at et bedre digitalt indre marked, hvor borgerne har tillid til at give deres data, kan maksimere EU-medlemsstaternes økonomi

ved øget handel. Jean Claude Junker, formand for Europa-Kommissionen, nævner, at væksten kan øges med op til 250 mia. EUR, og samtidig kan der skabes hundredtusindvis af nye jobs grundet Forordningen.[266] I en strategi for et digitalt indre marked i EU nævntes yderligere, at

> "*(...) Europa har forudsætningerne for at føre an i den globale digitale økonomi, men i øjeblikket udnytter vi dem ikke optimalt. Opsplitning og barrierer, der ikke findes på det fysiske indre marked, holder EU tilbage. Hvis disse barrierer inden for Europa bliver nedbrudt, kan det bidrage med yderligere 415 mia. euro til EU's BNP.*"[267]

Hermed opsummeres, at der forventes, at der findes et stort økonomisk potentiale, ved at EU udnytter den digitale økonomi optimalt.

3.3.3 Perfekt og symmetrisk information

Hvis Forordningens ønske om at borgeren anerkender virksomheder som værende kompetente til at behandle deres persondata, vil det unægteligt øge virksomhedernes adgang til borgernes information.

Dette taler for, at virksomhedernes opnår mere *perfekt information* og forøget *symmetrisk information*. Dette skyldes to grunde: 1) virksomheden ved, hvordan den selv agerer, og 2) når borgerne fortæller mere om sig selv, jo mere viden opnår virksomheden om borgeren. Ud fra borgernes synspunkt er denne øgede perfekte og symmetriske information svær at lokalisere, da informationen kun går fra borgeren til virksomheden.

Dermed har virksomhederne et stort ønske om, at forbrugerne anerkender Forordningen, og at de udviser tillid til virksomheden, mens forbrugerne først har behov for at dele deres data, når de reelt får noget retur. Dette uddybes i næste afsnit.

3.3.3.1 Når forbrugeren nyttemaksimerer - quid pro quo

Der opstår et naturligt krav om, at forbrugere vil have noget igen, før de vil afgive deres persondata. Denne nyttemaksimering er idéen om "*noget for noget*"-princippet[268]. Hvis forbrugeren får adgang til en applikation, nyhedsbrev, e-bog, spil, hjemmeside o.l. ved at

[266] http://ec.europa.eu. (u.d.). Hentet fra http://ec.europa.eu/priorities/sites/beta-political/files/pg_da.pdf (tilgået 15/2/2018).
[267] Citat: Meddelelse Fra Kommissionen Til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget - Bruxelles, den 6.5.2015 COM(2015) 192 final, s. 2 (tilgået 15-02-2018).
[268] *Quid pro quo*.

afgive data, opstår der en gensidig (elektronisk) kontrakt, hvor virksomheden opnår data, og forbrugeren opnår en reel ydelse.

> "*For instance, an app developer may consider their "free" offering to warrant some invasion of privacy which can be monetized to off-set the cost of the game development and yield a reasonable profit*"[269].

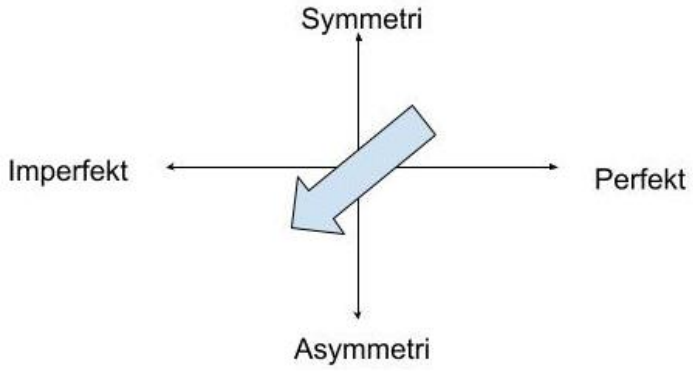
Begge parter nyttemaksimerer hermed, og ud fra et økonomisk synspunkt er dette mere efficient, end hvis handlen ikke blev indgået.

Hvis fx virksomheder sender spørgeskemaer ud, får forbrugeren ikke en reel ydelse eller produkt ud af at besvare det, og derfor er der mindre incitament til at besvare spørgeskemaet. Hvis borgeren gør det alligevel, er det kun virksomheden, der opnår nytte ved øget viden og data. Modsætningsvist vil den imperfekte og asymmetriske information fra borgerens synspunkt blive øget.

Dette betyder, at det totale gensidige informationsforhold mellem virksomheden og borgeren bliver mindre symmetrisk og mindre perfekt, da skævvridningen bliver forøget af, at dataen kun bevæger sig den ene vej. Skævvridningen bliver større og større; da "*Information asymmetries are arguably escalated with the increase use of big data and emergence of personal data markets.*"[270].

Visuel oversigt af bevægelsen ved ændret informationsøkonomi - fra symmetrisk og perfekt, til imperfekt og asymmetrisk:

[269] Kim, D.-H., Hettche, M., & Clayton, M. J. (2015). The Privacy Paradox and Calculus Among Millennials: An Empirical Study of Privacy Attitude–Behavior Congruence. AMA Marketing & Public Policy Academic Conference Proceedings(25), s. 86.
[270] Citat: Bandara, R., Fernando, M., & Aktera, S. (2017). The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. *Procedia computer science*, s. 564.



271

Det vurderes, at det er svært at præsentere økonomiske rationaler for, hvorfor borgere skal afgive deres persondata alene på baggrund af en øget tillid, hvis de ikke får noget igen. Det er kun virksomheden, der profitmaksimerer ved denne opbygning af data-deling.

Borger / virksomhed	***Give ydelse***	***Ikke give ydelse***
Dele data	***10***, ***10***	-10, 10
Ikke dele data	*10, -10*	***0***, ***0***

Matriks der viser, det ikke er efficient for borgerne at dele data, når de ikke får nogen ydelse retur (-10, 10).

Derfor argumenteres der for, at borgeren skal have en ydelse retur, før begge parter nyttemaksimerer. EU kan ikke tvinge virksomhederne til at give borgerne en ydelse igen. EU kan blot skabe incitament til at øge tilliden mellem borgeren og virksomheden. Herefter er det op til parterne på markedet at løse, komplikationerne mellem borgerne og virksomhederne. Derfor er der krav om følgende fra borgernes synspunkt for at indgå en handel:

$$Værdi\ i\ at\ dele\ data\ *\ tilliden\ > Tabet\ i\ at\ dele\ data * (1 - tilliden)$$

Hvor tilliden er den tiltro, som forbrugerne og borgerne har til udbyderne af ydelsen.

Umiddelbart har borgeren først incitament til at dele sin data, hvis der både er udsigt til at få en ydelse retur, og betalingsmidlet bliver håndteret sikkert. Dette genererer en gensidig nyttemaksimering. Derfor kan det være svært at overbevise borgeren om, at de kan stole på den dataansvarlige uden en réel gensidige sikker handel.

[271] Figuren er forfatternes egen tilegnelse med inspiration fra Clausen, NJ, Kronborg, A, Legind, ND & Mortensen, BOG (eds) 2017, *Festskrift til Hans Viggo Godsk Pedersen*, Djøf / Jurist- og Økonomforbundet, København, s. 609.

3.3.3.2 Risikoaverse og begrænset rationelle borgere

På trods af ovenstående videregiver borgeren typisk ikke sin data, når den førnævnte økonomiske formels fokus tipper fra at være negativ til at være positiv. Dette skyldes, at borgere gennemgående er *risikoaverse*[272] og *begrænset rationelle*[273]. Selvom der økonomisk kan bevises øget nytte ved at afgive persondata til virksomheder, gør borgeren det nogle gange alligevel ikke. Det er irrationelt, men alligevel den adfærd som borgere almindeligvis udviser.

Risikoaversion er den adfærd, som størstedelen af den økonomiske litteratur forudsætter, at borgere har. "*It is the reluctance of a person to accept a bargain with an uncertain payoff, rather than one who offers a more certain, but possibly lower, expected payoff*"[274]. Derfor opnår virksomheder stor succes med fx konkurrencer, hvor borgeren svarer på et spørgeskema for at deltage. Usikkerheden og risikoaversionen gør, at borgeren handler, som citatet foreskriver.

Dette er ikke efficient for markedet, og derfor skal der være udsigt til en endnu større nytte ved afgivelse af data, før borgeren reelt vil foretage handlingen. En stor gevinst med lille sandsynlighed for at vinde er altså mere værd end en lille gevinst med stor sandsynlighed for at vinde. Dette argumenterer for, at tilliden til virksomhederne og Det Digitale Indre Marked skal være stærk, ufejlbarligt og sikkert, før handlen af data og ydelse bliver foretaget.

3.3.4 Efficiensteori - Pareto og Kaldor-Hicks

For at forstå hvorfor udnyttelsen af persondata er kommet så vidt, at der er behov for en en Forordning, vil efficiensteori blive benyttet. Dette skyldes, at det økonomisk kan forklares, hvorfor udbydere er endt med at overudnytte borgernes persondata.

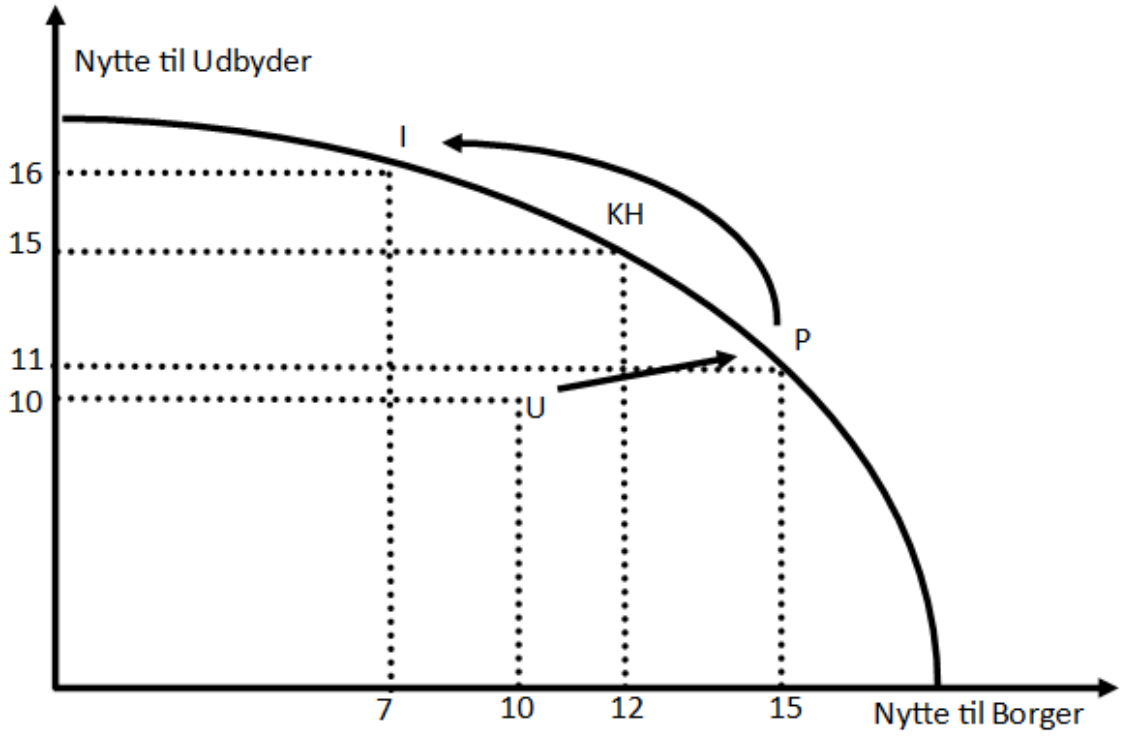
Paretoefficiens bygger på princippet om, at ingen parter må stilles værre ved en given handling. Med andre ord, når pareto-optimaliteten er fundet, kan man ikke stille en part

[272] Arrow, K. (1986). *Handbook of Mathematical Economics* (1 udg., Årg. 3), s. 1188.
[273] Knudsen, C. (2011). *Økonomisk psykologi - adfærdsøkonomiske perspektiver på virksomhedens organisering, økonomiske grænser og identitet* (1 udg.). Samfundslitteratur, s. 267, og Lyck, L. (2008). Service- og oplevelsesøkonomi i teori og praksis (1. udg.). Academica, s. 24.
[274] Citat: Benchimol, J. (2014). Risk aversion in the Eurozone. Research in Economics, 68(1), s. 48.

bedre uden at stille en anden part dårligere.[275] Dertil skal en handling, som giver værdi til én part, og samtidigt giver ingen skade for andre parter, realiseres.[276]

I sammenhæng med dette speciale betyder teorien, at udbyderne af fx applikationer får en højere nytte, jo mere de sælger og bearbejder borgernes data, og ligeledes er overudnyttelsen til ulempe for borgerne, da de føler sig udnyttet.

Når borgernes persondata bliver udnyttet i moderate mængder, kan ulempen for borgeren kompenseres af de nye innovative muligheder, som salget af dataen bringer med sig. Når udnyttelsen af borgernes data bliver højere, vil borgerens nytte falde betragteligt, mens udbyderens nytte fortsat vil stige langsomt, da ↑ $udbyders\ nytte < borgerens\ tab\ af\ nytte$. Dette ses nedenfor i punkt $KH \rightarrow I$.



277

Kaldor-Hicks-efficiens kræver, at den part der får størst nytte på bekostning af den anden part, blot kan kompensere den tabende ved at reallokere nytten. Det er naturligvis et krav, at den vindende part skal vinde mere, end hvad den tabende part taber - ellers er det irrationelt. Dette er fx punkt $P \rightarrow KH$, da *Udbyder* vinder mere (+4), end hvad *Borger* taber (-

[275] Eide, E., & Stavang, E. (2008). Rettsøkonomi (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 96-97.
[276] Eide, E., & Stavang, E. (2008). Rettsøkonomi (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 107.
[277] Grafen er forfatternes tilegnelse med inspiration fra Eide, E., & Stavang, E. (2008). Rettsøkonomi (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 109. Grafen er ikke målbar.

