

Databeskyttelse gennem design

En analyse af art. 25, stk. 1 i Persondataforordningen

Data protection by design

An analysis of art. 25 (1) in the General Data Protection Regulation

Cand.merc.(jur.) - erhvervsøkonomi og jura
Copenhagen Business School
Kandidatafhandling, 2018

Navn: Daniel Kim Rasmussen & Eyðun Trúgvason
Eksamensnr.: 54809 & 53976
Vejledere: Mette Vestergaard Huss & Lasse Holt

Anslag: 265.295 (I alt 273.603)
Sider: 120 (I alt 125)

Dato: 14. maj 2018



Abstract

In the context of the rapid evolution of the digital world, the EU has developed the General Data Protection Regulation (GDPR) in replacement of the current Data Protection Directive. The overall aim of this thesis is to examine the economic efficiency of the introduction of the Data Protection by Design provision in Article 25 (1).

The analysis starts off by investigating the substantive content of the notion of Data Protection by Design. According to the report of the Danish Ministry of Justice, the notion is not new, since it is already covered by Article 17 of the current directive. All though this might be the case, others are claiming that this new explicit provision will be broader, as it will no longer only include security measures, as was the case with Article 17. Based on the analysis, it can be concluded that the provision covers more than security measures - especially when it is to be interpreted in accordance with Ann Cavoukian's term. The provision therefore entails a change in relation to applicable law.

Next, the economic analysis investigates if the principle of Data Protection by Design has an economic value for companies. It is concluded that some companies may implement the principle on their own initiative, since it gives them a competitive advantage. However, due to the lack of data protection demand and the high value of personal data, most companies will not have incentives to introduce the principle. This low demand for data protection may be due to market failures, which can justify regulation from an economic viewpoint.

In conclusion, the economic efficiency of the provision is investigated. The efficiency of the provision depends in part on whether the market failures are effectively corrected. Here are two conditions. Firstly, it is crucial that the legislator has chosen the optimal data protection level, which corresponds to what rational individuals with complete information would have demanded. Secondly, there must be effective enforcement so that the data controller complies with the provision. However, the efficiency of the provision also depends on whether it is efficient in relation to the purpose of the legislation, and what other effects it has on companies and thus society. The analysis concludes that although the provision presumably corrects the market failures in part, it is still not considered to be efficient, since it is deemed to be innovation retardant, and thus inhibiting economic growth, which is one of the overall purposes of the EU.

Indholdsfortegnelse

Abstract.....	1
Indholdsfortegnelse.....	2
Kapitel 1.....	5
1.1. Indledning.....	5
1.2. Problemformulering	6
1.3. Synsvinkel	6
1.4. Afgrænsning	7
1.5. Struktur.....	7
1.6. Metode og teori	8
1.6.1. Juridiske metode	8
1.6.1.1. EU-ret	9
1.6.1.2. Primær regulering	9
1.6.1.3. Sekundær regulering.....	9
1.6.1.4. EU-retspraksis.....	10
1.6.1.5. Dansk regulering.....	10
1.6.2. Økonomisk metode	10
1.6.2.1. Økonomisk videnskabsteori.....	11
1.6.2.2. Økonomiske teorier og begreber	12
1.6.3. Integreret metode	13
Kapitel 2: Juridisk analyse.....	16
2.1. Indledning.....	16
2.2. Baggrunden for de persondataretlige regler	16
2.3. Hvorfor indholdet af bestemmelsen har betydning for de dataansvarlige.....	18
2.4. Justitsministeriets betænkning nr. 1565 om forordningen	19
2.5. Rådet for Digital Sikkerhed.....	22
2.5.1. Rådets formand uddyber uenighed	23
2.6. Hvad handler uenigheden i virkeligheden om?	24
2.7. Hvad er en sikkerhedsforanstaltning?	25
2.8. Ann Cavoukians Privacy by Design begreb.....	28
2.8.1. Gennemgang af de syv principper	29

2.9.	Ministerspørgsmål og svar	32
2.10.	Tilsynsmyndigheder	35
2.10.1.	Det danske datatilsyn.....	35
2.10.2.	Det britiske datatilsyn.....	36
2.10.3.	Det norske datatilsyn	37
2.11.	ENISA.....	39
2.12.	Artikel 29-gruppen.....	42
2.13.	EU-Domstolens hidtidige praksis	44
2.14.	EU-domstolens fortolkning	47
2.14.1.	Ordlyd.....	48
2.14.2.	Sammenhæng og helhed.....	50
2.14.3.	Formål	55
2.14.3.1.	Overordnet formål med persondatareglerne	56
2.14.3.2.	Google Spain-dommen	56
2.14.3.3.	Formålet med Persondataforordningens art. 25.....	58
2.14.3.4.	Formålsfortolkning af databeskyttelse gennem design.....	58
2.14.4.	EU-rettens udviklingstrin	60
2.14.4.1.	Internettets udviklingstrin.....	60
2.14.5.	Fortolkningskonklusion.....	61
2.15.	Konklusion på juridisk analyse.....	63
Kapitel 3:	Økonomisk analyse	65
3.1.	Indledning.....	65
3.2.	Databeskyttelse gennem design – en økonomisk byrde eller en konkurrencefordel?.....	65
3.3.	Produktdifferentiering og Hotelling model	67
3.4.	Den økonomiske værdi af persondata	70
3.5.	Efterspørgsel på databeskyttelse	71
3.6.	Hvordan markedet finder et databeskyttelsesniveau	73
3.7.	Adam Smith's model for sikkerhed på arbejdsmarkedet	75
3.8.	Markedsfejl.....	77
3.8.1.	Adfærdsmæssige antagelser	78
3.8.2.	Informationsfejl.....	79
3.8.3.	Hvordan markedet reagerer på informationsfejl	80

3.8.4. Opportunisme.....	81
3.9. Spilteori med to spil	81
3.10. Konklusion på økonomisk analyse	85
Kapitel 4: Integreret analyse.....	86
4.1. Indledning.....	86
4.2. Bestemmelsens efficiens i forhold til markedsfejlen	87
4.2.1. Forskel på virksomheder	89
4.2.2. EU's valg af databeskyttelsesniveau	91
4.2.3. Overholdelse af forordningen	92
4.2.3.1. Bøden for overtrædelse af bestemmelsen	92
4.2.3.2. Sandsynligheden for at blive opdaget.....	94
4.2.3.3. Omkostning til overholdelse	97
4.2.3.3.1. Stigende omkostninger for databeskyttelse	97
4.2.3.3.2. Omkostninger til overholdelse af databeskyttelse gennem design.....	99
4.2.3.3.3. Principal-agent-teorien	100
4.2.3.3.4. Coase-teoremet	102
4.2.4. Konklusion på efficiens i forhold til markedsfejlen.....	104
4.3. Bestemmelsens efficiens i forhold til forordningens og EU's formål	104
4.3.1. Økonomisk vækst i samfundet	106
4.3.2. Schumpeters teori om innovatøren	106
4.3.3. Big data er fremtiden.....	108
4.3.3.1. Big data i Danmark.....	110
4.3.3.2. Forsigtighed med deling af persondata.....	110
4.3.4. Innovationshæmmende forordning?	111
4.3.5. Innovation i forbindelse med databeskyttelse gennem design	113
4.4. Konklusion på integreret analyse	116
Kapitel 5: Samlet konklusion	118
Litteraturliste	121

Kapitel 1

1.1. Indledning

Set i lyset af den rivende udvikling inden for den digitale verden, har EU udarbejdet en ny persondataforordning til erstatning af det nuværende Persondatadirektiv. Forordningen blev endeligt vedtaget den 14. april 2016, og der blev her sat punktum for 4 års EU-lovarbejde. Forordningen er en spændende nyskabelse, og EU-lovarbejdet har været underlagt stor politisk og pressemæssig interesse.

I og med at forordningen ikke blev en så vidtgående reform, som Kommissionen oprindeligt lagde op til, er der uenighed om, hvor nyskabende den er. Mens nogle mener, at der blot er tale om det samme indhold, så mener andre, at der er tale om en omvæltning af hele persondataretten. Det er dog et faktum, at forordningen indeholder både nogle nye og skærpede krav.

Et af disse er forordningens art. 25 om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Begreberne er dog ikke klart defineret i forordningen, og der er allerede nu opstået uenighed om fortolkningen af bestemmelsen. Justitsministeriets opfattelse er, at begrebet databeskyttelse gennem design ikke er nyt, og at det allerede er en del af det nugældende direktiv. Dette er efterfølgende blevet kritiseret, hvor det er påpeget, at begrebet skal forstås og fortolkes langt bredere end tidligere. Det er derfor yderst relevant at få afklaret begrebet, så de dataansvarlige har mulighed for at overholde forordningen og udføre deres behandling i overensstemmelse med denne.

Spørgsmålet er i den forbindelse også, om bestemmelsen er økonomisk efficient. Det vil derfor være interessant at se nærmere på, om virksomhederne overhoved vil overholde bestemmelsen, idet der kan være meget store omkostninger til indførelse af databeskyttelse gennem design. Her er det også interessant at se på, hvilke øvrige effekter kravet har på virksomhederne, og om kravet er efficient i forhold til både forordningens og EU's overordnede formål – herunder formålet med det indre marked.

1.2. Problemformulering

Det overordnede formål med denne afhandling er at undersøge den økonomiske efficiens af kravet om databeskyttelse gennem design, som introduceres i Persondataforordningens art. 25, stk. 1.