3). Modsat kan dette ikke lade sig gøre ved punkt $KH \rightarrow P$, da *Udbyder* taber mere (-4), end hvad *Borger* vinder (+3), og derfor er denne sidste relokation ikke fordelagtig totalt set.

Af disse grunde skal Forordningen omplacere parterne til det sted, hvor betingelserne er mere gunstige.

Oversigtstabel over samfundsnytten ved Pareto og Kaldor-Hicks:

Borger / udbyder	*Udnytter ikke data (**U**dgangspunkt)*	Udnytter moderat *(**P**areto)*	Udnytter mere *(**K**aldor-**H**ichs)*	Udnytter groft *(**I**nefficiens)*
Handler	*10 , 10 (=20)*	**15 , 11** (=26)	**12**, **15** (=27)	**7** , **16** (=23)
Handler ikke	*0 , 0*	0 , 0	0 , 0	0 , 0

Udgangspunktet beskrives som punkt U i ovenstående graf og tabel. Her er parternes nytte sammenlagt kun 20. Der optimeres ved, at parternes placering rykkes mod højre og op på grafen. Ved at benytte efficiensteori til at forklare Forordningen, er det tydeliggjort, at der opstår innovative og synergiske fordele, når udbydere får lov til at benytte borgeres data til udvikling. Dette kan ses ved forskydningen fra punkt $U \rightarrow P$. Der er først, når *Udbyder* "udnytter mere", at placeringen går mod KH. Ved punktet I er der ingen efficiensforbedring, så det optimale punkt findes, hvor de to nytter tilsammen er størst (12,15).

Teorien stemmer overens med realiteten, da den viser, hvordan udbydere udnytter data til egen fordel. Nash-ligevægten i punkt (7,16) viser, at det er udbyderen, der bestemmer, da denne nytteoptimerer på borgerens bekostning. Dette sker på trods af, at borgeren sættes dårligere. Derfor vælger udbyderen ikke det sammenlagte bedste punkt (12,15).

The Privacy Paradox

Strategien for det indre marked viser, at 74% af EU-borgere gerne vil have lov til at give deres tilladelse, inden deres data bliver indsamlet og bearbejdet, og kun 22% af EU-borgerne stoler fuldstændigt på internetbaserede virksomheder.[278] Modsvarende benytter borgere alligevel databasserede tjenester i høj grad.

Der er en tydelig diskrepans mellem borgeres bekymring over at dele personlig data, og hvor meget borgere reelt deler deres data.[279] Denne forskel er i økonomisk og socialt fagligt

[278] Clausen, N. J., Kronborg, A., & Mortensen, B. O. (2017). Festskrift til Hans Viggo Godsk Pedersen (1 udg.). Jurist- og Økonomforbundets Forlag, s. 605.
[279] Bandara, R., Fernando, M., & Aktera, S. (2017). The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. Procedia computer science, s. 564.

litteratur beskrevet som *The Privacy Paradox*[280]. I dette speciale belyses to teorier indenfor dette paradox.

Den første er *The Private Calculus Theory*, hvor borgeren reelt foretager en *cost-benefit*-udregning. Borgeren kommer frem til, at fordelene er større end risikoen, og derfor underkendes de private persondatabekymringer.[281] Det skyldes, at sociale relationer fravælges, hvis borgeren ikke vil røbe sin data over en platform. Derfor er sociale normer og gevinster elementer, der trumfer privatheden.

Den anden er *Theory of Incomplete Information,* som er spilteoretisk.[282] Denne baseres på, at hverken borgeren eller virksomheden ved lige meget om hinandens værdier, nytter og regler. Persondataretligt ved borgerne sjældent, hvad deres data bliver brugt til[283], og derfor udregnes borgerens *cost-benefit* forkert ud fra *The Private Calculus Theory.* Studier viser, at denne miskalkulation giver hazardlignende adfærd, når borgeren har begrænset viden om, hvad teknologien kan, og de samtidigt har et fordrejet billede af sandsynligheden for misbrug af persondata.[284]

Et amerikansk empirisk forsøg fra 2015 vedr. studerendes skepsis ved at afgive persondata for at få adgang diverse applikationer konkluderer ligeledes, at;

" *(...) it is foreseeable that a large number of app developers will continue to push the envelope as far as what is acceptable and necessary in terms of tracking online behavior and capturing personal information. Without some form of self-regulation by the community of developers, there may continue to be an erosion of consumer privacy* (...)*"*[285], og artiklen afslutter med sætningen:

"Thus the government or tech oligopoly which controls the flow of apps may need to create some form of regulation to protect consumers' privacy."

[280] Kokolakis, S. (2017). *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*. Computers & Security, s. 122-134.
[281] Culnan, M. J., & Armstrong, P. K. (1999). *Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation*. Organization Science, 10(1), s. 104-115.
[282] Harsanyi, J. C. (1967). *Games with incomplete information played by "Bayesian" players, i–iii: part i. the basic model*. Management Science, 14(3), s. 159-182
[283] Hofacker, C. F., Brudvig, S., Raman, P., Grosso, M., Castaldo, S., & Premazzi, K. (2010). *Customer Information Sharing with E-Vendors: The Roles of Incentives and Trust*. International Journal of Electronic Commerce, 14(3), s. 63-91.
[284] Acquisti, A., & Grossklags, J. (2005). *Privacy and rationality in individual decision making*. IEEE Security & Privacy, 3(1), s. 26-33.
[285] Citat: Kim, D.-H., Hettche, M., & Clayton, M. J. (2015). *The Privacy Paradox and Calculus Among Millennials: An Empirical Study of Privacy Attitude–Behavior Congruence*. AMA Marketing & Public Policy Academic Conference Proceedings(25), s. 86.

Forordningen vurderes relevant at implementere, da markedet hverken er paretooptimalt eller kaldor-hicks-optimalt længere - men derimod inefficient. Forordningen vil være med til at reallokere nytterne på markedet, så borgerne ikke udnyttes i samme grad efter implementeringen. Der er bred samfundsvidenskabelig enighed om, at paretooptimalitet er en god målsætning for samfundsøkonomien.[286] Dette er for sent at rette op på ved en paretorelokering, da Forordningen som udgangspunkt kommer til at sætte de globale *tech*-virksomheder dårligere. Derfor er det en Kaldor-Hicks-forbedring.

Dermed har den tidligere regulering fejlet, da den har skabt en mistillid fra borgerne mod virksomhederne. Det er blevet konkluderet, at det politiske ønske om at skabe Det Digitale Indre Marked, ikke har været forenelig med borgernes reelle risikovurdering ved at videregive deres data under Direktivet.

3.3.4.1 Tragedy of the Commons

Denne teori[287] blev første gang beskrevet ud fra et biologisk synspunkt om konsekvensen af overudnyttelse af delte naturressourcer. Principperne fra denne teori kan benyttes analogt til at vurdere konsekvensen og løsningsforslagene, når udbydere af data handler hæmningsløst med borgerens data. Som forfatteren, Garrett Hardin, skriver i artiklen: "*Consider bank-robbing. The man who takes money from a bank acts as if the bank were a commons. How do we prevent such action?*"[288]. For at undgå at bankrøvere behandler bankens penge som et *common*, straffes røveriet ved regulering. Samme koncept kan benyttes til at undgå udbyderes udnyttelse af borgeres data som et *common*.

Det antages, at borgernes data følger med som betaling, hver gang borgeren fx erhverver en applikation. Dataen er derfor en ressource, som udbydere har adgang til, og den benyttes i stort omfang for at tjene penge. Hver gang udbyderen 1) sælger data videre til tredjepart, 2) benytter data til direkte markedsføring eller 3) vil kende borgernes handlemønstre, undergraver det borgerens ønske om, at udbyderne har dataen, da borgerne i stigende omfang bliver mindet om, at de udnyttes. Ifølge Europa-Kommissionens pressemeddelelse *Et digitalt indre marked i Europa: Kommissionen fastsætter 16 initiativer for at gøre det til en*

[286] Eide, E., & Stavang, E. (2008). Rettsøkonomi (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 97.
[287] *The Tragedy of the Commons*-teorien blev beskrevet af Garrett Hardin.
Kilde: Garrett, H. (1968). The Tragedy of the Commons. Journal Science, 162(3859). Hentet fra http://science.sciencemag.org/content/sci/162/3859/1243.full.pdf, (tilgået 07-04-2018).
[288] Citat: Garrett, H. (1968). The Tragedy of the Commons. Journal Science, 162(3859). Hentet fra http://science.sciencemag.org/content/sci/162/3859/1243.full.pdf, s. 1247.

realitet[289] mister borgerne tilliden, og de ender på sigt med at at gå i "baglås" og negligere udbyderne. Borgerne vælger deling og handel med personlig data fra. Ifølge teorien vil udbyderne ende uden persondata, som der ellers skal benyttes, før at udbyderne kan innovere EU til fx at blive mere teknologisk.

The Tragedy of the Commons foreslår to løsningsmodeller: 1) privatisering af ejendomsretten eller 2) statslig regulering.[290] Det er forslag nr. 2 om at inkorporere statslig regulering, der er interessant i dette speciale i forhold til persondata, da dette er, hvad EU lægger op til ved at implementere Forordningen. Reelt set vil reguleringen, som EU lægger op til, være med til at konkretisere ejendomsrettighederne af persondata, og derfor opnås punkt 1 samtidigt. Det skal understreget, at persondataen er privatiseret under Direktivet, men virksomheder og menigheder har haft tendens til at handle som om, at persondataen var et *common*.

3.3.5 Theory of the Firm

Theory of the Firm er en neoklassisk økonomisk disciplin, der forklarer, hvordan firmaer, borgere eller arbejdstagere handler ud fra en given situation. I bund og grund allokerer subjektet sine ressourcer, efter hvor der forventes af opstå mest muligt nytte i fremtiden. Nytte kan for selskaber være overskud på bundlinjen, og for borgere og arbejdstagere kan det være penge eller fritid. Dvs. at hvis en arbejdstager kan få mest muligt ud af ikke at lave noget, vil dette være at foretrække. For at komme dårligt udført arbejde til livs bliver kontrakter, monitorering, medejerskab o.l. indført i forholdet. Dette styrker incitamentet for at arbejde og handle, som det er ønsket af principalen. Alle handlinger der foretages, tages på baggrund af en udsigt til at blive stillet bedre i fremtiden. Dette er det marginale overskud, og derfor ender udbydere med at udnytte borgernes persondata.[291]

Transaktionsomkostninger

Alle handler konstant. Ligegyldigt om det er et forhold mellem kunde/supermarked, selskab/revisionsafdelingen eller en applikationsudbyder/applikationsbruger. Som Ronald Coase skriver i *The Nature of the Firm*, vælger aktører at få deres behov dækket, hvor det er billigst. Dette betyder, at hvis det billigst at have sin egen regnskabsafdeling, findes den

[289] Europakommissionen. (u.d.). Europa-Kommissionen - Pressemeddelelse. Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_IP-15-4919_da.htm, søjle II, trin 12 (tilgået 15/04/2018).
[290] Garrett, H. (1968). The Tragedy of the Commons. Journal Science, 162(3859). Hentet fra http://science.sciencemag.org/content/sci/162/3859/1243.full.pdf, s. 1248.
[291] theory of the firm. (u.d.). Hentet fra http://www.businessdictionary.com: http://www.businessdictionary.com/definition/theory-of-the-firm.html, (tilgået 25/03/2018).

internt i selskabet, og modsat findes den eksternt, hvis dette er billigere. Den imperfekte information gør, at transaktionsomkostningerne bliver afgørende for handlen.[292] Forhandlingen er mere efficient, når udvekslingen af ydelser sker med så få transaktionsomkostninger som muligt. Det kræver blot, at ejerrettighederne er veldefinerede, at der kan forhandles, og ydelsen kan allokeres mellem parterne. Hvis dette sker, forventer *Coase Theorem*, at hver handel og allokation vil være pareto-efficient.[293]

Grundet faldende transaktionsomkostninger bliver der nemmere indgået aftaler, og derigennem bliver selskaber stiftet for at afhjælpe andres behov. Dette er allokeringen af nytter, hvor det bliver billigere, hvis aktørerne gør det, de er bedst til. Det er som udgangspunkt det frie marked og Adam Smiths *usynlige hånd*, der gør, at den højeste mulige nytte finder sted, og priser vil automatisk gå mod produktionsomkostningerne. Den naturlige frihed er afgørende, da dette tvinger konkurrenter til at underbyde hinanden for at erhverve marked. Hermed undgås på sigt monopolister, politikere og embedsmænd, som kan bestikkes. Hermed er denne umiddelbare liberale grundtanke begyndelsen til de efterfølgende økonomiske teorier om fuldkommen konkurrence.[294]

Ifølge teorien er der dermed ikke behov for at påvirke handlen eller markedet, da det er selvregulerende, når alle handler i egen interesse. Det er dog et krav, at det skal være nemt for nye spillere at komme ind på det frie marked. Hvis kravene er opfyldt, er der ud fra denne teori ikke behov for Forordningen.

Producenten af applikationer har brug for midler til at udvikle applikationer (udbuddet). Dertil har borgerne en nytte i at erhverve applikationen (efterspørgslen). Borgeren har data om sig selv, som ikke har nogen stor værdi, så længe borgeren har den. Modsætningsvist har dataen stor værdi hos applikationsproducenten, da den fx kan sælges eller benyttes til *direct marketing*. Dataen har så stor værdi, at producenten vil give sin applikation mod betaling med borgerens data.

[292] Coase, R. H. (1937). The Nature of the Firm. Economica, 4(16), s. 386–405.
[293] Hendikse, G. (2003). Economics and Management of Organizations. McGrawHill, s. 68.
[294] Smith, A. (1776). An Inquiry into the Nature and Causes of the Wealth of Nations. London: W. Strahan and T. Cadell, s. 505, 620 og 726.

Matriks over forventet nytte ved at indgå handel

Borger / producent	Udvikle og sælge app	Ikke udvikle og sælge app
Give data	10 , 10	*N/A*[295]
Ikke give data	10 , -10	0 , 0

I ovenstående matriks er det tydeligt gjort, at der både er nash-ligevægt i (10,10) og (0,0).

Derfor allokeres dataen som ved en handel, hvor applikationen er modydelsen. Det er ligeledes vist, at hvis borgeren ikke vælger at give sin data, er der ikke midler til at udvikle applikationen. Derfor er det samfundsøkonomisk vigtigt, at borgeren ønsker at handle.

3.3.6 Hvordan Forordningen retfærdiggøres

Hvis borgerne har mistet tilliden til virksomhederne, skader det den samlede omsætning i EU. Derfor er det i EU's interesse at rette op på dette ved at sikre, at borgerne igen har incitament til at handle og dele deres persondata på forsvarlig vis.

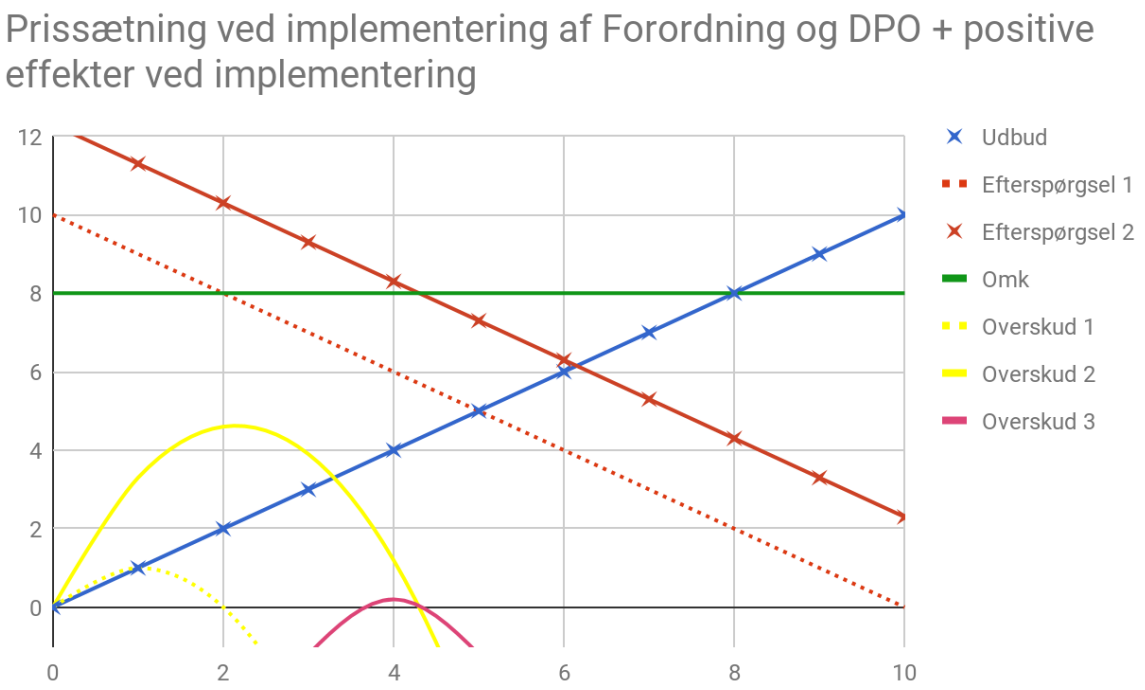
En forventning om en øget beskyttelse af privat data vil føre til større samfundsmæssig accept af behandlingen af persondata. Dette har antageligvis en positiv påvirkning på købekraften, beskæftigelsen og dermed økonomien, da flere mennesker kommer i arbejde, når flere begynder at handle, som det allerede blev ønsket under Direktivet;

> "*Protection of individual privacy (...) will promote growth and job creation in the, private and public sectors.*"[296].

Grafen nedenfor beskriver, hvordan efterspørgselslinjen flytter sig mod højre, når borgerne får mere tiltro til virksomhederne, og af den grund handles der mere. Det vises ved, at efterspørgslen bevæger sig ud af x-aksen (fra *Efterspørgsel 1* til *Efterspørgsel 2*). Resultatet er, at overskuddet går fra $(1 * 1 =)$ 1 til $(2{,}2 * 4{,}7 =)$ 10,34 for monopolisten, som denne nyder godt af, da borgerne udviser tillid. Der kommer hermed en stigning af omsætning til monopolisten fra 8[297] til 10,34 fra før implementering til efter implementering. Dette kan sammenlignes med, at kvaliteten af en vare/ydelse forøges, og dette skaber større incitament for borgerne til at købe en given ydelse. Ændringen giver virksomhederne mere persondata, som de skal bruge til at vækste og innovere med.

[295] Der blev vist på side 87, at denne mulighed ikke kan lade sig gøre spilteoretisk.
[296] Citat: COMMISSION OF THE EUROPEAN COMMUNITIES COM(92) 422 final - SYN 287 Brussels, 15 October 1992, Amended proposal for a COUNCIL DIRECTIVE on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Tilgået ved http://aei.pitt.edu/10375/1/10375.pdf, s. 128:
[297] Som det blev vist på side 76.

Hvis der sker ændringer i individets behov, har betalingsvilligheden ændret sig.[298] I dette tilfælde svarer øget regulativ beskyttelse for et "positivt skift", som ses ved, at betalingsvilligheden øges, og efterspørgselskurven går mod højre.



De efterfølgende effekter af Forordningen og strategien for det Indre Marked er, at flere små og mellemstore virksomheder skal komme ind på markedet, og derfor vil prisen ende med at at gå fra 10,3 til omkring 8. Dette er tendensen ved fuldkommen konkurrence. Prisændringen svarer til, at den solgte mængden på markedet går fra $(10{,}3 * 2{,}2 =)$ 22,66 til $(4{,}2 * 8 =)$ 33,6. Denne udvikling vil udfase monopolisten, så markedet bliver mere konkurrencedygtigt til sidst, da CS stiger. Det vises ved, at prissætningen går fra *overskud 1* (monopolistens prissætning uden de fordele som Forordningen bringer med sig) til *overskud 2* (monopolistens prissætningen med de fordele som Forordningen bringer med sig) til *overskud 3* (den endelige prissætning når markedet går fra monopolistisk til fuldkommen konkurrence).

Dette er reelt rationalet bag, at Forordningens store implementeringsomkostninger alligevel kan betale sig. Forordningen lægger op til, at borgerne opnår mere "kvalitet for pengene", og

[298] Eide, E., & Stavang, E. (2008). Rettsøkonomi (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 67.

en øget tillid til markedet og virksomhederne gør, at efterspørgslen stiger. Europas økonomi vil ifølge Europa-Parlamentet stige med 250 mia. euro.[299]

Dermed er dette speciales grafer i det økonomiske udgangspunkt fra side 64 blevet uddybet, og yderligere mikroøkonomiske argumenter for at implementere Forordningen er blevet analyseret og påvist.

3.3.6.1 Dynamisk konkurrence

I kontrast til afsnittet om statisk konkurrence på side 69, hvor der konkurreres på pris, er *den dynamiske konkurrence*, hvor der bl.a. konkurreres på kvaliteten. Da der i sidste afsnit blev fastslået, at *kvaliteten* på ydelserne intensiveres ved Forordningen, bliver denne konkurrenceform ligeså inddraget i specialet. Den dynamiske konkurrence tvinger udbydere til at følge med standarden (*benchmarken*) på markedet, da der mistes markedsandel og kunder, hvis der ikke sættes de samme høje krav til håndteringen af persondataen. Hvis alle udbydere følger med de nye persondatakrav, vil det nye *benchmark* for håndtering af persondata ikke skabe en konkurrencemæssig fordel mellem konkurrenter. Samtidig tvinger Forordningen konkurrenter til at overholde de nye krav, da den dynamiske konkurrence giver konkurrencemæssige fordele, til dem der følger den.[300]

3.3.7 Fuldkommen konkurrence og dataportabilitet

Ved at regulere så EU-borgere fx kan få flyttet deres profil til et andet socialt medie (til en anden dataansvarlig), opstår der mere fuldkommen konkurrence. Dataportabilitet hjemles i artikel 20 i Forordningen, og formålet forventes at give stor værdi for fx nye og små sociale medier. Dette påvirker efterfølgende markedet positivt. Behovet for artikel 20 skyldes primært, at de dominerende spillere på markedet nyder godt af *fastlåsningen* af EU-borgernes profiler, da det i dag er meget besværligt at flytte sin konto.[301]

3.3.8 Forordningens effekt

Der er behov for, at Forordningen efterleves i alle udstrækninger, før borgerne udviser den tillid, som der kræves. Herefter kan den digitale økonomi i Europa øges med de substantielle beløb, som specialet tidligere har nævnt, at Forordningen kan generere. Hvis virksomhederne udviser ansvarlighed overfor borgernes data, forventer Forordningen, at

[299] Europakommissionens hjemmeside. (u.d.). Hentet fra http://ec.europa.eu: http://ec.europa.eu/priorities/sites/beta-political/files/pg_da.pdf, (tilgået 21/2/2018)
[300] Eide, E., & Stavang, E. (2008). Rettsøkonomi (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG, s. 64.
[301] Dall, N. P., Langemark, J., & Langebæk, A. (2016). Persondataforordningen - en håndbog for praktikere (1 udg.). Ex Tuto Publishing, s. 217.

økonomien vil blive positivt påvirket. Det er forventet, at Europas BNP stiger med 415 mia. euro svarende til en stigning på omkring 2,8 %.[302] Derfor er der behov for, at alle virksomheder overholder Forordningens regler, ellers falder Forordningens formål på gulvet.

Forordning / virksomhed	Lav overholdelse	Middel overholdelse	Komplet overholdelse
Forordningens gennemførselsværdi	–	– / +	+ +

I december 2017 var det blot 8,5 % er globale virksomheder, der følte sig klar til Forordningen[303]*, derfor er det verserende, om de resterende 91,5 % bliver klar inden 25. maj 2018, da det kan gøre Forordningens gennemførselsværdi lav - som vist ved ovenstående tabel.*

Derfor er de harmoniserede bødesanktioner hævet til et højere niveau, så virksomhederne ikke har nogen grund til at bryde Forordningen.

Det er dyrt for virksomhederne at implementere Forordningen ift. advokathjælp, kurser, interne krav, retningslinjer og processer, men alternativt risikerer virksomheden at gå konkurs, hvis den ikke gør det.[304] Som Morten Boel Sigurdsson[305] udtaler: "*En vigtig pointe er, at man ved et læk af persondata kraftigt kan reducere sin bøde, hvis man med rettidig omhu har implementeret de rette tekniske og organisatoriske foranstaltninger. Det er en kraftig motivation for at gøre det fornødne*"[306]. Dertil risikeres tabet af virksomhedens *image*, som er svært at rette op på, når det først er tabt.

Grundet ovenstående vil virksomhederne være nødt til at forholde sig Forordningen.

3.3.8.1 Samfundskonsekvens af bøder

Forordningens strategi om at have et tilstrækkeligt højt bødeniveau, kan muligvis adfærdsregulere tilstrækkeligt til, at Forordningen bliver overholdt. Dette er en afvejning af:

1. *bøden* for at bryde Forordningen,
2. *sandsynligheden* for at blive opdaget,
3. *prisen* for at implementere Forordningen og
4. *etik*, *moral* og *interne strategier* i virksomheden.

---

[302] Dansk Industri. (u.d.). Dansk Industris hjemmeside. Hentet fra https://digital.di.dk: https://digital.di.dk/SiteCollectionDocuments/Publikationer/Faktaark%20om%20strategi%20for%20EUs%20digitale%20indre%20marked.pdf, s. 1 (tilgået 14/04/2018).
[303] Omada. (u.d.). Hvem har egentlig adgang til dine data? Hentet fra https://www.business.dk: https://www.business.dk/annonce/hvem-har-egentlig-adgang-til-dine-data, (tilgået 23/04/2018).
[304] Clausen, N. J., Kronborg, A., & Mortensen, B. O. (2017). Festskrift til Hans Viggo Godsk Pedersen (1 udg.). Jurist- og Økonomforbundets Forlag, s. 609.
[305] CEO for den danske it-sikkerhedsvirksomhed Omada.
[306] Citat: Omada. (u.d.). Hvem har egentlig adgang til dine data? Hentet fra https://www.business.dk: https://www.business.dk/annonce/hvem-har-egentlig-adgang-til-dine-data, (tilgået 23/04/2018).

Disse elementer skal gerne ende med at give tilliden tilbage til borgeren, og derfor vurderes *antallet af reelle krænkelser* og *medierne* at have en stor indflydelse på, hvor meget tillid der udvises fra borgerne efter implementeringen: "*Opbygningen af tillid (...) vil være afhængig af, at antallet af krænkelsessager vil være (...) ubetydelige. Mediedækningen vil formodningsvist have betydning for, hvorvidt borgerne vinder tillid til, at personhenførbare data, bliver behandlet i overensstemmelse med [F]orordningen.*"[307]

Da en reel krænkelse af Forordningen vil blive betragtet som markedssvigt, vil sanktionerne ende med at være så store, at der ikke er økonomisk incitament til at bryde Forordningen. Det må ikke kunne betale sig at bryde Forordningen, hvis målet for Forordningen skal opnås. Som det er vist i nedenstående spilmatriks, er der en interesse i ikke at overholde Forordningen, hvis bødeniveauet sættes lavt. Der er ligevægt i hhv. (10,10) og (-5,10), hvor den førstnævnte er den ønskede ligevægt.

Incitament for at overholde baseret på bødeniveau:

Forordningens bødeniveau / virksomhedens politik	**Overholder Forordningen**	**Overholder ikke Forordningen**
Høj	**10**, **10**	0, -10
Lav	10, 8	**-5**, **10**

Der skal bemærkes, at den enkelte borger ikke har nogen reel værdi af, at en virksomhed får en bødestraf for ikke at overholde Forordningen.[308] Forordningen giver derfor størst værdi for borgerne, så længe virksomhederne overholder den. Det skal derfor forstås, at det er virksomheden, der skaber værdien og nytten af Forordningen.