Afhandlingen vil i denne forbindelse undersøge det materielle indhold af begrebet databeskyttelse gennem design, og sammenligne med gældende ret. Det skal undersøges, om princippet i sig selv har en økonomisk værdi for virksomheder, og om de af egen drift vil implementere princippet. Det skal endvidere undersøges, hvilke virkninger kravet har på virksomhederne, og om dette er efficient i forhold til det overordnede formål med både Persondataforordningen og EU's overordnede formål. På baggrund af ovenstående, vil afhandlingen besvare følgende spørgsmål:

Juridisk problemformulering

Hvad indeholder begrebet databeskyttelse gennem design i Persondataforordningens art. 25, stk. 1? Og er det en forandring i forhold til gældende ret?

Økonomisk problemformulering

Har databeskyttelse gennem design en økonomisk værdi for virksomheder? Og vil virksomheder af egen drift implementere princippet?

Integreret problemformulering

Hvilke virkninger har indførelsen af kravet om databeskyttelse gennem design på virksomhederne? Og er dette efficient i forhold til Persondataforordningens og EU's overordnede formål – herunder formålet med det indre marked?

1.3. Synsvinkel

Det er de dataansvarlige, der skal overholde reglerne i art. 25, og det er derfor mest nærliggende, at afhandlingen tager udgangspunkt i de dataansvarlige.

En dataansvarlig defineres i Persondataforordningens art. 4, nr. 7 som “en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ...”. Dog begrænses synsvinklen i afhandlingen til at være juridiske personer.

1.4. Afgrænsning

Afhandlingen vil primært undersøge, hvad begrebet databeskyttelse gennem design i forordningens art. 25, stk. 1 dækker over. Databeskyttelse gennem standardindstillinger i art. 25, stk. 2 inddrages kun i det omfang, det findes relevant i forhold til analysen af art. 25, stk. 1. Det analyseres dermed ikke som et selvstændigt princip, i og med at det efter den oprindelige definition af begrebet Privacy by Design er en del heraf. Forordningens art. 25, stk. 3 inddrages ikke i analysen.

1.5. Struktur

Kapitel 1 introducerer afhandlingens emne, problemstilling, synsvinkel og afgrænsning. Derudover bliver den metodiske tilgang til de tre analyser gennemgået.

Kapitel 2 indeholder den juridiske analyse, hvor den juridiske problemformulering søges besvaret ved en analyse af begrebet databeskyttelse gennem design samt en sammenligning mellem Persondatadirektivet og Persondataforordningen for en afklaring af, om der er en ændring i forordningen i forhold til gældende ret.

Kapitel 3 indeholder den økonomiske analyse, der har til formål at besvare den økonomiske problemstilling. Her anvendes flere teorier for at få afklaret, om databeskyttelse gennem design har en økonomisk værdi for virksomheder og om de af egen drift vil implementere princippet. Her inddrages bl.a. konkurrencefordele og værdien af data. Derudover ses der på markedsfejl, der kan være årsagen til manglende implementering af princippet.

Kapitel 4 indeholder den integrerede analyse, hvor den integrerede problemstilling søges besvaret ved en analyse af, om forordningens bestemmelse om databeskyttelse gennem design er efficient. Der ses her på, om markedsfejlen effektivt bliver rettet op, hvilket både afhænger af det valgte databeskyttelsesniveau, og om der er effektiv håndhævelse af bestemmelsen. Der ses også på, om bestemmelsen er i overensstemmelse med EU's formål med det indre marked.

Kapitel 5 indeholder den samlede konklusion, som er en sammenfatning af de delkonklusioner, der er lavet til hvert kapitel.

1.6. Metode og teori

1.6.1. Juridiske metode

Formålet med den juridiske analyse er at undersøge hvad begrebet databeskyttelse gennem design indeholder.

Til analyse af en juridisk problemstilling anvendes retskildelæren, der bygger på Alf Ross' variant af realistisk retsteori. I denne teori opdeles de bindende normer i fire kategorier - regulering, retspraksis, retssædvaner og forholdets natur.¹

Til at udlede og analysere gældende ret anvendes den retsdogmatiske metode. Det er nødvendigt at skelne mellem retskildelæren og den retsdogmatiske metode, idet der inden for retskildelæren ikke er en rangorden mellem de fire normer, men inden for den retsdogmatiske metode er en rækkefølge, hvori normerne undersøges. Dette for at sikre, at alle træned brugere, herunder lovgiver, domstole og juridiske forskere etc., kommer frem til samme resultat ved analyse af en juridisk problemstilling.²

Selvom der ikke er en rangorden mellem retskilderne, er der som følge af lex-principperne en rangorden inden for normen regulering. Det følger af de tre lex-principper - lex superior, lex specialis og lex posterior. Lex superior medfører, at ingen lov må stride mod en højere rangeret lov. Det vil sige, at f.eks. ingen lov må stride mod Grundloven, og da bekendtgørelser har hjemmel i lov, må ingen bekendtgørelse stride mod en lov. Lex specialis medfører, at en speciallov har højere rang end en generel lov og lex posterior, at en ny lov har højere rang end en ældre lov.³

I denne afhandling anvendes den retsdogmatiske metode, hvormed alle retskilder gennemgås, men inddrages når og kun, hvis de er relevante for belysning af en problemstilling.

¹ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 56

² Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 33-34

³ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 235-240

1.6.1.1. EU-ret

Inden for EU-retten findes primær og sekundær regulering. Primær er EU's traktatgrundlag og grundlæggende rettigheder og almindelige retsprincipper. Sekundær er afledet af den primære og har således hjemmel heri. Den sekundære består af forordninger, direktiver, beslutninger m.v.⁴ I denne afhandling vil både primær og sekundær regulering blive inddraget.

1.6.1.2. Primær regulering

Den nye Persondataforordning er sekundær regulering, men denne bygger bl.a. på Den Europæiske Unions charter om grundlæggende rettigheder (chartret) og traktaten om Den Europæiske Unions funktionsmåde (TEUF), da retten til beskyttelse af personoplysninger fremgår af TEUF art. 16, stk. 1. og chartrets art. 8, stk. 1 jf. Persondataforordningens præambel 1. Det vil derfor være relevant ligeledes at inddrage primær regulering, som chartret og TEUF er en del af.

1.6.1.3. Sekundær regulering

Persondatadirektivet (dir. 95/46 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) blev udstedt i 1995. I Danmark blev direktivet implementeret i 2000 med Persondataloven.⁵

Den 25. januar 2012 fremlagde Kommissionen et udkast til en Persondataforordning, som skulle afløse Persondatadirektivet. Den 14. april 2016 blev forordningen vedtaget, og dens direkte virkning i medlemslandene træder i kraft to år efter. Forordningen træder i kraft den 25. maj 2018. Selv om forordningen afløser de hidtidige regler, så vil de bærende principper, som direktivet hviler på, også være fundamentale for forordningen.⁶

⁴ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 97-98

⁵ Lov 2000-05-31 nr. 429 om behandling af personoplysninger (Persondataloven), senest ændret ved L 2017-05-03 nr. 426

⁶ Udsen, Henrik. 2016. *IT-ret*. Ex Tuto. 3. udgave, s. 307

1.6.1.4. EU-retspraksis

I og med at Persondataforordningen ikke er trådt i kraft endnu, har EU-Domstolen ikke taget stilling til mulige problemstillinger i den. EU-Domstolen betjener sig dog af en kendt fortolkningsstil, hvor hovedreglen er objektiv formålsfortolkning, også kaldet teleologisk fortolkning.⁷ Denne anvendes i analysen, men derudover anvendes også ordlydsfortolkning og fortolkning i forhold til sammenhængen og det nuværende udviklingstrin. Ydermere inddrages domme der omhandler lignende problemstillinger.

1.6.1.5. Dansk regulering

Persondatadirektivet blev implementeret i Danmark gennem Persondataloven i 2000. Den vil blive ophævet med ikrafttrædelsen af Databeskyttelsesloven, som træder i kraft samtidig med Persondataforordningen.

Selvom en forordning normalt hverken skal eller må implementeres i national ret,⁸ er det med Persondataforordningen lidt anderledes. Der er områder, der er lagt ud til national selvbestemmelse. Derfor vil der komme en ny Databeskyttelseslov. Der er på nuværende tidspunkt udarbejdet en betænkning og et lovforslag, som ligeledes vil blive inddraget i den juridiske analyse.

1.6.2. Økonomisk metode

I den økonomiske analyse skal princippet om databeskyttelse gennem design analyseres fra et økonomisk perspektiv.

Denne del af afhandlingen gør brug af den deduktive metode, i og med at der tages udgangspunkt i de teoretiske antagelser samt konklusionen fra den juridiske analyse, som så bliver holdt op imod afhandlingens økonomiske problemstilling.