Ved ovenstående argumenter er det svært at afklare konkret, om borgeren opnår en øget tillid til databehandlingsvirksomhederne i EU, når Forordningen implementeres. Det kan dog ikke udelukkes, at det kan have en positiv virkning på *Det Digitale Indre Marked*, da tillid og tiltro til øget sikkerhed kan skabe den ønskede økonomiske virkning i Europa. Dette skyldes, at virksomhederne løber en stor risiko ved ikke at overholde Forordningen, og denne risikoafvejning giver borgerne sikkerhed og efterfølgende tillid. Dette øger købemængden på nationalt og europæisk plan.

[307] Citat: Clausen, N. J., Kronborg, A., & Mortensen, B. O. (2017). Festskrift til Hans Viggo Godsk Pedersen (1 udg.). Jurist- og Økonomforbundets Forlag, s. 611.
[308] Dette er kompliceret, da der skal anlægges et civilt søgsmål om erstatning.

3.4 DPO'en i økonomisk kontekst

3.4.1 Den forventede nytte som DPO'en tilfører

Det vil være relevant at undersøge, om der reelt opnås yderligere nytte ved ansættelsen af en DPO, da det burde give mere sikkerhed og kvalitet for alle parter. Virksomheden opnår omsætning og kunden opnår sikkerhed.

Et af argumenterne for at implementere Forordningen er den øgede sikkerhed, som forbrugerne nyder godt af. Ud fra et spil-teoretisk synspunkt betyder dette, at forbrugerne har mere tendens til at stole på virksomheder, der tager persondataen seriøst. Spilmatriksen beskrives således:

Positivt stemte borger overfor datadeling:

Forbruger/virksomhed	**DPO**	**Ikke DPO**
Handle	**4 , 6**	**5 , 6**
Ikke handle	0 , 5	0 , 5

Negativt stemte borger overfor datadeling:

Forbruger/virksomhed	**DPO**	**Ikke DPO**
Handle	**5 , 6**	**4 , 6**
Ikke handle	0 , 5	0 , 5

Som tydeliggjort findes der ikke en dominerende strategi, men ud fra et Kaldor-Hicks-synspunkt ender parterne i de med fed-markerede situationer (5,6). EU lægger op til, at flere og flere borgere har en tendens til at have den holdning, som matriksen "*Negativt stemte forbrugere overfor datadeling"* beskriver.[309]

Derfor vil det være mere nytteoptimalt, hvis flere virksomheder anerkender behovet for en DPO. Det er vurderet, at det ikke er alle virksomheder, har behov for en DPO, da nogle typer virksomheder ikke arbejder med tilstrækkelig følsomt data, og derfor er borgerne reelt ligeglade, om de har en DPO eller ej.

[309] Jourová, V. (januar 2016). Reformen af EU's databeskyttelsesregler og big data. Hentet fra http://ec.europa.eu: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41558, s. 1 (tilgået 17/04/2018).

3.4.1.1 Virksomhedernes behov for en DPO

Som Peter Blume understreger i bogen *Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680*, er der to primære argumenter for, at DPO'er er at foretrække for den dataansvarlige databehandleren og Datatilsynet. Den ene er, at "*(...) [m]ange former for persondatabehandling er kompleks og kan i det daglige være vanskelig at overskue for den dataansvarlige og undertiden ligeledes for databehandleren.*". Dette er et argument, der udtrykker selskabets behov for at blive *compliant*. Derudover har Datatilsynet en yderligere interesse i, at selskaberne hyrer DPO'er, da det "*(...) kan være svært at vide, hvad der egentlig foregår på (...) gulvet, og om de forskellige regler faktisk bliver overholdt."*.[310] Hermed er det argument for, at Datatilsynet får hjælp til at holde øje med virksomhederne.

Ifølge Datatilsynets *Vejledning om databeskyttelsesrådgivere*[311] er ansættelsen af DPO'er et udtryk for ansvarlighed ift. at efterleve Forordningen. Dermed er DPO'ens rolle relevant ift. at etablere et gensidigt forhold mellem borgeren og virksomheden, og rollen fungerer derfor også som et kvalitetsstempel for virksomheden. "*Arbeidet med personvern* [DPO red.] *er en del av en bedrifts compliance-arbeid, eller etterlevelse av lover og regler (...). Fokus på dette arbeidet i alle ledd er et sentralt kvalitetsstempel i et marked hvor det er viktig å knytte til seg samarbeidspartnere som vekker tillit og som fremstår ryddige*"[312].

3.4.1.1.1 Mindre transaktionsomkostninger ved DPO

Ansættelse af DPO'en giver mulighed for at spare ressourcer. Dette gøres ved, at selskabet har én person, som de ansatte kan gå til, hvis de har persondataretlige spørgsmål. Dette betyder, at hver person eller afdeling ikke vil have behov for en juridisk person ansat, som kender til feltet. Denne tilgang er benyttet i Tyskland, hvor virksomheder giver udtryk for, at de er glade for denne uddelegering af et stort problematisk område til én ekspert.[313]

---

[310] Blume, P. (2016). Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680. København: Jurist- og Økonomforbundets Forlag, s. 128.
[311] Datatilsynets hjemmeside. (December 2017). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf, (tilgået 21/04/2018).
[312] Citat: Korsnes, R. (4. april 2017). DERFOR BØR DU VÆRE OPPTATT AV AT INKASSOSELSKAPET DITT HAR ET PERSONVERNOMBUD. Hentet fra http://blogg.intrum.no: http://blogg.intrum.no/derfor-bor-du-vare-opptatt-av-at-inkassoselskapet-ditt-har-et-personvernombud, (tilgået 24/04/2018) som skrives af en af Norges ledende leverandører af faktura og inkassotjenester (www.intrum.no).
[313] Meyer, D. (6. Juni 2016). What will mandatory DPOs look like under the GDPR? Germany could tell you. The Privacy Advisor. Se mere i afsnit "*DPO-rollen før direktivets ikrafttræden (Den Tyske Model)*" i dette speciale.

Af ovenstående begrundelser kræver Forordningen, at organisationer i EU initierer DPO'er, hvis betingelserne i artikel 37 er opfyldt.

3.4.1.2 Principal-agent-teori

Afsnittet *Theory of the Firm* på side 93 berørte denne teori, men dette principal-agent-afsnit uddyber DPO'ens incitament til at arbejde tilfredsstillende som DPO. DPO'en er vigtig for at Forordningen fungerer tilstrækkeligt, og derfor skal der opstilles en aflønningsstruktur, som er fordelagtig og skaber incitament for at udføre DPO-arbejdet bedst muligt. Som udgangspunkt er det arbejdsgiveren på arbejdspladsen, der er principalen, og DPO'en der er agenten. Relationen mellem parterne eksisterer, når;

- der er mindst to individer med økonomisk relation,
- det er agenten, der vælger mellem de eksisterende alternativer,
- agentens handling påvirker principalens adfærd, og
- agentens belønning fastsættes af principalen før forholdet påbegyndes, men under påvirkning af agentens markedsmuligheder.[314]

3.4.1.2.1 Nytten ved en motiveret DPO

Der er mange elementer i at vurdere, hvornår en DPO neoøkonomisk vil yde sit bedste. Hele argumentationen tager udgangspunkt i følgende variable:

Subjektet	**Intern DPO**	**Ekstern DPO**
DPO'en	Bedre mulighed for nytteoptimering. Svært at vise sit værd og få lønforhøjelse.	Bedre vidensdeling, når DPO'en kommer fra et DPO-hus. Dette gør også, at DPO'en bliver mere kompetent, og får flere kontakter. Når DPO'en bliver mere kompetent stiger timesatsen. Når DPO'en er mere kompetent, vil der være mulighed for at få øget ansvar. Selskaber stoler løbene mere på en DPO, der bliver bedre med tiden. Til sidst får DPO'en mulighed for at undervise og skifte mellem DPO-huse efter bedste vilkår. DPO'en kan ende med at blive partner.
Selskabet	Risiko for *Moral Hazard.* Altid en DPO tæt på.	Altid adgang til dygtig DPO, som har bagland og lyst til at gøre sit bedste.
DPO-huset	*N/A*	DPO-huset bliver løbende bedre, når miljøet er bedre. Dertil vil der vindes flere klienter.

315

[314] Bogen *Elm-Larsen, R. (2013). Forvaltningsrevision: begreb, teori og proces (3. udg.). Samfundslitteratur*, s. 186, kommenterer Arrow, Kenneth J, *Agency and Market*.

Efter ovenstående gennemgang af nytteafvejninger er nedenstående spilmatriks udformet. Matriksen viser, at nash-ligevægtene findes, hvor DPO'en kan vælge at gøre sin klient 1) meget meget *compliant*, 2) lidt *compliant* eller 3) slet ikke *compliant* overfor Forordningen:

Matriks over langsigtet nytte for hhv. selskabet, der har brug for en DPO, og selve DPO'en.

Selskabet / DPO	**Yder stor *compliance***	**Yder lille *compliance***	**Yder ingen *compliance***
Hyrer intern DPO	*7 , 5*	**5 , 6**	*-5 , 4*
Hyrer ekstern DPO	**7 , 6**	*5, 3*	*-2 , 2*

Ud fra ovenstående er der argumenteret for, at det kan betale sig at hyre en ekstern DPO, da $(7{,}6 =)13 > (5{,}6 =)11$. Dette skyldes især, at selskabet har svært ved at styre og monitorere DPO'en, da det ikke er andre ansættes fagspecifikke kompetence. Derfor bliver denne opgave allokeret ud fra DPO-huset, som har lettere ved at give et incitament, der består i, at DPO'en gør sit bedste. For den interne DPO kommer der først en konsekvens, den dag Datatilsynet kontrollerer selskabet.

3.4.1.3 Certificering af DPO'en

3.4.1.3.1 Kvalifikationen for at være DPO

Forordningen beskriver DPO'ens kunnen som værende *fagligt kvalificeret* med *ekspertise indenfor databeskyttelsesret og -praksis* samt med *evnen til at udføre de konkrete opgaver, der står i artikel 39 i Forordningen*.[316] Dermed stilles der ikke krav om en bestemt uddannelse eller certificering for at optræde som DPO for en virksomhed.[317] Dog mener andre, at "*(...) the DPO should be a senior data protection lawyer (...)*"[318] for at kunne leve op til kravene udtrykt i artikel 37, stk. 6 og artikel 39 i Forordningen. Dertil nævner artiklen (af Eric Lachaud) et behov for en erfaren *project manager*, da DPO'en skal kunne træne og auditere virksomheden.[319] Med andre ord synes formuleringerne for DPO'ens kvalifikationer

[315] Matriksen er blevet til på baggrund af: Barnes, A. H. (u.d.). The "Dark Side" of Going In House. (BCG Attorney Search) Hentet fra https://careers.findlaw.com: https://careers.findlaw.com/legal-career-options/the-dark-side-of-going-in-house.html (tilgået 26/03/2018).
[316] Artikel 37, stk. 5 i Forordningen.
[317] Karnovs note 251 til Forordningen: Europa-Parlamentets og Rådets forordning af 2016-04-27. (KARNOV) Hentet fra https://pro.karnovgroup.dk: https://pro.karnovgroup.dk/document/7000751611/6#EUFOR2016679_NKAR251 (tilgået 28/03/2018).
[318] Lachaud, E. (2014). Should the DPO be certified? International Data Privacy Law, 4(3), s. 192.
[319] Datatilsynets hjemmeside. (December 2017). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf, s. 23, (tilgået 28/03/2018).

ikke at være direkte konkrete. Derfor bliver det ved den givne situation, der skal vurderes, om en hyret DPO er tilstrækkeligt kvalificeret.

For at de bedste DPO'er bliver ansat, valgte Tyskland at etablere muligheden for at udstede bøder på op til 50.000 euro[320] under Direktivet, hvis der ansættes en DPO uden de nødvendige ukonkrete kvalifikationer.[321] I medlemsstaten Luxembourg er implementeret reelle *objektive* uddannelseskrav, der beskriver, hvornår en DPO er kvalificeret til at udøve erhvervet.[322]

3.4.1.3.2 Fordele ved certificeringer

Det bliver en stor udfordring for Datatilsynet at tage rundt i Danmark for at undersøge, hvorvidt virksomheder overholder Forordningen. Derfor kan certificeringer af DPO'erne være med til at gøre, at virksomhederne i større omfang overholder Forordningen.[323] Af andre relevante fordele nævnes:

1) Større konform fortolkning af den komplekse Forordning.
2) Mindre asymmetrisk information mellem DPO'en og selskabet.[324]

---

[320] BAMBERGER, K. A., & MULLIGAN, D. K. (2013). Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. George Washington Law Review, 81(5), s. 1576.
Bøden bliver dog meget sjældent udstedt. Citat fra s. 1576: "*If a noncompliant company has at least gone through the ritual of appointing an internal privacy officer-even if it is found to be guilty of privacy abuse-it is extremely unlikely that a punishment will ensue*."

[321] Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814), Section 4f, subsection 2: DPO'en i Tyskland skal "*(...) fulfill several legal, technical and organizational qualifications (...)*". Kilde: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html (tilgået 17/04/2018).
Dette indebærer krav om at have stor viden indenfor databeskyttelsesloven, generel institutionelle love og at være bevidst om de juridiske aktiviteter, der er forbundet med DPO'ens arbejde.

[322] Artikel 40.7, 40.8 and 40.9 i the Data Protection Law of 2th of August 2002 https://cnpd.public.lu/content/dam/cnpd/fr/legislation/droit-lux/doc_loi02082002_en.pdf, (tilgået 17/04/2018). Citat: "*Approval for the activity of data protection official will be subject to proof of completion of university studies in law, economics, commercial management, natural science or information technology*".