⁷ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 253

⁸ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 105

1.6.2.1. Økonomisk videnskabsteori

I den økonomiske analyse tages der udgangspunkt i den nyinstitutionelle økonomi. Den kaldes den nyinstitutionelle økonomi, for at den ikke skal blandes med den 'gamle institutionelle økonomi', som blev udviklet for mere end 100 år siden, og som i nyere tid har stået i skyggen af den neoklassiske økonomi.⁹

Den nyinstitutionelle økonomi har mange lighedspunkter med den neoklassiske økonomi. De har begge markedet som analyseniveau, virksomheden som analyseenhed og opererer med på forhånd fastlagte aktørforudsætninger.¹⁰

Fremvæksten af den nyinstitutionelle økonomi har sin oprindelse i Ronald Coases artikel *The Nature of the Firm* fra 1937, hvor Coase stillede nogle spørgsmål, som ikke kunne besvares inden for den neoklassiske økonomi - herunder det grundlæggende spørgsmål: Hvorfor findes der virksomheder? Ronald Coase udfordrede med artiklen den neoklassiske antagelse om det perfekte marked, hvor transaktionsomkostningerne er lig nul.¹¹

Inden for den nyinstitutionelle teori er udgangspunktet, at aktørerne er begrænset rationelle, der er ikke perfekt information på markedet og teorien inddrager transaktionsomkostningerne. Inden for den neoklassiske teori er aktørerne rationelle, der er perfekt information og transaktionsomkostninger eksisterer ikke. De to teorier er dermed på disse punkter diametrale modsætninger. Den nyinstitutionelle økonomi antager endvidere, at aktørerne vil handle opportunistisk, og vil maksimere egne interesser inden for den institutionelle ramme ved f.eks. at handle svigagtigt.¹²

Med erkendelsen af, at aktører er begrænset rationelle, og at der ikke er perfekt information, anses den nyinstitutionelle økonomi derfor som den mest realistiske tilgang i metodisk forstand. Den nyinstitutionelle metode vil derfor være et velegnet udgangspunkt for analysen.

⁹ Hansen, Anders Christian. 2007. *Uden for hovedstrømmen - Alternative strømninger i økonomisk teori*. Roskilde Universitetsforlag, s. 41-42

¹⁰ Østergaard, Kim. 2003. *Metode på cand. merc. jur. studiet. Julebog 2003*, s. 272

¹¹ Hansen, Anders Christian. 2007. *Uden for hovedstrømmen - Alternative strømninger i økonomisk teori*. Roskilde Universitetsforlag, s. 41-42

¹² Østergaard, Kim. 2003. *Metode på cand. merc. jur. studiet. Julebog 2003*, s. 273

1.6.2.2. Økonomiske teorier og begreber

De økonomiske teorier og begreber, der anvendes til at besvare den økonomiske problemformulering, skal introduceres her.

Det er påstået, at det kan være en konkurrencefordel for virksomheder at opfylde kravene til databeskyttelse gennem design. For at kvalificere konkurrencefordele, inddrages Michael Porters generiske konkurrencestrategier. Såfremt en virksomhed skal anvende databeskyttelse gennem design, må udgangspunktet være, at der vil være en højere omkostning, end hvis det ikke anvendes. Virksomheder der benytter sig heraf, vil derfor have en højere omkostning og dette vil alt andet lige medføre en højere pris. Da udgangspunktet inden for den økonomiske teori er, at virksomheden med den laveste pris vil tage hele markedet, vil the Hotelling model blive anvendt, da den kan vise, hvordan to virksomheder med et ens produkt godt kan tage en differentieret pris for varen, uden at den ene virksomhed tager hele markedet. Det skyldes, at transportomkostningen inddrages i modellen. Derudover kan modellen anvendes til at beskrive den situation, hvor to virksomheder har et differentieret produkt. Her konverteres transportomkostningen til en aversion mod, at man ikke får præcis det ønskede.

I analysen opstilles et tilbagevendende eksempel med to forskellige lygteapps, der som udgangspunkt er ens. Dog skal der på den ene gives tilladelse til deling af persondata, hvilket der ikke skal på den anden, som til gengæld koster penge. Eksemplet anvendes her til at illustrere, hvordan databeskyttelse gennem design ifølge the Hotelling model kan udgøre en konkurrencefordel, selvom der vil være en højere omkostning for virksomheden og prisen for produktet dermed bliver højere.

For at vise hvordan markedet selv finder det optimale niveau af databeskyttelse anvendes den klassiske model for udbud og efterspørgsel. Som et alternativ til dette, og for at anvende en model, der lidt bedre kan sammenlignes med databeskyttelse, anvendes Adam Smiths model for sikkerhed på arbejdsmarkedet. Både i modellen for udbud og efterspørgsel og i Adam Smiths model kan der ske det, at markedet ikke selv finder det optimale punkt. Hvis dette er tilfældet, kan det skyldes markedsfejl, hvorfor teorien om markedsfejl også vil blive inddraget i analysen.

For at illustrere de økonomiske aktørers nyttemaksimering og beslutningstagning anvendes spilteorien. Spilteorien betragtes som et selvstændigt forskningsprogram, og en videreudvikling af den neoklassiske økonomi.¹³ Eksemplet med de to lygteapps inddrages her igen, for at illustrere hvordan virksomhedernes opportunisme og forbrugernes begrænsede rationalitet påvirker markedsligevægten.

1.6.3. Integreret metode

Overordnet skal der i den integrerede analyse laves en efficiensanalyse af Persondataforordningens art. 25, stk. 1, hvor virksomhederne er i fokus.

Bestemmelsens efficiens afhænger for det første af, om eventuelle markedsfejl effektivt bliver rettet op. Her opstilles to betingelser. Det er for det første afgørende, at lovgiver har valgt det optimale databeskyttelsesniveau, hvilket svarer til, hvad rationelle individer med fuldkommen information ville efterspørge. For det andet skal der være effektiv håndhævelse, således at de dataansvarlige overholder bestemmelsen. Men bestemmelsens efficiens afhænger derudover af, om den er efficient i forhold til lovgivningens formål, samt hvilke øvrige effekter den har på virksomhederne og dermed samfundet. Disse efficiensbetingelser undersøges i den integrerede analyse.

Til dette formål anvendes til dels retsøkonomien. Retsøkonomi er ikke en del af det juridiske hus og ikke en integration mellem jura og økonomi, men en del af den økonomiske videnskab, som kan anvendes til at belyse en problemstilling i en retsvidenskabelig analyse ved brug af økonomiske betragtninger. På den måde anvendes retsøkonomien til en økonomisk analyse af retten.¹⁴

Retsøkonomien anvender både neoklassisk- og nyinstitutionel teori.¹⁵

Retsøkonomien anvendes på det samfundsmæssige niveau. Det vil sige, at den kan anvendes til at belyse problemstillinger, der påvirker samfundet – altså på en form for makroniveau. Skal der i stedet analyseres på mikroniveau – f.eks. mellem to virksomheder, anvendes i stedet kontraktøkonomien.¹⁶ Retsøkonomien anvendes således til at belyse de implikationer, som bestemmelsen kan medføre for

¹³ Knudsen, Christian. 1997. *Økonomisk Metodologi Bind 2 – Virksomhedsteori & Industriøkonomi*. Jurist- og Økonomforbundets Forlag, s. 88-89

¹⁴ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 429-431

¹⁵ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 434

¹⁶ Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag, s. 434

virksomhederne, samt efficiensen af bestemmelsen, og kontraktøkonomien anvendes i forbindelse med kontraktkoncipering mellem en virksomhed og dennes it-leverandør.

Til den integrerede analyse anvendes en model til at vise, hvorledes lovgiver kan påvirke virksomheder til at opnå et højere niveau af databeskyttelse. Modellen skal vise problematikken i, at niveauet kan sættes for højt af lovgiver, således at det ikke kan betale sig for virksomhederne at overholde lovgivningen. I den forbindelse skal modellen udvides, således at det fremgår hvorledes lovgivning kan påvirke virksomheder forskelligt, idet virksomheders nuværende niveau og omkostninger til overholdelse er forskellige, og der derfor kan være forskel på, om det kan betale sig at overholde lovgivningen.

Modellen, der anvendes i denne forbindelse, er oprindeligt lavet til at vise, hvordan der sættes det optimale niveau af lovgiver om sikkerhed på arbejdspladsen, men den kan altså også bruges til at beskrive situationen med beskyttelse af persondata, da modellen viser, både om det kan betale sig for virksomheder at overholde lovgivningen, og hvor lovgiver skal sætte niveauet for at sikre overholdelse, herunder også bødestørrelser.

For at undersøge, om virksomheder vil overholde bestemmelsen, tages der udgangspunkt i følgende ligning, hvor hver enkelt del af ligningen skal undersøges i forbindelse med databeskyttelse gennem design: *Omkostning til overholdelse < sandsynligheden for at blive opdaget x bøden for overtrædelse af bestemmelsen.*

For at virksomheder skal kunne overholde bestemmelsen, kræver det for de fleste it-udvikling, da deres nuværende systemer ikke lever op til kravene. Mange virksomheder er ikke selv ejer af deres it-systemer, men køber rettigheden til at bruge det af en it-virksomhed. Der er således tale om standardssystemer, som virksomhederne ikke umiddelbart har indflydelse på. Virksomhederne kan selvfølgelig vælge at få udviklet specialtilretninger, men det er som oftest med en stor omkostning til følge, og med risiko for at andre virksomheder også får del i den tilretning, som virksomheden således har betalt.

Til belysning af denne problemstilling anvendes kontraktøkonomien. I relationen mellem en virksomhed og en it-virksomhed opstår der en situation, hvor der er stor forskel på vidensniveauet.

Denne asymmetriske information kan udnyttes, hvorfor principal-agent-teorien inddrages. Principal-agent-teorien kan netop beskrive den problematik der opstår i et samarbejde mellem to parter - en principal og en agent, som typisk har modsatrettede ønsker/hensyn.

For yderligere at understrege problematikken mellem de to parter, anvendes Coase-teoremet. Ifølge Coase-teoremet vil der i en forhandlingssituation altid opstå et Pareto-optimalt resultat, hvis tre betingelser er opfyldt. Der skal være tale om en forhandlingssituation, ejendomsrettighederne skal være veldefinerede og transaktionsomkostningerne skal være lig nul (eller meget lave). Det skal derfor undersøges, om alle disse betingelser er opfyldt og om en mangel på opfyldelse af alle tre betingelser kan være en årsag til, at Pareto-optimale resultater ikke opnås i forhandlingen mellem parterne. Ved Pareto-optimalitet skal forstås det punkt, hvor det ikke er muligt at stille en part bedre, uden minimum én bliver stillet værre.

For at undersøge om bestemmelsen er efficient i forhold til EU's overordnede formål, inddrages formålet med det indre marked, som bl.a. er at skabe økonomisk vækst. Til denne undersøgelse anvendes Joseph Schumpeters teori om innovation. Ifølge Schumpeter opstår økonomisk vækst på baggrund af innovatører som innoverer og dermed skaber en fremgang i økonomien. Denne tese er interessant, da den økonomiske vækst dermed påvirkes, såfremt bestemmelsen virkelig er hæmmende for innovationen. Dermed kan Schumpeters teori være med til at belyse, om bestemmelsen strider mod et af EU's overordnede formål.

Schumpeters teori udspringer af den neoklassiske teori, men er ændret, i det Schumpeter gjorde oprør mod de neoklassiske økonomer og deres tilgang til aktører som fuldkommen informerede og rationelle.¹⁷ Schumpeter nærmer sig derfor den nyinstitutionelle økonomi, hvor der arbejdes med begrænset rationalitet. Dog er Schumpeters teori om innovatøren skrevet tidligere, hvorfor det ikke kan siges, at Schumpeter anvender den nyinstitutionelle økonomi.

¹⁷ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 29 og 31-32

Kapitel 2: Juridisk analyse

2.1. Indledning

I Persondataforordningen bliver databeskyttelse gennem design introduceret som et begreb i forordningens art. 25. Det skal i den juridiske analyse belyses, hvad begrebet dækker over.

Justitsministeriet er i betænkning nr. 1565 om forordningen kommet med deres udlægning af begrebet, men denne er blevet kritiseret af bl.a. Rådet for Digital Sikkerhed. Denne uenighed om fortolkningen af den nye bestemmelse skal derfor undersøges nærmere.

For at skabe en større forståelse af reglerne som helhed, skal baggrunden for persondatareglerne, og de hensyn der ligger bag, først kort gennemgås.

2.2. Baggrunden for de persondataretlige regler

Persondataretten er en del af personlighedsretten, hvor personlighedsret overordnet omfatter regler, der beskytter individets integritet og personlighed. Personlighedsretten er et bredere begreb, der også omfatter andre regler, der er beslægtede med de persondataretlige regler.¹⁸

Alle lovregler springer ud fra afvejninger af nogle modsatrettede hensyn, og dette gælder også for de persondataretlige regler. Sammenlignes persondataretten med f.eks. immaterialretten, hvor hensynene overordnet er økonomiske, så er det ikke lige så nemt at beskrive hensynene bag persondataretten, hvor beskyttelsen har en mere moralsk-filosofisk karakter baseret på ideelle hensyn til individet.¹⁹

Persondataretten bygger overordnet på et privatlivshensyn, hvor individets behov for at kunne bevare oplysninger om sig selv, er i fokus, da det kan være integritetskrænkende, hvis personlige oplysninger om individet deles med offentligheden. Med andre ord er der tale om retten til ikke at optræde i

¹⁸ Udsen, Henrik. 2016. *IT-ret*. Ex Tuto. 3. udgave, s. 298

¹⁹ Udsen, Henrik. 2016. *IT-ret*. Ex Tuto. 3. udgave, s. 299

offentligheden. Derudover bygger persondataretten på et personlighedshensyn, hvilket indebærer, at individet selv skal bestemme, hvordan vedkommende vil fremtræde i offentligheden, da der ellers kan tegnes et falsk eller forvrænget personlighedsbillede af vedkommende.²⁰ Disse to hensyn har individet i fokus, og taler for et generelt forbud mod enhver behandling af personoplysninger. På den anden side er der nogle andre hensyn, der trækker i den modsatte retning. Det følger af informations- og ytringsfriheden, at information frit skal kunne spredes. Ytringsfriheden er en grundlæggende ret i et velfungerende demokrati, da den går ud på, at alle skal have ret til at udtrykke sin mening i skrift og tale uden andres forudgående godkendelse. Derudover er der andre hensyn, f.eks. hensynet til en effektiv forvaltning, muligheden for at drive virksomhed og kriminalitetsbekæmpelse, som taler for, at der skal ske indskrænkninger i persondatabeskyttelsen.²¹ Persondatareglerne bliver derfor en afvejning af disse modsatrettede hensyn.

At persondatabeskyttelse har fået større og større betydning indenfor EU-retten kommer bl.a. til udtryk ved, at EU's charter om grundlæggende rettigheder både indeholder en bestemmelse om privatlivets fred i art. 7, og en bestemmelse om beskyttelse af personoplysninger i art 8. Chartret blev vedtaget i 2000, hvilket er fem år efter udstedelsen af persondatadirektivet, og chartret blev juridisk bindende for medlemsstaterne med vedtagelsen af Lissabon-traktaten i 2009. Selv om de konkrete regler om persondata fortsat vil blive fastlagt gennem sekundær ret, har persondatabeskyttelsen fået karakter af en grundlæggende rettighed. Dette har betydning for fortolkningen af persondatareglerne, i og med at der lægges endnu mere vægt på, at der skal ske beskyttelse af persondata, hvilket understreges ved, at EU-Domstolen konsekvent har henvist til chartrets art. 8 ved de seneste afgørelser om fortolkning af persondatadirektivet.²²

Selv om analysen af persondatareglerne tager udgangspunkt i selve Persondataforordningen, vil forståelsen af, at der ligger nogle væsentlige privatlivs- og personlighedshensyn bag reglerne, og at behovet for databeskyttelse er en grundlæggende rettighed - som stadfæstet i chartret - danne en god grobund for analysen af det materielle indhold af forordningens art. 25, stk. 1.

²⁰ Udsen, Henrik. 2016. *IT-ret. Ex Tuto.* 3. udgave, s. 300

²¹ Udsen, Henrik. 2016. *IT-ret. Ex Tuto.* 3. udgave, s. 300

²² Udsen, Henrik. 2016. *IT-ret. Ex Tuto.* 3. udgave, s. 306

2.3. Hvorfor indholdet af bestemmelsen har betydning for de dataansvarlige

Art. 25 er blot én ud af i alt 99 artikler i Persondataforordningen, og derfor kan det måske undre, at netop denne bestemmelse skal underlægges en nærmere analyse.

I og med at bestemmelsen er ny, og at det materielle indhold er uklart, giver det dog god mening at se nærmere på, hvilke krav bestemmelsen sætter til de dataansvarlige. Dette styrkes endvidere af, at overtrædelse af bestemmelsen er bødebelagt, jf. art. 83, stk. 4, litra a.

Overtrædelse af bestemmelsen straffes med administrative bøder på op til 10 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale årlige omkostning i det foregående regnskabsår, såfremt dette beløb er højere, jf. art. 83, stk. 4. Bødens størrelse kan dog reguleres efter de hensyn, der opremses i art. 83, stk. 2, og her nævnes bl.a. "den dataansvarliges eller databehandlerens grad af ansvar under hensyntagen til tekniske og organisatoriske foranstaltninger, som de har gennemført i henhold til artikel 25 og 32", jf. art. 83, stk. 2, litra d.

Det fremgår af præambelbetragtning nr. 150, at forordningen bør angive overtrædelser og maksimumsbeløb og kriterier for fastsættelse af de tilknyttede administrative bøder, der bør bestemmes af den kompetente tilsynsmyndighed i hvert enkelt tilfælde under hensyntagen til alle relevante omstændigheder i den specifikke situation og med behørig hensyntagen til karakteren, alvoren og varigheden af overtrædelsen og dens konsekvenser og de foranstaltninger, der er truffet for at sikre overholdelse af forpligtelserne i henhold til forordningen og for at forebygge eller begrænse følgerne af overtrædelsen.

Persondataforordningens art. 83, stk. 9 tager højde for lande som Danmark, hvor administrative bøder ikke er mulige. Dette fremgår af Grundlovens § 3. Persondataforordningens art. 83, stk. 3 kræver dog, at den kompetente tilsynsmyndighed i så fald tager skridt til bøderne, og at de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af tilsynsmyndighederne. Bøderne skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Det skal her bemærkes, at der i lovforslaget til den nye databeskyttelseslov,²³ derfor er indsat supplerende bestemmelser vedrørende retsmidler, ansvar og sanktioner. Det fremgår her af lovforslagets § 41, stk. 1, nr. 1, at medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder den, der overtræder bestemmelserne om den dataansvarliges og databehandlerens forpligtelser i henhold til databeskyttelsesforordningens art. 8, 11, 25-39, 42 eller 43.

Bestemmelser er dermed identisk med forordningens art. 83, stk. 4, litra a, bortset fra at der ikke her udtrykkeligt nævnes en konkret maksimumbødestørrelse, og at der nu er tale om "almindelige" bøder i stedet for administrative bøder. Det fremgår endvidere af lovforslagets § 41, stk. 2, at forordningens art. 83, stk. 2, skal følges ved pålæggelse af straf efter stk. 1.

I modsætning til de tidligere bødestørrelser, udstedt efter Persondataloven, så er der altså nu tale om betydelige bøder, hvilket de dataansvarlige naturligvis helst vil undgå. Den hidtil største bøde for overtrædelse af Persondataloven er på 25.000 kr., så der er tale om en mærkbar forskel på dette punkt.