[323] Det har været svært for Tysklands Datatilsyn at undersøge *compliance*-niveauet for alle virksomheder og dertil DPO'ernes baggrund. Derfor er certificeringen af DPO'er med til at gøre Datatilsynets arbejde mere komplet. Kilde: Lachaud, E. (2014). Should the DPO be certified? International Data Privacy Law, 4(3), s. 193.
På trods af dette tydeliggør *Vejledningen om databeskyttelsesrådgivere* s. 5, at DPO'en hverken optræder som en del af eller optræder som repræsentant for Datatilsynet, men rollen skal forstås som et kontaktled mellem virksomheden og Datatilsynet. Kilde: Datatilsynets hjemmeside. (December 2017). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf, (tilgået 21/04/2018).

[324] Michael Spences *Job Market Signaling* er økonomisk kontraktteori, der bygger på at minimere principalens asymmetrisk viden om agenten i et potentielt ansættelsesforhold. På denne måde differentierer agenten sig fra andre agenter, da certificeringen viser en hvis kvalifikation, og samtidig ved principalen, at agenten har kvalifikationer (undgår *moral hazards*). Spence, A. M. (1974). Market Signaling, Information Transfer in Hiring and Related Processes. *Harvard University Press*.

3) Virksomheden har et statsautoriseret bevis på deres *compliance.* Dette mindsker en potentiel bøde/sanktion fra Datatilsynet.
4) Der er mulighed for at monitorere niveauet af *compliance*, som gør det nemmere at fastholde certificeringen på sigt.[325]

Certificeringen er derfor med til at ensrette de produkter og ydelser, som findes på det meget udviklende og innovative marked, og derfor bliver DPO'ernes arbejde over tid mere vertificeret[326] og hermed tillidsskabende mellem virksomheden og borgeren.

3.4.1.3.3 "Minimums-DPO'er"

Der er to årsager til, at organisationer har incitament til at ansætte minimalt kvalificerede DPO'er:

1) Der er en risiko for, at selskaberne i god tro hyrer DPO'er, som ikke er kvalificerede til at varetage deres rolle, og
2) modsat kan selskaberne i ond tro hyre DPO'er, som kun sikrer en minimums-*compliance*.

Begge scenarier er ikke at ønske for EU, da dette minimerer de positive effekter ved Forordningen. Ud fra inticamentsteorien nævnt på side 98 er det som udgangspunkt kun de potentielle bøder, som neoøkonomisk kan sikre, at Forordningen bliver overholdt til fulde. Dette garanterer ikke, at selskaberne hyrer de bedste DPO'er, da;

1) de er dyrere, og
2) de udfordrer, hvordan ledelsen styrer virksomheden.

Det forventes derfor, at en "billigere" DPO, som ikke stiller kritiske spørgsmål og sikrer minimums-*compliance*, vil have en vis interesse for virksomheder.

Det er derudover svært at lokalisere tærskelværdierne for, hvornår en DPO ikke udfører sit erhverv tilstrækkeligt efter Forordningen. Ligeledes er der tale om et arbejdsgiverforhold, hvor DPO'en er beskyttet under Danske Lov 3-19-2. Derfor er arbejdsgiveren ansvarlig for DPO'ens fejl, men principalen har svært ved at vide, hvornår arbejdet er rigtigt udført. Samtidigt må principalen kun fyre DPO'en, hvis denne ikke udfører sit arbejde. Monitorering af den ansatte DPO er derfor svært at udføre af principalen.

Alle ovenstående tre argumenter er med til at understrege, at *compliance*-niveauet er op til den enkelte virksomheds politik.

[325] Lachaud, E. (2014). Should the DPO be certified? International Data Privacy Law, 4(3), s. 194.
[326] Graz, J. C., & Hartmann, E. (2010). Global regulation of the knowledge-based economy: The rise of standards in educational services. Université de Lausanne Institut d'Etudes Politiques et Internationales, s. 16.

På trods af at der (ifølge Datatilsynets vejledning om databeskyttelsesrådgivere) ikke kræves certificering af DPO'er[327], findes talrige private advokat og konsulenthuset, der tilbyder certificeringer. Dette peger i retning af, at markedet selv kræver certificering af DPO'en, og at der derfor ikke kræves en regulativ indblanding på området.

Statslige certificeringer er med til at;

1) demonstrere DPO'ens kompetencer,
2) virksomheden har argumenter for, at den har handlet *compliant* ved at have hyret en certificeret DPO, og
3) Datatilsynet får bedre overblik over DPO'ernes kompetencer, så de ikke behøver at baggrundstjekke dem.[328]

EU har før argumenteret imod EU-certificeringer og EU-*trustmarks*, da;

1) det er dyrt (EU har vurderet, det koster over 1 mio. € pr. stat pr. år),
2) certificeringer kræver, at der ikke sker fejl, ellers mister certificeringen værdi,
3) det er historisk set kun EU, der bliver påvirket af EU-certificeringer, og dermed opnås der ingen global gevinst,
4) hvis alle alligevel får certificeringen, står alle parter som før certificeringskravet, og
5) små spillere, der ikke har råd til certificerede ansatte, vil blive afholdt fra at indtræde på markedet.[329]

På trods af ovenstående positive og negative argumenter ved certificeringer benytter EU historisk set ofte certificeringer, da det er et alternativ til, at det offentlige skal gå ind og holde øje med alle, som er omfattet af regulering.[330] Der er dog vigtigt at understrege to ting:

1) Der kan realistisk set ikke lovgives ud af lovbrud. EU kan kun straffe dem, der bryder loven, og dette skaber blot incitamentet til at overholde loven, og
2) certificeringer er en hjælp til loven, men den kan ikke erstatte loven. Især da der opstår risikoen for, at private certificeringsudbydere bestemmer fortolkningen.[331]

Hvis EU anerkender private certificeringer, anerkendes også den hurtige udvikling indenfor IT. Hermed anerkender de ligeledes de offentlige videregående uddannelsers mangel på at følge med teknologien. Dette skyldes, der ikke findes statslige kurser, der direkte kan bruges

[327] Datatilsynets hjemmeside. (December 2017). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf, (tilgået 28/03/2018).
[328] Lachaud, E. (2014). Should the DPO be certified? International Data Privacy Law, 4(3), s. 195.
[329] Alleweldt, F., & Senda, K. (2012). Directorate-general for internal policies. Hentet fra http://www.europarl.europa.eu: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492433/IPOL-IMCO_ET(2012)492433_EN.pdf, s. 71-74, (tilgået 28/03/2018).
[330] Bokhorst, A. M. (2010). Effectiveness of certification and accreditation as a public policy instrument in the Netherlands. ECPR conference in Reykjavik, s. 3.
[331] Lachaud, E. (2014). Should the DPO be certified? International Data Privacy Law, 4(3), s. 205.

som DPO i Forordningen.[332] Derfor er det behov for øget viden på området, da anerkendelsen eller underkendelsen har konsekvenser for EU.

3.5 Diskussion

3.5.1 Offentlige samkøring af persondata

I dag opbevarer stater, kommuner og virksomheder store mængder persondata om borgerne. Danmarks suppleringslov til Forordningen lægger op til, at offentlige instanser må dele persondata imellem hinanden. Rent praktisk har de færreste givet tilladelse til dette, og rent juridisk er det uafklaret, hvem der reelt ejer denne data. Både offentlige og private organisationer agerer, som om de ejer dataen, og dette skaber et stort netværk af *Big Data*.[333] Forordningen er med til at skabe bevidsthed om, hvem ejeren af en borgers data er.

Tilhængere af *Big Data* har udtrykt: "*Registerdata er et samfundsmæssigt gode, og forskningen skaber viden til samfundets fælles bedste. En vigtig forudsætning for den danske data-revolution er, at Danmark et af de lande i verden, hvor borgerne har størst tillid til hinanden, til virksomheder og til det offentlige.*".[334] Dertil skal "*(...) samarbejde mellem offentlige styrelser, universitetseksperter og teknologivirksomheder (...) løse alt fra at forudsige oversvømmelser og skabe enklere patientgange til bedre individuel undervisning og mindre administrativt besvær for virksomhederne.*"[335] Det er dog besværligt under Direktivet at køre data sammen på tværs af instanser, og dette skaber inefficiens ifølge kilderne. Besværligheden kommer af persondataloven, som ikke tillader denne samkøring. Et direkte eksempel er, at Region Sjælland ville kunne forudsige kroniske sygdomme med over 80 % præcision, hvis data mellem sygehusdata og kommunedata måtte køres sammen. Horsens Regionshospitals forskningsprogram *Tværspor*, fokuserer netop på datamulighederne inden for sundhedssektoren.[336] Dette understøtter de uanede muligheder, som data kan bruges til.

[332] Lachaud, E. (2014). Should the DPO be certified? International Data Privacy Law, 4(3), s. 194.
[333] Citat: Ingeniørforeningen, I. (u.d.). Big data – privacy og vækst. Hentet fra https://ida.dk: https://ida.dk/sites/default/files/big_data_-_privacy_og_vaekst.pdf, (tilgået 10/04/2018).
[334] Sørensen, T. Ø., Elmeskov, J., & Lebech, A. (2015). Big data til gavn for vækst og velfærd – en unik dansk mulighed. Hentet fra http://samf.ku.dk: http://samf.ku.dk/presse/kronikker-og-debat/big-data-konference/, (tilgået) 10/04.2018
[335] Citat: Breinstrup, T. (2016). Superdataknusere skal skabe guld sammen. Hentet fra https://www.business.dk: https://www.business.dk/digital/superdataknusere-skal-skabe-guld-sammen, (tilgået 10/04/2018).
[336] Horsens, R. (u.d.). Forskningsprogram TVÆRSPOR. Hentet fra http://www.regionshospitalet-horsens.dk: http://www.regionshospitalet-horsens.dk/siteassets/om-os/virksomhedsgrundlag/forskningsprogram-tvarspor.pdf, (tilgået 10/04/2018).

Spørgsmålet opstår, om det er i borgernes interesse, at personfølsom data køres sammen. Der er mange økonomiske argumenter for, at dataen skal deles, mens argumenterne imod typisk går på etik og moral. Udlægget fra Region Sjælland blev kommenteret af 27 personer, hvor langt de fleste er negative tilkendegivelser på opslaget. Dertil er der knapt 9.000 mennesker, der er medlem af gruppen "*Bevar Tavshedspligten - fordi du har ret til fortrolighed hos lægen*" på Facebook. Ligeledes præsenterer Etisk Råd argumenter imod, at borgere bliver stemplet som fremtidige kriminelle på baggrund af en algoritme.[337]

Økonomisk forventede finansloven fra 2017, at investeringen på 100 mio. kr. til at oprette *Nationalt Genom Center* og *NEXT* ville komme igen 1,64 gange på det danske BNP.[338] Dermed er det ikke kun patientens sundhed, der er i betragtning, men også økonomiske effekter som nye arbejdspladser og øget BNP ved datadeling mellem instanser. Fx giver Styrelsen for Dataforsyning og Effektivisering "*(...) mulighed for, at både det offentlige og det private kan bruge data til at understøtte deres arbejde eller skabe helt nye forretningsområder"*.[339]

Når det kommer til patientsikkerhed og samkøring af personlig følsom helbredsdata, er der klare argumenter både for og imod. Der er en naturlig tendens til, at jo mere personligt dataen bliver, jo flere protester forekommer der. Som analyseret på side 88 og frem er problemet, at det som udgangspunkt *ikke* er borgerne, der er skyld i deres tab på markedet. Det er virksomhederne, der udnytter borgerne. Derfor er det som udgangspunkt beslutningstagerne (politikerne), der afgør, om (helbreds-)dataen skal køres sammen på tværs af (inter-)nationale enheder.

Med andre ord bliver modstandsgruppen mod samkøringen holdt udenfor, når den endelige beslutning skal tages, da der er økonomiske og samfundsmæssige efficienter, som overtrumfer de moralske og etiske argumenter.

[337] Råd, D. E. (2017). Debatdag om fremtidens sundhedsvæsen, big data og wearables. Hentet fra http://www.etiskraad.dk: http://www.etiskraad.dk/etiske-temaer/sundhedsdata/fremtidens-sundhedsvaesen-big-data-og-wearables, (tilgået 10/04/2018).
[338] Jervelund, C., Brenøe, S., & Kirk, A. R. (2017). NEXT Partnership, Lægemiddelindustriforeningen. Hentet fra Værdien af kliniske forsøg i Danmark: https://biopeople.eu/fileadmin/user_upload/Editor/Rapport_Vaerdien-af-kliniske-forsoeg-i-Danmark.pdf, (tilgået 10/04/2018).
[339] Citat: Styrelsen for Dataforsyning og Effektiviseringens hjemmeside. (u.d.). Hentet fra http://sdfe.dk: http://sdfe.dk/data-skaber-vaerdi/en-bedre-og-hurtigere-offentlig-sektor/, (tilgået 10/04/2018).

3.5.2 Compliance-niveau for virksomheder og myndigheder

Ovenstående analyser giver anledning til at vurdere, hvor *compliant* det kan betale sig for virksomheder og myndigheder at være. Det er tydeliggjort, at der opstår efficiens ved at implementere Forordningen, og ligeledes at DPO'er skaber værdi. DPO'er er dog en stor udgift at have i organisationer og virksomheder, og derfor er der argumenter for, at de kun skal ansættes, når der er tale om bestemte typer organisationer. Dette er årsagen til, at der reelt kan være et tab af nytte, hvis alle organisationer skal hyre DPO'er. Art. 37 i Forordningen (om hvornår der skal udpeges en DPO) er med til at gøre markedet for virksomheder og organisationer, der beskæftiger sig med persondata, mere efficient. Der er ikke forventning fra EU eller borgernes side om, at organisationer, der fx ikke beskæftiger sig med følsom persondata, skal hyre en DPO. Derfor lægger Forordningen op til nash-ligevægt i det punkt, hvor Forordningen overholdes, og DPO'en ansættes i tilfælde af de art. 37 gældende grunde. Dette skitseres nedenfor.