At der er uklarhed om det materielle indhold af en bestemmelse, som måske stiller helt nye krav til de dataansvarlige, samtidig med at der kan udstedes betydelige bøder for overtrædelser af bestemmelsen, betyder at en nærmere analyse af bestemmelsens materielle indhold er påkrævet.

2.4. Justitsministeriets betænkning nr. 1565 om forordningen

Den 24. maj 2017 udkom Betænkning nr. 1565/2017 til den nye Persondataforordning. Betænkningen analyserer forordningens krav nærmere og beskriver på den baggrund retlige rammer for dansk lovgivning.

²³ L 68 Forslag til 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).

Justitsministeriet fastlægger i betænkningen, at hverken direktivet eller Persondataloven kræver databeskyttelse gennem design eller databeskyttelse gennem standardindstillinger. Det anerkendes således, at gældende ret ikke indeholder en bestemmelse, der svarer til forordningens art. 25.

Justitsministeriet er dog af den opfattelse, at art. 25 er dækket af flere bestemmelser i gældende ret, og at dens indhold derfor ikke er nyt.²⁴

Justitsministeriet har her fokus på direktivets art. 17, sammenholdt med direktivets præambelbetragtning nr. 46. Præambelbetragtningen fastslår at sikkerhedsforanstaltningerne, der skal træffes jf. direktivets art. 17, skal træffes både under selve udformningen og under iværksættelsen af en behandling. Direktivets art. 17 har overskriften “Behandlingssikkerhed”, og er implementeret i Persondatalovens § 41, stk. 3. Bestemmelsen omtaler de sikkerhedsforanstaltninger, der skal iagttages for at undgå tilintetgørelse, tab eller forringelse af oplysninger samt sikring mod, at data misbruges eller kommer til uvedkommendes kendskab.

Justitsministeriet er af den opfattelse, at begrebet databeskyttelse gennem design implicit er omfattet af § 41, stk. 3 sammenholdt med direktivets art. 17, og at begrebet derfor ikke har et materielt indhold – som går ud over, hvad der allerede gælder.

Justitsministeriet antager, at forordningens art. 25, stk. 1 om databeskyttelse gennem design indebærer en overvejelserforpligtelse om eventuelle sikkerhedstiltag og en håndteringsforpligtelse.²⁵ Selv om Justitsministeriet er af den opfattelse, at forordningens art. 25 skal fortolkes bredt, så har de kun fokus på it-sikkerhed. Og Persondatalovens § 41, stk. 3, som ministeriet sammenligner med, nævner også kun de tekniske og organisatoriske *sikkerhedsforanstaltninger*. Denne bestemmelse omfatter dermed kun it-sikkerhed, såsom den dataansvarliges passende tekniske og organisatoriske foranstaltninger mod tab eller forringelse af data eller mulighed for at data kommer til uvedkommendes kendskab.

Ministeriet kommer ligeledes med et eksempel på en sag fra Datatilsynet, som omhandlede en sag om en hjemmeside, der gav brugeren adgang til en personlig helbredsboks med kobling til

²⁴ Betænkning nr. 1565/2017. *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, s. 420

²⁵ Betænkning nr. 1565/2017. *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, s. 417

helbredsoplysninger fra læger.²⁶ Hjemmesidens login bestod af et brugernavn og en adgangskode, som ikke levede op til de sikkerhedskrav, man måtte forlange til en hjemmeside, der indeholdt så personlige oplysninger. Igen er der fokus på sikkerhed og mulighed for brud på sikkerheden og uvedkommendes adgang til personoplysningerne.

Justitsministeriet inddrager også eksempler på allerede gældende regler om databeskyttelse gennem design i sikkerhedsbekendtgørelsen, som har hjemmel i Persondatalovens § 41, stk. 5. Her nævnes adgangsbegrænsninger som et eksempel.

Derudover inddrages Udtalelse nr. 02/2013 fra Artikel 29-gruppen "om apps i intelligente enheder", hvor de udtaler at "indbygget privatlivsbeskyttelse" ("privacy by design") er et vigtigt princip, som allerede indirekte blev nævnt i databeskyttelsesdirektivet, navnlig i artikel 17 og præambelbetragtning nr. 46, og som sammen med "privatlivsbeskyttelse som standard" ("privacy by default") kommer mere klart frem i e-databeskyttelsesdirektivet.”.

Sammenfattende mener Justitsministeriet derfor ikke, at databeskyttelse gennem design er et nyt begreb inden for persondataretten. Justitsministeriet konkluderer, at "artikel 25 etablerer ikke i sig selv nye krav til den dataansvarlige", da de "allerede følger af gældende databeskyttelsesret", herunder direktivets art. 17 sammenholdt med direktivets præambelbetragtning nr. 46. Dette støttes derudover på nogle bestemmelser i sikkerhedsbekendtgørelsen, udtalelser fra Artikel 29-gruppen og praksis fra Datatilsynet. Det nye er ifølge Justitsministeriet blot, at kravet om databeskyttelse gennem design nu står eksplicit i forordningen.²⁷ Dog betragtes det af Justitsministeriet som en nyskabelse ved bestemmelsen, at den dataansvarlige er forpligtet til at overveje og håndtere, hvorledes denne ved hjælp af tekniske og organisatoriske foranstaltninger kan sikre databeskyttelse gennem design, for derved at efterleve reglerne i databeskyttelsesforordningen allerede på tidspunktet for fastlæggelse af midlerne til en given behandling af personoplysninger.²⁸

²⁶ Afgørelse fra Datatilsynet. Journalnummer 2015-631-0108. Sag mod Cure4you ApS.
<https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/login-til-helbredsoplysninger-paa-sundhedsomraadet/>

²⁷ Betænkning nr. 1565/2017. *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, s. 422

²⁸ Betænkning nr. 1565/2017. *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, s. 422-423

Spørgsmålet er herefter, om databeskyttelse gennem design kun omhandler *sikkerhedsforanstaltninger* som nævnt i Persondatalovens § 41, stk. 3, eller om det er bredere end kun omhandlende sikkerhed.

2.5. Rådet for Digital Sikkerhed

Rådet for Digital Sikkerhed har den 13. november 2017 udgivet en vejledning om databeskyttelse gennem design.²⁹ Rådet er en uafhængig medlemsorganisation med højt specialiseret viden og erfaring om informationssikkerhed og privatlivsbeskyttelse.³⁰

Vejledningen tager udgangspunkt i den oprindelige definition af begrebet, hvilken stammer fra tidligere direktør i det canadiske datatilsyn, Ann Cavoukian. På baggrund af denne definition konkluderes det i vejledningen, at begrebet rækker langt ud over blot at iværksætte tekniske og organisatoriske sikkerhedsforanstaltninger.

Vejledningen kan opfattes som en reaktion på bl.a. Justitsministeriets betænkning, og det fremhæves også i vejledningen, at der fra forskellig side har været en udlægning af begrebet, som om det alene handler om at implementere foranstaltninger, der understøtter it-sikkerhed. I modsætning til Justitsministeriet inddrager Rådet altså den oprindelige definition, når de fortolker begrebet. Begrebet er af Cavoukian opsummeret gennem syv principper, som vil blive gennemgået nærmere senere i analysen.

Med udgangspunkt i disse principper skriver Rådet i vejledningen, at implementering af foranstaltninger der understøtter it-sikkerhed, er en vigtig del af databeskyttelse gennem design, men at det dog kun er ét af de mange formål, som begrebet omfatter. Vejledningen inddrager endvidere ENISA's rapport "Privacy and Data Protection by Design", samt Artikel 29-gruppens rapport "The Future of Privacy", for at komme nærmere ind på begrebets indhold. Rådet konkluderer herefter, at databeskyttelse gennem design har et bredere materielt indhold, der går ud over kun at indtænke it-

²⁹ Rådet for Digital Sikkerheds vejledning om Databeskyttelse gennem Design. Udarbejdet af Rådet for Digital Sikkerhed. 2017. Direkte link til vejledning: <https://static1.squarespace.com/static/5592479ee4b0224fac5497af/t/5a1597bcec212d9bd353bb99/1511364544563/RfDS-vejledning-om-DPbD.pdf>

³⁰ Information om Rådet for Digital sikkerhed fra deres hjemmeside. <http://www.digitalsikkerhed.dk/>

sikkerhed. Vejledningen er dog kort, og går ikke i dybden med, hvad dette bredere indhold indebærer, bortset fra at der gives nogle konkrete eksempler.

Det kan dermed slås fast, at Rådet for Digital Sikkerhed har en anden opfattelse af begrebets indhold end Justitsministeriet.

Rådet får støtte fra Institut for Menneskerettigheder i deres kritik af betænkningens fortolkning af begrebet. Rikke Frank Jørgensen, seniorforsker, og Anja Møller Pedersen, Ph.d.-stipendiat i Forskningsafdelingen hos Institut for Menneskerettigheder, har skrevet en artikel, hvor de påpeger, at regeringen med lovforslaget nedtoner de skærpede krav, herunder kravet om databeskyttelse gennem design.³¹

2.5.1. Rådets formand uddyber uenighed

Formanden for Rådet for Digital Sikkerhed, Henning Mortensen, har skrevet en artikel,³² hvor han nærmere uddyber sin uenighed med Justitsministeriets udlægning af begrebet databeskyttelse gennem design i betænkningen.

Henning Mortensen inddrager bl.a. Artikel 29-gruppen. De har, som han skriver, flere gange udtalt sig om databeskyttelse gennem design og kommet med deres udlægning af begrebet. Artikel 29-gruppens udlægning af begrebet Privacy by Design er ifølge Henning Mortensen meget bredt, og det vil sige, at det omfatter mere end bare sikkerhed.

Kommissionen har ligeledes skrevet om begrebet. Ud fra et fact sheet, Kommissionen har skrevet i 2017, uddrager Henning Mortensen, at begrebet også af Kommissionen betragtes som et nyt begreb, som indeholder mere end bare sikkerhed.

Privacy by Design er som nævnt et begreb, der er introduceret af Ann Cavoukian. Henning Mortensen inddrager hendes fortolkning af begrebet og påpeger, at begrebet af opfinderen indeholder mere end

³¹ Jørgensen, Rikke Frank og Pedersen, Anja Møller. 2017. *Grib chancen for at styrke databeskyttelsen*. <https://menneskeret.dk/nyheder/debat-grib-chancen-styrke-databeskyttelsen>

³² Mortensen, Henning. 2017. Databeskyttelse gennem design – en nyskabelse i databeskyttelsesforordningen? Artikel fra Karnov Group Denmark. RR.2017.12.0064

bare sikkerhed og påpeger, at hendes udlægning af begrebet er anerkendt på den 32. internationale konference for datatilsyn i 2010 og både Datatilsynet og EDPS (European Data Protection Supervisor) henviser til hendes udlægning af begrebet.

Henning Mortensens konklusion i artiklen er, at databeskyttelse gennem design har et bredere materielt indhold, der går ud over kun at omhandle sikkerhedskrav. Hvis dette ikke er tilfældet, er bestemmelsen overflødig, da begrebet i så fald kun vil finde anvendelse, når det samtidig understøtter nogle af de øvrige målsætninger i forordningen, som f.eks. sikkerhedsbestemmelsen i forordningens art. 32. Hvis begrebet har et bredere materielt indhold, som kan opfylde mere end bare sikkerhedskrav i forordningen, vil det derimod være med til at sikre, at de registrerede får den beskyttelse, som de burde kunne forvente ud fra forordningen.

2.6. Hvad handler uenigheden i virkeligheden om?

Både Henning Mortensen og Justitsministeriet henviser til mange af de samme kilder, og ved en hurtig gennemlæsning kan det være svært at få øje på, hvad uenigheden i virkeligheden drejer sig om. Inden der gås i dybden med begrebet, skal uenigheden derfor først kort koges ned, således at analysen har et klart udgangspunkt.

Justitsministeriet påstår som tidligere nævnt, at databeskyttelse gennem design allerede er omfattet af gældende regler. De henviser her til direktivets art. 17, sammenholdt med direktivets præambelbetragtning nr. 46. Dette støttes også af Udtalelse nr. 02/2013 fra Artikel 29-gruppen, hvor de siger, at princippet allerede indirekte blev nævnt i databeskyttelsesdirektivet, navnlig i art. 17 og præambelbetragtning nr. 46.

Henning Mortensen anerkender, at begrebet ikke er ukendt i gældende ret, og at de foranstaltninger, der er blevet henvist til under begrebet, fortrinsvist har haft sit udspring i sikkerhedsbestemmelsen i persondatadirektivets art. 17. På dette punkt er Henning Mortensen dermed ikke uenig med Justitsministeriet. Henning Mortensen er dog af den opfattelse, at begrebet går længere end det.

Uenigheden er derfor om begrebet databeskyttelse gennem design rækker længere, end det allerede gjorde implicit gennem sikkerhedsbestemmelsen i persondatadirektivets art. 17. Persondatadirektivets

art. 17 omhandler behandlingssikkerhed, hvilket i Persondataforordningen reguleres efter art. 32. Hvis databeskyttelse gennem design, allerede er dækket fuldt ud i denne bestemmelse i gældende ret, så begrænses begrebet til kun at omhandle de sikkerhedsforanstaltninger, som falder ind under anvendelsesområdet for art. 17. Det vil med andre ord sige, at begrebet ikke har noget bredere materielt indhold end at omhandle sikkerhed, og derfor ikke i sig selv etablerer nye krav til den dataansvarlige.

Det bliver derfor helt afgørende for den videre analyse at få defineret, hvad en sikkerhedsforanstaltning er.

2.7. Hvad er en sikkerhedsforanstaltning?

En sikkerhedsforanstaltning er ikke klart defineret i hverken forordningen eller i direktivet. I direktivet findes den såkaldte sikkerhedsbestemmelse, der har overskriften behandlingssikkerhed i art. 17, mens den i forordningen findes i art. 32. Bestemmelserne gennemgås nedenfor.

I direktivets art. 17, stk. 1 om registeransvarlige (i forordningen ændret til dataansvarlige) er blot omtalt tekniske og organisatoriske foranstaltninger. I art. 17, stk. 2 som omhandler registerfører (i forordningen ændret til databehandlere), omtales derimod de tekniske *sikkerhedsforanstaltninger* og organisatoriske foranstaltninger. Så for databehandlere er det ikke kun tekniske foranstaltninger, men tekniske *sikkerhedsforanstaltninger*. Der er altså en sproglig forskel, men det må antages, at der ikke er en forskel i indholdet af de to bestemmelser, idet forskellen vurderes til blot at skulle være, om der er tale om en dataansvarlig eller en databehandler.

I art. 17, stk. 1, er nævnt “...tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang...”. Altså handler foranstaltningerne om sikkerhed – nærmere bestemt sikkerhed mod tilintetgørelse, tab, forringelse, udbredelse eller uautoriseret adgang. Der er dermed fokus på beskyttelse.

Direktivets art. 17, stk. 1 og 2 er implementeret i Persondatalovens § 41 stk. 3. Både direktivets art. 17 og Persondatalovens § 41 har overskriften behandlingssikkerhed.

De passende tekniske og organisatoriske foranstaltninger er dermed i denne sammenhæng sat ind under overskriften *Behandlingssikkerhed*. Hvad definitionen på denne behandlingssikkerhed er, tydeliggøres dog ikke nærmere.

I forordningens art. 32, stk. 1. er nævnt at “...den dataansvarlige og databehandleren (skal gennemføre) passende tekniske og organisatoriske foranstaltninger for at sikre et *sikkerhedsniveau*, der passer til disse risici...”. Der er ikke nævnt udtrykket sikkerhedsforanstaltninger i forordningens art. 32, men jf. direktivets art. 17, stk. 1 og 2 antages det, at der ikke er forskel på tekniske og organisatoriske foranstaltninger og sikkerhedsforanstaltninger i dette tilfælde, hvilket også bekræftes af, at vi stadig befinder os under overskriften behandlingssikkerhed.

Sikkerhedsforanstaltningerne skal altså sikre et *sikkerhedsniveau*, der passer til risiciene. Og hvordan skal dette sikkerhedsniveau vurderes?

Her det relevant at se på forordningens art. 5, som bærer overskriften Principper for behandling af personoplysninger. I art 5, stk. 1, litra f er beskrevet, hvordan passende tekniske og organisatoriske foranstaltninger kan bruges til at sikre opfyldelse af, at personoplysningerne “behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse”. Der er her ingen definition af, hvad der er tilstrækkelig sikkerhed, men der gives eksempler på, hvad det tilstrækkelige sikkerhedsniveau skal beskytte.

I forordningens præambel 83 kommes med en vurdering af, hvordan det “tilstrækkelige sikkerhedsniveau” opnås. Den dataansvarlige eller databehandleren skal ved vurdering af det ønskede sikkerhedsniveau tage “...forhold til risiciene og karakteren af de personoplysninger, der skal beskyttes...” i betragtning. Den ansvarlige kan ligeledes ved vurderingen tage “...hensyn til de risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger...”.

Det tilstrækkelige sikkerhedsniveau skal altså vurderes ud fra de risici, der er ved den pågældende behandling. Og hvordan skal disse risici vurderes?

I følge art. 35, stk. 1 skal den dataansvarlige “Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder...” udarbejde en konsekvensanalyse for at se på aktivitetens “...konsekvenser for beskyttelse af personoplysninger.”.

I art. 35, stk. 3 er nævnt eksempler på situationer, hvor der skal udarbejdes en konsekvensanalyse. Med den er kun vejledende. Lovgiver har altså her givet en vurdering af, hvornår der menes at være høj risiko.

Af præambel 84 fremgår, at “Resultatet af analysen bør tages i betragtning, når der skal træffes passende foranstaltninger med henblik på at påvise, at behandlingen af personoplysningerne overholder denne forordning.”. Konsekvensanalysen kan altså anvendes som værktøj til at vurdere risiciene ved den aktuelle behandling og dermed hjælpe til at sikre et tilstrækkeligt sikkerhedsniveau, som omtalt i præambel 83.

I forordningens art 32, stk. 1, litra a-d kommes der ligeledes med eksempler på, hvad der kan sikre det optimale sikkerhedsniveau. Men det er kun eksempler, så ingen steder kan der fås de præcise kriterier til et tilstrækkeligt sikkerhedsniveau og dermed kan der ikke laves en klar definition af begrebet sikkerhedsforanstaltning. Dog kan det siges at være en foranstaltning, der sikrer det tilstrækkelige sikkerhedsniveau. Det tilstrækkelige sikkerhedsniveau kan der heller ikke kommes en klar definition på, men det er en individuel vurdering, der skal laves på baggrund af de reelle risici og de risici kan findes og vurderes bl.a. på baggrund af en konsekvensanalyse. Sikkert er det, at der ved tekniske og organisatoriske foranstaltninger tænkes på foranstaltninger, der skal sikre sikkerheden.