Borgerens og samfundets nytte ved handel

Borger / samfund	**Ingen Forordning**	**Forordning**	**Forordning og DPO efter behov**	**Forordning og altid DPO**
Handle	*5 , 5*	*7 , 6*	***9 , 7***	*6 , 6*
Ikke handle	*0 , 0*	*0 , -3*	*0 , -4*	*0 , -5*

Denne løsning giver den højeste værdi for parterne (9,7).

3.6 Delkonklusion

Delspørgsmål: Er Forordningen økonomisk efficient ud fra en nytteteoretisk tilgang, og under hvilke omstændigheder kan DPO'en bedst påvirke den mulige efficiens?

Der er bevist flere negative konsekvenser ved, at Forordningen implementeres. Dette er fx de store udgifter, som organisationer er tvunget til at afholde for at blive *compliant* med reglerne. Mikroøkonomisk er det vist, at dette som udgangspunkt påvirker markedet negativt, da færre borgere har råd til ydelser, hvis prisen følgeligt sættes op. Det er dog samtidigt vist, at Forordningen reelt ændrer dataansvarliges holdning til persondata, og derfor får borgerne totalt set en større nytte ud af Forordningen, da efterspørgslen påvirkes positivt. Af denne årsag er der behov for, at Forordningen opfyldes i størst muligt omfang af organisationerne, der behandler borgernes persondata. Ellers giver Forordningen mere tab end overskud på det europæiske marked. Databeskyttelsesrådgiveren (DPO'en) er et vigtigt element for at få *compliance*-niveauet hævet tilstrækkeligt. Derfor vil de organisationer, hvor

en DPO er påkrævet, være nødt til at hyre DPO'er, som sikrer en maksimal overholdelse af Forordningen, og en størst mulig efficiens på det europæiske økonomiske marked. Spilteoretisk principal/agent-teori har vist, at eksterne DPO'er udviser større interesse i at gøre organisationen mere *compliant* end interne.

Kapitel 4 - integreret analyse

4.1 Indledning - retstilstanden under Forordningen

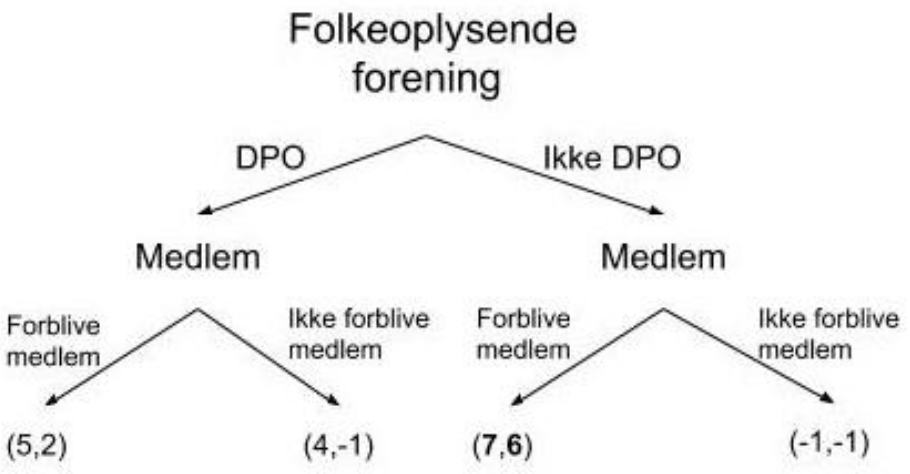
Det er vist i de foregående kapitler, at folkeoplysende spejderforeninger ikke er forpligtet til at udpege en DPO efter art. 37. Ud fra de økonomiske betragtninger, der er gjort i kapitel 3, er denne retsfølge efficient. Med dette menes, at Forordningen er efficient, så længe databehandlere med øget risiko for misbrug af persondata overholder Forordningen. På dette grundlag er det i princippet de dataansvarlige, der (via deres overholdelse af Forordningen) generer den nytteefficiens, der udspringer af Forordningen. Nytten er derfor en funktion af det *compliance*-niveau, der samlet set bliver udført af de dataansvarlige. Her spiller DPO'en en vigtig rolle, idet det er denne, der skal rådgive den dataansvarlige, således at Forordningen bliver overholdt. Dermed er den dataansvarliges *compliance*-niveau afhængig af DPO'ens indsats, og den samlede nytte fra Forordningen er afhængig af *compliance*-niveauet hos de dataansvarlige.

Baseret på den retsdogmatiske analyse må det ligeså gælde, at foreninger der opfylder folkeoplysningsloven heller ikke vil være forpligtet til at udpege en DPO i de fleste tilfælde.

På trods af at dette behandler de folkeoplysende foreninger persondata i forbindelse med deres virke. Jo flere medlemmer den folkeoplysende forening har, jo mere data behandles der i foreningen. Grundet Forordningens art. 37 kan de folkeoplysende foreninger i realiteten have et ubegrænset antal medlemmer, uden at de skal udpege en DPO. Dette skyldes som tidligere nævnt, at foreningerne ikke er at betragte som offentlige myndigheder eller organer efter art. 37, stk. 1, litra a), og at deres kerneaktivitet ikke er persondatabehandling efter de kumulative betingelser i litra b-c).

Da der ikke skal ansættes en DPO, er der mindre beskyttelse af medlemmernes persondata. Det er vist i specialets økonomiske kapitel, at borgerne bekymrer sig om deres persondata, men ønsket om at være social opvejer som udgangspunkt dette nyttetab. Dette var princippet fra *The privacy paradox.* På nuværende tidspunkt bekymrer borgere sig ikke tilstrækkeligt om misbrug af deres data, til at de finder det nødvendigt, at en forening har en DPO.

Ovenstående scenarie vil blive belyst spilteoretisk i det nedenstående spiltræ. Her afspejles data-subjekternes og foreningernes reaktioner, baseret på at medlemmerne ikke bekymrer sig.



[340]

Spiltræ hvor data-subjekterne ikke bekymrer sig om deres data.

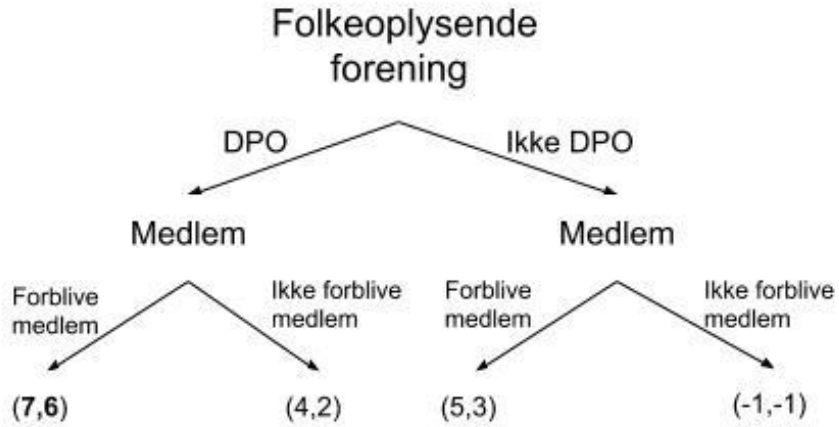
Ovenstående spiltræ viser, at den totale nytte for samfundet er $(7 + 6 =)$ 13, da data-subjekterne fortsat vil tilmelde sig eller forblive tilmeldt i en forening. Dette skyldes, at de har tillid til foreningen, og at denne passer tilstrækkeligt på persondataen uden en DPO.

Det er modsætningsvist belyst i specialet, at frygten for misbrug af persondata intensiveres. Dette betyder, at nytten ved at være medlem i en folkeoplysende forening på sigt vil blive overgået af data-subjekternes mistillid og frygt for misbrug af persondata.

På trods af at en folkeoplysende forening ikke har samme incitament som en global virksomhed til at misbruge data-subjekternes data, er der stadig et voksende behov for beskyttelse af persondataen. I takt med at foreningernes medlemstal stiger, behandles der mere og mere persondata. Data-subjekterne kan derfor ende med en øget mistillid til, at foreningerne ikke kan håndtere persondataen på en tilstrækkelig måde, der fx sikrer dataen mod lækage og hackerangreb. Begge eksponerer alle data-subjekternes persondata.

Nedenfor vises scenariet, hvor medlemmerne er mere mistroiske overfor foreningernes måde, de håndterer persondataen på. Hermed er der større krav til den enkelte forening, og derfor ændres ligevægten:

[340] Spiltræerne er udarbejdet af forfatterne.



Spiltræ hvor data-subjekterne bekymrer sig om deres data.

Hvis foreningen ikke udpeger en DPO, vil den forventede nytte for samfundet være $(5 + 3 =)$ 8, hvorimod der er $(7 + 6 =)$ 13 i samfundsnytte, hvis foreningen udpegede en DPO.

Hvis udviklingen mellem de to spiltræer fortsætter, så data-subjekterne ønsker mere og mere persondatabeskyttelse, vil det påvirke foreningssamfundet, hvis DPO'en ikke bliver udpeget. Dette skyldes, at medlemmerne melder sig ud.

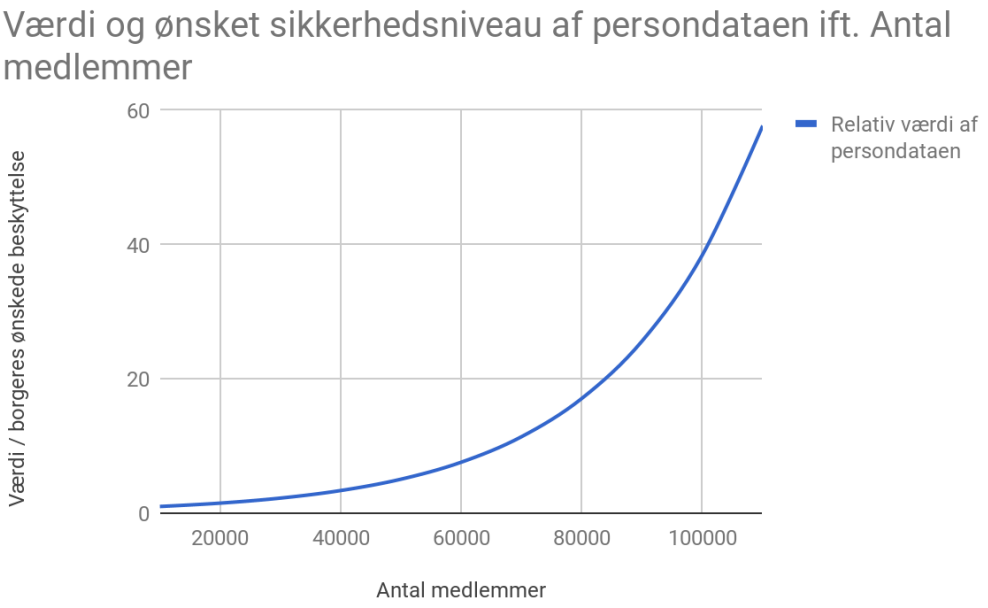
Hvis data-subjekterne mister tilliden til de folkeoplysende foreninger, vil de ikke kunne nyde godt af de aktiviteter, som foreningerne udbyder. Dermed bliver samfundsnytten, der udspringer fra Forordningen, påvirket negativt. Således vil de folkeoplysende foreninger komme til at påvirke nytteefficiensen af Forordningen negativt.

Der skal udledes med ovenstående, at det er vigtigt, at folkeoplysende foreninger følger med deres medlemmers databeskyttelsesbehov, så de ikke melder sig ud. Den dag medlemmerne gerne vil have mere beskyttelse af deres persondata, må foreningerne deraf udpege en DPO, så de ikke mister medlemmer, og samfundets nytteefficiens falder. Hvis foreningerne ikke formår at følge med dette behov, må lovgiver gå ind og sikre, at dette sker.

4.2 Hvordan lovgivningen bør udformes - *de lege ferenda*

Folkeoplysende foreninger vil i de fleste tilfælde være undtaget fra at udpege en DPO. Dette er nødvendigvis ikke altid samfundsefficient som vist med ovenstående spiltræer. Derfor foreslås der, at udlede en måde hvor de folkeoplysende foreninger kan blive omfattet af kravet om udpegelse af DPO, selvom persondatabehandlingen ikke er kerneaktiviteten.

Det er bevist i det økonomiske kapitel, at værdien (og borgernes ønske om sikker behandling) af persondata stiger i takt med, at medlemstallet i en forening øges. Grafisk vises dette som:



[341]

Graf, der viser værdien af persondata, og hvor meget sikkerhed medlemmerne ønsker, når medlemstallet stiger.

Under Forordningen er der ingen forskel på, om folkeoplysende foreninger skal udpege en DPO ved få eller mange medlemmer. Hermed forbliver sikkerhedsniveauet det samme. At dette databeskyttelsesniveau ikke stiger i takt med mængden af konsolideret persondata, kan vise sig at blive problematisk. Dette skyldes særligt, at dataens værdi stiger eksponentielt i takt med mængden. Problematikken ligger i, at folkeoplysende foreninger kan ende med så meget data, at det vil skabe mistillid til Forordningen faktiske virke, hvis der sker misbrug af persondataen. I de tilfælde, hvor der behandles persondata i meget stort omfang, burde det derfor objektivt set være uundgåeligt ikke at udpege en DPO - også selvom det ikke er kerneaktiviteten at behandle persondata.

Det vil være relevant at foreslå en ændring af Forordningen som følgende:

Der foreslås, at Forordningens art. 37, stk. 1, litra b) ændres, således at betingelsernes kumulativitet genovervejes, når medlemstallet er i tilpas stort omfang. Det vil med forslaget være obligatorisk at udpege en DPO, hvis medlemstallet er stort nok, og hvis blot betingelse

[341] Grafen er udarbejdet af forfatterne.

1 (om kerneaktivitet) eller 2 (regelmæssigt og systematisk) er opfyldt i Forordningens art. 37, stk. 1, litra b).

Hermed skal den dataansvarlige stadig udpege en DPO, når;

1) alle tre betingelser er opfyldt (som under Forordningen),

og når der behandles tilpas stort omfang af persondata (både som bi- eller kerneaktivitet). Dette er, når blot ét af følgende to scenarier er tilfældet:

2) Når betingelserne om *i stort omfang* og *regelmæssig* og *systematisk overvågning* er opfyldt, eller
3) når betingelserne om *i stort omfang* og *kerneaktivitet* er opfyldt.