Som det fremgår af ovenstående gennemgang, så findes der ikke en konkret definition på, hvad en sikkerhedsforanstaltning er. Men det er åbenbart, at den vedrører sikkerhed, og der er fokus på beskyttelse mod f.eks. tilintetgørelse, tab, forringelse, udbredelse eller uautoriseret adgang. Disse eksempler nævnes både i direktivet og forordningen, og giver dermed et godt billede af, hvordan sikkerhed generelt skal forstås.

Det betyder, at hvis princippet om databeskyttelse gennem design går udover kun at omhandle ovennævnte sikkerhedsforanstaltninger, og dermed går videre end at være et krav om, at systemerne

skal designes således, at der sikres mod tilintetgørelse, tab, forringelse mv., så er der netop tale om et nyt krav, som ikke fuldt ud er dækket af de hidtil gældende bestemmelser i direktivet og Persondataloven.

For at finde ud af om dette er tilfældet, skal der derfor gås i dybden med begrebet databeskyttelse gennem design. I det følgende skal selve begrebet udforskes ved at gennemgå både dets oprindelse, samt hvordan det hidtil er blevet fortolket. Begrebet stammer som tidligere nævnt fra canadieren Ann Cavoukian, hvor det er kendt under det engelske udtryk Privacy by Design.

2.8. Ann Cavoukians Privacy by Design begreb

Ann Cavoukian har i en rapport³³ til den 33. internationale konference for datatilsyn skrevet om Privacy by Design (PbD). Herunder hvad status er og hvordan det kan anvendes til at sikre beskyttelse af privatliv.

Cavoukian omtaler privatliv som en social norm. En norm er inden for sociologisk videnskab et begreb, der henviser til regler eller værdier, som er ønskelige eller forventet adfærd. En norm er altså, hvordan vi ønsker, at ting skal foregå.

Når Cavoukian således skriver, at privatliv er en norm, så mener hun, at det er det, samfundet ønsker, og sådan det bør være. Det vil sige, at vi ønsker alle privatliv og det er det, der bør være normen og dermed det, vi stræber efter.

Cavoukian mener, at nøglen til at nå målet om beskyttelse af privatliv er at benytte PbD.

Fordelen er, at alle interessenters behov tilfredsstilles ved benyttelse af PbD. Borgere får beskyttet deres privatliv og virksomheder får tilfredse kunder og vil have en fordel over andre virksomheder, som ikke beskytter deres brugeres privatliv. En myte har ifølge Cavoukian været, at beskyttelse af privatliv kvæler innovationen, men dette er ikke sandt, idet et af principperne i PbD netop er fuld

³³ Cavoukian, Ann. 2011. Privacy by Design, Strong Privacy Protection – Now, and Well into the Future, A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners. <https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf>

funktion samtidig med beskyttelse, og det kræver et højt niveau af innovation at sikre opfyldelse af begge krav.

I følge Cavoukian ønsker borgere privatliv, uagtet om der er lovgivning om beskyttelse heraf eller ej, og derfor handler PbD altså om mere end blot opfyldelse af loven.

Cavoukian udtaler, at PbD søger at give kontrollen til brugerne, men at det alligevel skal ses som en positiv ting for virksomhederne også, da det hjælper virksomhederne til at se privatlivsbeskyttelse som en omkostningsbesparende konkurrencefordel og ikke som en byrde pålagt af lovgiver.

Cavoukian skriver netop om at inkorporere PbD i lovgivningen, som det er sket med forordningen. Cavoukian mener, at dette vil kræve "...an approach to privacy that is () broader..." og målet er "...to have privacy woven directly into business processes in much the same way that other core values such as fairness, transparency, and proportionality, are". Virksomheder skal altså omfavne beskyttelse af privatliv og gøre det til en naturlig del af deres virksomhed og ved at inkorporere PbD i lovgivningen, kan det være med til at påvirke og sikre, at virksomheder anvender PbD.

Ann Cavoukian har flere gange skrevet og udtalt, at PbD handler om mere end blot opfyldelse af loven. Det handler om at opfylde normen, som altså er beskyttelse af privatliv. Dette kan være krævet i lovgivningen, men midlerne hertil er ikke altid klart defineret. Det er derfor, at et af principperne til PbD netop er, at der skal tænkes proaktivt. Det vil sige, hvordan optimal beskyttelse af brugernes privatliv sikres. PbD kan hjælpe til at sikre beskyttelse af brugernes privatliv, men kan ikke hjælpe med at løse problemer, når først de er opstået. PbD er altså et middel til at undgå, at problemer opstår - ikke et middel til at løse dem.

2.8.1. Gennemgang af de syv principper

Ann Cavoukian har introduceret begrebet Privacy by Design og har i den forbindelse udviklet syv principper til uddybelse af indholdet i begrebet.

De syv principper er:

1. Proaktiv, ikke reaktiv

Foranstaltninger skal altså iværksættes inden en risiko materialiserer sig.

2. Privacy som standardindstilling

Den registrerede skal ikke selv foretage sig noget for at beskytte sine oplysninger; beskyttelsen skal være slået til fra starten.

3. Privacy skal være indlejret i systemet

Foranstaltningerne skal designes ind i et systems arkitektur og ikke tilføjes efterfølgende.

4. Der skal være fuld funktionalitet

Der skal være fuld funktionalitet. Det må ikke være sådan, at man kan få begrænset funktionalitet, der er sikker, kontra fuld funktionalitet, hvis man opgiver sin sikkerhed. Generelt må der ikke være en modstrid mellem sikkerhed og databeskyttelse.

5. Beskyttelse i hele livscyklussen

Beskyttelsen skal indbygges i designfasen inden systemet sættes i drift og være aktiv i hele systemets levetid.

6. Transparens

Der skal være gennemsigtighed i forretningsmodeller og teknologier, og det der signaleres, skal kunne verificeres (af en uafhængig tredjepart).

7. Brugeren i centrum

De registreredes interesser skal være i fokus f.eks. gennem standardindstillinger, notifikation og empowerment af brugerne, så de er i kontrol.

Cavoukian har uddybet indholdet af de syv begreber i teksten "Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices".

Med det første begreb er det intentionen, at PbD skal være proaktivt. Det vil sige, at PbD kan anvendes til at hjælpe med privatlivsbeskyttelse. Men det kan ikke hjælpe med en løsning på et brud på beskyttelsen. Cavoukians bud på hvordan første punkt opfyldes er, at alle parter føler sig forpligtet til at sikre en høj standard af privatlivsbeskyttelse - ikke kun i designfasen men konstant, så der sikres en kultur, hvor der konstant er fokus på forbedring af privatlivsbeskyttelse. Altså er det ikke kun i udviklingsfasen, at der skal tænkes proaktivt. Det er i hele livscyklussen fra vugge til grav, at der skal

indtænkes privatlivsbeskyttelse. Det handler om hele tiden at være på forkant med den konstante udvikling. En måde hvorpå det kan sikres, er, at der udvikles metoder til at sikre identifikation af punkter, hvor et system ikke lever op til krav om privatlivsbeskyttelse.

Privacy by Default skal sikre privatliv, ved at information kun anvendes til godkendte formål. Beskyttelse af privatliv kræver altså ikke en aktiv handling, men er standard. Dette opfyldes ved, at der ved dataindsamling gives en kort og klar beskrivelse af, hvorfor data indsamles og til hvilken brug. Der skal være fokus på dataminimering og således kun indsamles nødvendige data og så vidt muligt ikke identificerbare data. Det skal sikres, at data kun anvendes til de godkendte formål og kun opbevares, så længe de er nødvendige for opfyldelse heraf.

For opfyldelse af det tredje princip skal privatliv være indlejret i systemet. Det skal være tænkt ind fra starten og må ikke være en senere tilføjelse. Dette gøres ved at anvende anerkendte standarder, som kan revideres af udefrakommende og skal indtænkes i alle steps af designet og udviklingen af et system. På den måde er det sikkert, at der hele tiden indtænkes privatliv i systemet, så det ikke er noget, der bliver tilføjet senere, når hele systemet til sidst er designet og udviklet. Ved at have fokus på det fra starten bliver det en naturlig del af systemet og ikke en senere ugennemtænkt tilføjelse.

Det fjerde princip er vigtig også ud fra et økonomisk synspunkt. Det indebærer, at der skal ses på privatlivsbeskyttelse som en positiv ting for alle parter. Der er ikke tale om enten eller. Det er både og. Der kan altså sagtens både være fuld funktionalitet og beskyttelse af privatliv. Det må ikke kræve kompromis med beskyttelsen af privatliv at få fuld funktionalitet.

Det femte princip omhandler beskyttelse i hele livscyklussen - fra indsamling af data til sletning. Beskyttelse opnås ved høj sikkerhed, som skal gælde for hele cyklussen.

Princippet om synlighed og gennemsigtighed gælder for alle parter og skal kunne verificeres af en uafhængig tredjepart. Det er vigtigt, at man kan stole på en part, som der udleveres data til. Denne tiltro sikres gennem en klar politik for opbevaring og behandling af data, som kommunikeres åbent til den registrerede.

Brugeren i centrum er det syvende princip. Det handler altså hele tiden om, at brugeren skal være i centrum. Der skal være konstant fokus på at gøre det bedste for brugeren. Brugeren skal f.eks. give klart og tydeligt samtykke til indsamling, brug og udlevering af data. Det vil sige, at det ikke skal være skjult eller blot uklart, hvad der gives samtykke til. Og det skal være muligt nemt at tilbagetrække sit samtykke.