Dette vises nedenfor grafisk, at hvis antallet af medlemmer overskrider et bestemt antal, vil tærsklen for blot to betingelser ligeledes blive overskredet. Når tærskelværdien er under den fiktive værdi 40, skal alle tre betingelser være opfyldt (scenarie 1), og hvis værdien er over 40 skal blot scenarie 2 eller 3 være opfyldt.

342

4.3 Derfor kan ændringen føre til øget samfundsefficiens

Ved at foretage en sådan en ændring i reguleringen, kan de større folkeoplysende foreninger blive underlagt kravet om udpegelsen af en DPO. En DPO skal netop udpeges på

342 Grafen er udarbejdet af forfatterne.

baggrund af dennes kendskab til overholdelse af Forordningen baseret på de behandlingsaktiviteter, der foretages hos den dataansvarlige (i dette tilfælde de folkeoplysende foreninger). Ved at de folkeoplysende foreninger bliver pålagt ved lov at udpege en DPO, når de kommer op og behandler en tilpas stor mængde persondata, vil data-subjekternes tillid til foreningerne stige, og dermed stiger nytteefficiensen af Forordningen også. Dermed er ovenstående retspolitiske forslag en samfundsefficient forbedring af den retstilstand, der kommer ved Forordningens ikrafttræden.

4.4 Kritisk syn på det retspolitiske forslag

Grundet Forordningens nuværende udviklingstrin er særligt betingelsen om behandling af persondata i "*stort omfang*" svær at definere. Dermed også hvilke folkeoplysende foreninger der opfylder dette krav. Dette vil skulle blive udviklet via retspraksis, da det ligeledes kan være forskelligt fra foreningernes aktiviteter og geografiske placering.

Medlemsstaterne kan opnå samme retspolitiske forslag ved at udarbejde art. 37, stk. 4 i en national suppleringslov. Som nævnt på side 56 hjemler denne artikel, at staterne selv kan opsætte yderligere krav for, hvornår der skal udpege en DPO.

4.5 Afsluttende bemærkninger

Det skal huskes, at det økonomiske kapitels analyse om *compliance*-niveauet hos interne og eksterne DPO'er ligeledes skal tages i betragtning i det integrerede kapitel. Hvis den folkeoplysende forening har så mange medlemmer, at den skal udpege en DPO, vil det stadig være bedst for Forordningens virke, hvis der udpeges en ekstern DPO. Den interne DPO udviser stadig *compliance*, men den eksterne har størst incitament til at gøre foreningen mest *compliant*.

4.6 Delkonklusion

Delspørgsmål: Hvorledes er det muligt at ændre Forordningens art. 37 for at gøre Forordningens økonomiske udledninger mere efficiente?

Der konkluderes, at det vil være fordelagtigt for samfundsværdien af Forordningen, hvis medlemmerne af folkeoplysende foreninger altid har interesse i at være medlem i foreningerne. Dette giver værdi for samfundet. Hvis den store mængde persondata, som der er oplagret i foreningerne bliver lækket, vil borgerne både miste tilliden til foreningen, og

derigennem vil de også miste tilliden til Forordningen. Der foreslås, at hvis en forening har persondata tilstrækkeligt i stort omfang, er det nok, at bare betingelsen *regelmæssigt og systematisk* eller *kerneaktiviteten* er opfyldt, før der skal udpeges en DPO. Herved kan foreningerne alligevel komme til at udpege en DPO, selvom deres kerneaktivitet ikke er behandling af persondata.

Kapitel 5 - konklusion

Dette speciale inkluderer en juridisk analyse, der vurderer om folkeoplysende spejderforeninger er forpligtede til at udpege en DPO efter Forordningens § 37. Det konkluderes at disse foreninger er underlagt Forordningen, og derfor skal Forordningens regler overholdes fuldt ud. Yderligere konkluderes det, at foreningerne hverken er at betragte som offentlige myndigheder eller offentlige organer, eller beskæftiger sig med behandling af persondata som deres kerneaktivitet efter persondataforordningen § 37, stk. 1, litra a-c). Der er heller ingen nationale love, efter Forordningens art. 37, stk. 4, der forpligter spejderforeningerne til at udpege en DPO. Dermed konkluderes det at spejderforeningerne ikke er forpligtet til at udpege en DPO efter Forordningens art. 37.

Økonomisk analyserer specialet, om de økonomiske ulemper vil blive overgået af de positive effekter, som Forordningen bringer med sig. I denne kontekst vurderes, hvad der skal til for at øge de økonomisk positive effekter. Der konkluderes, at Forordningen godt kan skabe mere værdi end tab, da borgernes efterspørgsel på persondatarelaterede produkter og ydelser forhøjes, når Forordningen implementeres. Derfor bliver tabet overskygget af den øgede tillid og købekraft. Alt dette kræver, at Forordningen bliver overholdt i størst muligt omfang. DPO'en er med til at skabe denne øgede værdi, da de sikrer, at organisationer bliver gjort *compliant* med Forordningen. Det er analyseret, at incitamentet for størst mulig *compliance* findes hos de eksterne DPO'er, da de eksterne har spilteoretisk højest nytte i at yde deres bedste.

Da borgernes tillid til at dele deres persondata til organisationer ikke er optimal, er det vigtigt, at borgerne ikke bliver bekræftet i, at organisationer ikke kan finde ud af at håndtere dataen forsvarligt. Dette kunne være ved fx overudnyttelse af data, salg af persondata, succesfyldte *hacker*-angreb o.l. Hvis dette sker, deler borgerne mindre deres data, og dataen er med til at innovere og udvikle Europa. I kontekst mellem personlig datadeling og folkeoplysende spejderforeninger, er det i den integrerede analyse konkluderet, at de kumulative betingelser for hvornår en dataansvarlig skal udpege en DPO (jf. Forordningen art. 37, stk. 1, litra b-c)) er for milde. Under Forordningen kan meget store folkeoplysende spejderforeninger, der ikke beskæftiger sig med persondata som kerneaktivitet aldrig blive forpligtet til at udpege en DPO.

Dette speciale foreslår, at Forordningens art. 37 ændres, således at dataansvarlige, og dermed også folkeoplysende foreninger (deriblandt også spejderforeninger), skal udpege en DPO, når behandlingen af persondata foretages *i stort omfang* og *systematisk og*

regelmæssig eller *som kerneaktiviteten.* Dette betyder, at alle tre betingelser ikke længere behøver at være opfyldt, hvis foreningen er tilstrækkelig stor. Hvis foreningen behandler tilstrækkeligt lidt persondata, vil alle tre betingelser stadig være et krav, før der skal udpeges en DPO efter Forordningen.

Litteraturliste

Bøger

Arrow, K. (1986). *Handbook of Mathematical Economics* (1 udg., Årg. 3).

Blume, P. (2016). *Den nye persondataret - Forordningen 2016/679 om persondatabeskyttelse - Med en omtale af direktiv 2016/680.* København: Jurist- og Økonomforbundets Forlag.

Cabral, L. M. (2000). *Introduction to Industrial Organization.* MIT Press.

Clausen, N. J., Kronborg, A., & Mortensen, B. O. (2017). *Festskrift til Hans Viggo Godsk Pedersen* (1 udg.). Jurist- og Økonomforbundets Forlag.

Dall, N. P., Langemark, J., & Langebæk, A. (2016). *Persondataforordningen - en håndbog for praktikere* (1 udg.). Ex Tuto Publishing.

Eide, E., & Stavang, E. (2008). *Rettsøkonomi* (1. udg.). Olso: CAPELLEN ADADEMISK FORLAG.

Elm-Larsen, R. (2013). *Forvaltningsrevision: begreb, teori og proces* (3. udg.). Samfundslitteratur.

Hansen, S. F., & Krenchel, J. V. (2017). I*ntroduktion til dansk selskabsret II personselskaber, foreninger og fonde* (3 udg.). Karnov Group.

Hasselbalch, O. (2011). *Foreningsret* (4 udg.). Jurist- og Økonomforbundets forlag.

Hendikse, G. (2003). *Economics and Management of Organizations.* McGrawHill.

Høilund, D. (2017). *Persondataret* (1. udg.). Hans og Reitzels Forlag.

Lyck, L. (2008). *Service- og oplevelsesøkonomi i teori og praksis* (1. udg.). Academica.

Neergaard, U., & Nielsen, R. (2010). *EU ret* (6. udg.). København: Karnov Group.

Nielsen, R., & Tvarnø, C. (2014). *Retskilder & Retsteorier.* København: DJØF.

Olsen, B. E., & Sørensen, K. E. (2008). *Europæiseringen af Dansk ret* (1. udg.). Jurist- og Økonomiforbundets forlag.

Smith, A. (1776). *An Inquiry into the Nature and Causes of the Wealth of Nations.* London: W. Strahan and T. Cadell.

Stavang, E., & Eide, E. (2008). *Rettsøkonomi.* Cappelen Damm Akademisk Forlag.

Voigt, P., & Bussche, A. V. (2017). *The EU General Data Protection Regulation (GDPR) - A Practical Guide.* Springer International Publishing AG.

Artikler

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1).

Andrejevic, M. (Januar/Februar 2017). Personal Data: Blind Spot of the “Affective Law of Value”? *Information Society, 1*(31), s. 5-12.

BAMBERGER, K. A., & MULLIGAN, D. K. (2013). Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. *George Washington Law Review, 81*(5).

Bandara, R., Fernando, M., & Aktera, S. (2017). The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance. *Procedia computer science*.

Benchimol, J. (2014). Risk aversion in the Eurozone. *Research in Economics, 68*(1).

Besonko, D., Dranove, D., Shanley, M., & Schaefer, S. (2013). *Economics of Strategy* (6 udg.). Singapore: John Wiley & Sons.

Bokhorst, A. M. (2010). Effectiveness of certification and accreditation as a public policy instrument in the Netherlands. *ECPR conference in Reykjavik*.

Coase, R. (1994). The Firm, the market, and the Law. *University of Chicago Press*.

Coase, R. H. (1937). The Nature of the Firm. *Economica, 4*(16).

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1).

Djolov, G. (2013). The Herfindahl-Hirschman Index as a decision guide to business concentration: A statistical exploration. *Journal of Economic and Social Measurement*.

Epstein, R. A. (2007). The Neoclassical Economics of Consumer Contracts. *Minnesota Law Review*.

Ertl, H., & McCarrell, H. (2002). *The State of Telecommunications Services.* Science, Innovation and Electronic Information.

Fabech, S., & Hopp, M. (6. Marts 2016). Data er det 21. århundredes olie. *Børsen Ledelse*.

Flint, D. (Februar 2016). Computers and Internet What Is the Value of Personal Data? *Business Law Review, 1*(37), s. 38-39.

Garrett, H. (1968). The Tragedy of the Commons. *Journal Science, 162*(3859). Hentet fra http://science.sciencemag.org/content/sci/162/3859/1243.full.pdf

Ghosh, S. (11. April 2018). Mark Zuckerberg's personal notes hint that Facebook isn't ready for GDPR. *Business Insider Nordic*.

Graz, J. C., & Hartmann, E. (2010). Global regulation of the knowledge-based economy: The rise of standards in educational services. *Université de Lausanne Institut d'Etudes Politiques et Internationales*.

Harsanyi, J. C. (1967). Games with incomplete information played by "Bayesian" players, i–iii: part i. the basic model. *Management Science, 14*(3).

Hofacker, C. F., Brudvig, S., Raman, P., Grosso, M., Castaldo, S., & Premazzi, K. (2010). Customer Information Sharing with E-Vendors: The Roles of Incentives and Trust. *International Journal of Electronic Commerce, 14*(3).

Jaffe , J. (11. April 2018). How Facebook is responding to Europe's new GDPR privacy rules. *Cnet*.

Jensen, C. (25. Marts 2018). Hvor længe vil vi passivt se til, mens tech-giganter undergraver samfundet? *Politiken*.

Jeong, S. (11. April 2018). Zuckerberg says Facebook will extend European data protections worldwide — kind of. *The Verge*.

Kerkmeester, H. (2000). METHODOLOGY: GENERAL. *Erasmus University Rotterdam*.

Kim, D.-H., Hettche, M., & Clayton, M. J. (2015). The Privacy Paradox and Calculus Among Millennials: An Empirical Study of Privacy Attitude–Behavior

Congruence. *AMA Marketing & Public Policy Academic Conference Proceedings*(25).

organisering, økonomiske grænser og identitet (1 udg.). Samfundslitteratur.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*.

Kugler, L. (Februar 2018). The War Over the Value of Personal Data. *Communications of the ACM, 2*(61).

Lachaud, E. (2014). Should the DPO be certified? *International Data Privacy Law, 4*(3).

Mandelbrot, B. (1997). *Fractals and Scaling in Finance - Discontinuity, Concentration, Risk.* New york: Springer Publishing .

Meyer, D. (6. Juni 2016). What will mandatory DPOs look like under the GDPR? Germany could tell you. *The Privacy Advisor*.

Meyer, R. (15. April 2015). Europeans Use Google Way, Way More Than Americans Do. *The Atlantic*.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (17. Marts 2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*.

Spence, A. M. (1974). Market Signaling, Information Transfer in Hiring and Related Processes. *Harvard University Press*.

Varian, H. R. (2003). *Intermediate Microeconomics: A Modern Approach* (6. udg.). Norton, W. W. & Company, Inc.

Viscusi, W. K., Harrington, J. E., & Vernon, J. M. (2005). *Economics of Regulation and Antitrust* (4. udg.). Mit Press Ltd.

Voigt, P., & Bussche, A. V. (2017). *The EU General Data Protection Regulation (GDPR) - A Practical Guide.* Springer International Publishing AG.

Wittenstein, J. (20. Marts 2018). Facebook Just Lost More Than Tesla's Entire Market Cap in Two Days. *Bloomberg - Business of Quality* .

Domme

Domme afsagt fra EU-domstolen:

Sag C-119/92
Sag C-113/75
Sag C-222/84
Sag C-230/14

Nationale Domme:

UfR 1969.898V
UfR 2011.2343H

Forordninger

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af

personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

Charter

DEN EUROPÆISKE UNIONS CHARTER OM GRUNDLÆGGENDE RETTIGHEDER (2012/C 326/02)

Direktiver

Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA

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

Love og bekendtgørelser

Nationale love

Lov om behandling af personoplysninger LOV nr 429 af 31/05/2000

Bekendtgørelse af forvaltningsloven LBK nr 433 af 22/04/2014

Bekendtgørelse af lov om social service (LBK nr 102 af 29/01/2018)

Bekendtgørelse af lov om støtte til folkeoplysende voksenundervisning, frivilligt folkeoplysende foreningsarbejde og daghøjskoler samt om Folkeuniversitetet (folkeoplysningsloven) - LBK nr 854 af 11/07/2011.

Meddelelser og vejledninger

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET om udveksling og beskyttelse af personoplysninger i en globaliseret verden.

Pressemeddelelse fra Kommissionen - Et digitalt indre marked i Europa: Kommissionen fastsætter 16 initiativer for at gøre det til en realitet

REPORT FROM THE COMMISSION First report on the implementation of the Data Protection Directive (95/46/EC) Brussels, 15.5.2003 COM(2003) 265 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET - Stærkere beskyttelse, nye muligheder – Kommissionens vejledning om den

direkte anvendelse af den generelle forordning om databeskyttelse fra den 25. maj 2018 - COM(2018)

Retningslinjer for databeskyttelsesrådgivere - WP 243 rev.01 (Dansk version)

Guidelines on Data Protection Officers (*DPOs*) WP 243 rev. 01

Den Europæiske Union, Retningslinjer for vurdering af horisontale fusioner efter Rådets forordning om kontrol med fusioner og virksomhedsovertagelser, Den Europæiske Union, Luxembourg, 2004

U.S. Department of Justice and Federal Trade Commission, Horizontal Merger Guidelines, U.S. Department of Justice and the Federal Trade Commission, Washington DC, 1997 [1992]

Betænkninger

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning Betænkning nr. 1565.

Registerudvalgets betænkning 1345/1997 om behandling af personoplysninger

Betænkning om offentlighedsloven (1510/2209), s. 272.

Hjemmesider

Alleweldt, F., & Senda, K. (2012). *Directorate-general for internal policies*. Hentet fra http://www.europarl.europa.eu: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492433/IPOL-IMCO_ET(2012)492433_EN.pdf

Barnes, A. H. (u.d.). *The "Dark Side" of Going In House*. (BCG Attorney Search) Hentet fra https://careers.findlaw.com: https://careers.findlaw.com/legal-career-options/the-dark-side-of-going-in-house.html

Bloomberg. (17. Marts 2018). Tech Giants Set to Face 3% Tax on Revenue Under New EU Plan. *The Fortune*.

Breinstrup, T. (2016). *Superdataknusere skal skabe guld sammen*. Hentet fra https://www.business.dk: https://www.business.dk/digital/superdataknusere-skal-skabe-guld-sammen

Bækby, R. (2. Februar 2017). *Alexandra Instituttets hjemmeside*. Hentet fra https://www.alexandra.dk: https://www.alexandra.dk/dk/aktuelt/nyheder/2017/studie-hjaelper-danske-virksomheder-udnytte-data

Cadwalladr, C., & Graham-Harrison, E. (17. Marts 2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*.

Center for Frivilligt Socialt Arbejde . (29. November 2017). Hentet fra https://frivillighed.dk: https://frivillighed.dk/guides/regler-for-foreningers-brug-og-behandling-af-personoplysninger

Centralt ForeningsRegister. (1. December 2017). Hentet fra http://medlemstal.dk/: http://medlemstal.dk/

Commission Nationale de l'Informatique et des Libertés . (u.d.). Hentet fra https://www.cnil.fr/: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

Commission, E. (2014). *Progress on EU data protection reform now irreversible following European Parliament vote*. Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_MEMO-14-186_da.htm

Communication, D.-G. (2011). Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. Hentet fra http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf

Dansk Industri. (u.d.). *Dansk Industris hjemmeside.* Hentet fra https://digital.di.dk: https://digital.di.dk/SiteCollectionDocuments/Publikationer/Faktaark%20om%20strategi%20for%20EUs%20digitale%20indre%20marked.pdf

Datatilsynets hjemmeside. (December 2017). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO_-_revideret_offentliggoerelse__1_0_.pdf

Datatilsynets hjemmeside. (20. April 2018). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/

Datatilsynets hjemmeside. (28. Marts 2018). Hentet fra https://www.datatilsynet.dk: https://www.datatilsynet.dk/om-datatilsynet/medarbejdere/

Det Danske Spejderkorps hjemmeside. (u.d.). Hentet fra https://dds.dk/: https://dds.dk/om-det-danske-spejderkorps

DLA Piper - Data Protection Laws Of The World. (17. Januar 2017). Hentet fra https://www.dlapiperdataprotection.com: https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=DE

Edwards, J. (31. Januar 2018). GDPR could wipe 2% from Google's revenues, according to Deutsche Bank. *Business Insider Nordic*. Hentet fra http://nordic.businessinsider.com.

Effektivisering, S. f. (u.d.). *En bedre og hurtigere offentlig sektor*. Hentet fra http://sdfe.dk: http://sdfe.dk/data-skaber-vaerdi/en-bedre-og-hurtigere-offentlig-sektor/

Energi-, Forsynings og klimaministeriets hjemmeside. (21. Marts 2017). Hentet fra http://efkm.dk: http://efkm.dk/aktuelt/nyheder/nyheder-2017/marts-2017/frie-geodata-har-en-vaerdi-paa-3-5-mia-kr/

Europa Kommissionens hjemmeside. (u.d.). Hentet fra https://ec.europa.eu: https://ec.europa.eu/commission/priorities/digital-single-market_da

Europa Kommissionens hjemmeside. (27. Juni 2017). Hentet fra https://ec.europa.eu: https://ec.europa.eu/denmark/news/google-160627_da

Europa-Kommissionen. (2015). *Europa-Kommissionen - Pressemeddelelse*. Hentet fra Aftale om Kommissionens EU-databeskyttelsesreform vil styrke det digitale indre marked: http://europa.eu/rapid/press-release_IP-15-6321_da.htm

Europa-Kommissionen. (2004). *EUR-Lex Access to European Union law*. Hentet fra http://eur-lex.europa.eu: http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:52004XC0205(02)

Europakommissionen. (u.d.). *Europa-Kommissionen - Pressemeddelelse*. Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_IP-15-4919_da.htm

Europakommissionens hjemmeside. (u.d.). Hentet fra http://ec.europa.eu: http://ec.europa.eu/priorities/sites/beta-political/files/pg_da.pdf

Europa-Parlamentets og Rådets forordning af 2016-04-27. (27. 04 2016). (KARNOV) Hentet fra https://pro.karnovgroup.dk: https://pro.karnovgroup.dk/document/7000751611/6#EUFOR2016679_NKAR251

European Commission's website. (25. April 2013). Hentet fra http://europa.eu: http://europa.eu/rapid/press-release_MEMO-13-383_da.htm

European Commission's website. (12. December 2017). Hentet fra http://ec.europa.eu/: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=59485

European Commission's website. (16. Februar 2018). Hentet fra https://ec.europa.eu: https://ec.europa.eu/growth/sectors/tourism/business-portal/webinars/social-media-marketing-facebook_en

Forrest, M. (01. januar 2018). *Medlemslande i EU*. Hentet fra http://www.eu.dk: http://www.eu.dk/da/fakta-om-eu/medlemslande

Forsvarets efterretningstjenestes hjemmeside. (u.d.). Hentet fra https://fe-ddis.dk: https://fe-ddis.dk/Pages/default.aspx

Frederiksberg kommunes hjemmeside. (u.d.). Hentet fra https://www.frederiksberg.dk: https://www.frederiksberg.dk/borger/fritid-og-oplevelser/foreninger/foreninger-pa-frederiksberg

Horsens, R. (u.d.). *Forskningsprogram TVÆRSPOR.* Hentet fra http://www.regionshospitalet-horsens.dk: http://www.regionshospitalet-horsens.dk/siteassets/om-os/virksomhedsgrundlag/forskningsprogram-tvarspor.pdf

IBM New Room. (16. April 2018). Hentet fra http://newsroom.ibm.com: http://newsroom.ibm.com/2018-04-16-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacy-and-Security

Information Commissioners office's website. (5. Oktober 2016). Hentet fra https://ico.org.uk: https://ico.org.uk/action-weve-taken/enforcement/talktalk-telecom-group-plc-mpn/

Ingeniørforeningen, I. (u.d.). *Big data – privacy og vækst.* Hentet fra https://ida.dk: https://ida.dk/sites/default/files/big_data_-_privacy_og_vaekst.pdf

Ivanova, I. (10. April 2018). *CBS News*. Hentet fra https://www.cbsnews.com: https://www.cbsnews.com/news/facebook-stock-price-today-subdued-heading-into-ceos-testimony/

Jervelund, C., Brenøe, S., & Kirk, A. R. (2017). *NEXT Partnership, Lægemiddelindustriforeningen.* Hentet fra Værdien af kliniske forsøg i Danmark: https://biopeople.eu/fileadmin/user_upload/Editor/Rapport_Vaerdien-af-kliniske-forsoeg-i-Danmark.pdf

Jourová, V. (januar 2016). *Reformen af EU's databeskyttelsesregler og big data.* Hentet fra http://ec.europa.eu: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41558

justitsministeriets hjemmeside. (27. Oktober 2017). Hentet fra www.justitsministeriet.dk: http://www.justitsministeriet.dk/nyt-og-presse/nyhedsbrev/2017/nyhedsbrev-af-27-oktober-2017

justitsministeriets hjemmeside. (24. maj 2017). Hentet fra http://justitsministeriet.dk: http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2017/nye-regler-styrker-beskyttelsen-af-persondata-i-europa

Kallas, P. (4. December 2017). *Dreamgrow*. Hentet fra https://www.dreamgrow.com: https://www.dreamgrow.com/top-10-social-networking-sites-market-share-of-visits/

Klug, C. (2010). *The German Association for Data Protection and Data Security (GDD) .* Hentet fra https://www.gdd.de: https://www.gdd.de/international/english/DPO_Report_by_Christoph_Klug.pdf

Korsnes, R. (4.. april 2017). *DERFOR BØR DU VÆRE OPPTATT AV AT INKASSOSELSKAPET DITT HAR ET PERSONVERNOMBUD*. Hentet fra http://blogg.intrum.no: http://blogg.intrum.no/derfor-bor-du-vare-opptatt-av-at-inkassoselskapet-ditt-har-et-personvernombud

Københavns kommunes hjemmside. (u.d.). Hentet fra www.kk.dk: https://www.kk.dk/artikel/folkeoplysende-foreninger

National Commission For Data Protection. (u.d.). Hentet fra https://cnpd.public.lu/en.html: https://cnpd.public.lu/content/dam/cnpd/en/legislation/droit-lux/doc_loi02082002mod_en.pdf

Omada. (u.d.). *Hvem har egentlig adgang til dine data?* Hentet fra https://www.business.dk: https://www.business.dk/annonce/hvem-har-egentlig-adgang-til-dine-data

Politiets efterretningstjenestes hjemmeside. (u.d.). Hentet fra https://www.pet.dk/.

Poulsen, S. P. (2017-2018). *Folketingets hjemmeside*. Hentet fra http://www.ft.dk: http://www.ft.dk/samling/20171/lovforslag/L68/tidsplan.htm

Poulsen, S. P. (2017-2018). *Folketingets hjemmeside*. Hentet fra http://www.ft.dk: http://www.ft.dk/samling/20171/lovforslag/L69/tidsplan.htm

Riigi Teataja - Personal Data Protection Act. (3. Juli 2016). Hentet fra https://www.riigiteataja.ee: https://www.riigiteataja.ee/en/eli/ee/529012015008/consolide/current

Råd, D. E. (2017). *Debatdag om fremtidens sundhedsvæsen, big data og wearables.* Hentet fra http://www.etiskraad.dk: http://www.etiskraad.dk/etiske-temaer/sundhedsdata/fremtidens-sundhedsvaesen-big-data-og-wearables

Statista. (u.d.). Hentet fra https://www.statista.com: https://www.statista.com/statistics/266206/googles-annual-global-revenue/

Statista. (u.d.). Hentet fra https://www.statista.com: https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/

Styrelsen for Dataforsyning og Effektiviseringens hjemmeside. (u.d.). Hentet fra http://sdfe.dk: http://sdfe.dk/data-skaber-vaerdi/en-bedre-og-hurtigere-offentlig-sektor/

Sørensen, T. Ø., Elmeskov, J., & Lebech, A. (2015). *Big data til gavn for vækst og velfærd – en unik dansk mulighed*. Hentet fra http://samf.ku.dk: http://samf.ku.dk/presse/kronikker-og-debat/big-data-konference/

The German Law Archive. (17. August 2017). Hentet fra https://germanlawarchive.iuscomp.org: https://germanlawarchive.iuscomp.org/?p=712

The Laws of Malta website. (4. May 2018). Hentet fra http://www.justiceservices.gov.mt/: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8906&l=1

Theory Of The Firm. (u.d.). Hentet fra https://www.investopedia.com: https://www.investopedia.com/terms/t/theory-firm.asp

Thomsen, P. B. (19. Marts 2018). *Danmarks Radios hjemmeside*. Hentet fra https://www.dr.dk: https://www.dr.dk/nyheder/udland/eu-fordoemmer-paastaaet-tyveri-af-facebook-brugerdata

Worstall, T. (10. Maj 2017). Google And Facebook Are Dominant But Not Monopolies. *Forbes*.

Yahoo Finance. (u.d.). Hentet fra https://finance.yahoo.com: https://finance.yahoo.com/quote/FB/?guccounter=1