Som det fremgår af ovennævnte er PbD i følge Ann Cavoukian meget mere end blot en sikkerhedsforanstaltning. Dataminimering handler f.eks. ikke direkte om sikkerhed. Der kan sagtens være en høj sikkerhed, men anmodes om data, som egentlig ikke er nødvendige. Såfremt der indsamles data, som ikke er nødvendige, opfyldes altså ikke Privacy by Design i det et af kravene til princip to om Privacy by Default er dataminimering.

Det er altså Ann Cavoukian, der har udviklet og forfinet begrebet Privacy by Design, herunder ved udvikling af de syv principper. Hverken Ann Cavoukian eller hendes syv principper er nævnt i betænkningen, så om Justitsministeriets fortolkning og forståelse af begrebet er i overensstemmelse med Cavoukians, har været uklart, men der er stillet spørgsmål hertil af Retsudvalget, hvorfor der i det følgende skal ses nærmere på udvalgets spørgsmål og Justitsministeriets svar herpå.

2.9. Ministerspørgsmål og svar

I forbindelse med den nye Databeskyttelseslov, som er under behandling i folketinget, er der fra Folketingets Retsudvalg stillet en række spørgsmål til Ministeren. Spørgsmål 8, 9, 10, 11, 12, 30 og 31 omhandler direkte eller indirekte databeskyttelse gennem design. Besvarelsen til alle spørgsmål er dog i besvarelsen til spørgsmål 8 og 10, idet der i besvarelsen til de andre spørgsmål henvises til besvarelsene til spørgsmål 8, 10 eller begge.

Retsudvalget har efter ønske fra Zenia Stampe fra Radikale Venstre stillet spørgsmål til, om Ministeren er opmærksom på, at flere organisationer, herunder Rådet for Digital Sikkerhed, har påpeget vigtigheden af, at databeskyttelse gennem design fortolkes i overensstemmelse med Ann Cavoukians syv principper.³⁴ I svaret fra Justitsministeren lægges der vægt på, at der i betænkningen henvises til

³⁴ Udvalgsspørgsmål fra Retsudvalget til L 68 og L 69, spørgsmål 8

Artikel 29-gruppens udtalelser om begrebet og denne henvisning netop er lavet, fordi det fra Justitsministeriets side anerkendes, at det er vigtigt, at der sikres en fælles europæisk forståelse af begrebet og det er denne Justitsministeriet anvender. Selvom Ann Cavoukians syv principper ikke nævnes direkte i betænkningen, er der alligevel indirekte henvist til dem, da man omtaler Artikel 29-gruppen, der bruger principperne som en central del i forståelsen af begrebet. Justitsministeriet fastslår således, at de syv principper er gældende i forståelsen af begrebet og at de vil være med til udfyldelsen af begrebet fremadrettet.

Ministeriet påpeger, at artikel 25 skal ses i sammenhæng med de øvrige bestemmelser i forordningen, men særligt art. 5, 32 og 35. Ministeriet fastholder deres holdning fra betænkningen og mener således ikke, at der er nogen grund til ændring af deres udlæggelse, men bekræfter, at det er et vigtigt element til forebyggelse af eventuelle sikkerhedsbrud. Sammenfattende kan det forstås, at der stadig ses på databeskyttelse gennem design, som noget der skal sikre sikkerheden.

Selvom der ikke lægges op til en ændring af udlæggelsen i betænkningen, skrives der dog i svaret om nye krav, der kommer i forbindelse med forordningen ”... herunder f.eks. databeskyttelse gennem design”. Så det anerkendes her, at det er et nyt krav, selvom udlægningen i betænkningen er, at der ikke er tale om noget nyt. I betænkningen skriver Ministeriet, at det kun er nyt, at det står eksplicit, men at det også fremgik i direktivet, blot implicit. Der kan altså opstå forvirring på baggrund af svaret, men det må forstås sådan, at Ministeren fastholder, hvad der står i betænkningen.

Retsudvalget har efter ønske fra Zenia Stampe ligeledes stillet spørgsmål til, hvordan Ministeren vil sikre styrkelse af retten til privatliv og en bedre it-sikkerhed, hvis nye begreber i forordningen ikke skal anvendes af virksomhederne.³⁵ Dette spørgsmål er stillet i forlængelse af ovennævnte og afspejler spørgers forståelse af, at Ministeren ikke lægger op til en nyskabelse og nedtoner betydningen af begrebet og dets anvendelse. Der er yderligere i den sammenhæng stillet spørgsmål til, om Ministeren ikke gør virksomhederne en bjørnetjeneste ved at nedtone nyskabelsen i databeskyttelse gennem design.³⁶ Ministerens svar på dette er, at begrebet ikke nedtones i betænkningen og at der i betænkningen er lavet et grundigt analysearbejde, der vil hjælpe med forståelsen. Derudover henviser

³⁵ Udvalgsspørgsmål fra Retsudvalget til L 68 og L 69, spørgsmål 10

³⁶ Udvalgsspørgsmål fra Retsudvalget til L 68 og L 69, spørgsmål 9

Ministeren til, at der kommer en vejledning fra Datatilsynet og Justitsministeriet til forståelsen af begrebet.

Retsudvalget har efter ønske fra Zenia Stampe også stillet spørgsmål til, om Ministeren mener, at databeskyttelse gennem design bør være et konkurrenceparameter.³⁷ Til dette er der blot svaret, at det er Ministeriets håb, at dette vil ske. Ministeriet har ikke umiddelbart svaret på forlængelsen af spørgsmålet, der er, hvordan Danmark kan være med til at fremme dette. Databeskyttelse gennem design som et konkurrenceparameter vil blive analyseret nærmere i den økonomiske analyse.

Sammenfattende ud fra de spørgsmål, der er stillet af Retsudvalget, kan det udledes at også Retsudvalget har en bredere forståelse af begrebet databeskyttelse gennem design, og at de mener, at det er et vigtigt begreb, som Ministeriet i betænkningen har nedtonet betydningen af. Dog fastholder Ministeriet sin udlægning og mener ikke, at der er tvivl om fortolkningen, da der er lavet en grundig analyse i betænkningen, og de understreger at de ikke nedtoner databeskyttelse gennem design i denne.

Nogle af de spørgsmål der er stillet af retsudvalget, kommer Ministeriet let udenom, og nogle bliver ikke rigtig besvaret, men det skal også understreges, at det er de samme personer, der besvarer spørgsmålene, som har lavet betænkningen. Der kommer på baggrund af de stillede spørgsmål og svarene hertil ikke nogen nærmere afklaring af begrebet, andet end at det bekræftes, at Ann Cavoukians syv principper efter Ministeriets opfattelse kan anvendes til forståelse af begrebet.

Da Ministeriet i begge sine svar henviser til den vejledning om databeskyttelse gennem design og standardindstillinger, der udarbejdes af Datatilsynet og Justitsministeriet i fællesskab, må det antages, at begrebet nærmere specificeres i den. Netop Datatilsynets holdning til begrebet er interessant, i og med at Datatilsynet er den nationale tilsynsmyndighed i Danmark. Det er derfor relevant at inddrage denne.

³⁷ Udvalgsspørgsmål fra Retsudvalget til L 68 og L 69, spørgsmål 12

2.10. Tilsynsmyndigheder

Forordningen kapitel 2 omfatter kompetence, opgaver og beføjelser. Det fremgår af forordningens art. 55, at der i landende er en tilsynsmyndighed, der "...er kompetent til at udføre de opgaver og udøve de beføjelser, der tillægges den i overensstemmelse med denne forordning, på sin egen medlemsstats område". Tilsynets opgaver fremgår af art. 57 og jf. stk. 1, litra a er tilsynets opgave bl.a. at "føre tilsyn med og håndhæve anvendelsen af denne forordning".

Tilsynsmyndighederne vil derfor have en helt afgørende betydning for, hvordan Persondataforordningen bliver håndhævet og fortolket i praksis.

2.10.1. Det danske datatilsyn

Tilsynsmyndigheden i Danmark er som nævnt Datatilsynet. De har indtil videre ikke udtalt sig konkret om begrebet databeskyttelse gennem design i forbindelse med forordningen.

Datatilsynet har dog tidligere givet anbefalinger om anvendelse af Privacy by design. I et høringssvar til et lovforslag fra Digitaliseringsstyrelsen om obligatorisk selvbetjening, anbefalede Datatilsynet, at princippet skulle anvendes.³⁸ Ligeledes kan nævnes Datatilsynets udtalelse over Økonomi- og Indenrigsministeriets lovforslag om digitale vælgererklæringer, hvor Datatilsynet henstiller til, at designet af den pågældende løsning skulle ændres i en mere privatlivsfremmende retning.³⁹ I udtalelsen nævnes princippet dog ikke direkte.

Derudover kan der henvises til et par sager, hvor Datatilsynet indirekte kan siges at anvende princippet. Her kan nævnes sagen mod Irmatorvet A/S, hvor det blev slået fast, at rækkevidden af sikkerhedsbestemmelsen i Persondatalovens § 41, stk. 3, også omfatter testen af et it-system inden det sættes i drift.⁴⁰ Derudover kan nævnes den tidligere nævnte sag mod Cure4you ApS, hvor sikkerheden for at leve op til Persondatalovens § 41, stk. 3, skulle forbedres, så der ikke var mulighed for at logge ind kun med brugernavn og adgangskode.⁴¹ Der er dog i disse sager tale om foranstaltninger, der har sit

³⁸ Datatilsynets j.nr. 2013-112-0268, Datatilsynets høringssvar vedrørende høring over lovforslag om "bølge 3", 17. december 2013

³⁹ Datatilsynets j.nr. 2013-112-0252, Udtalelse over lovforslag om digitale vælgererklæringer

⁴⁰ Afgørelse fra Datatilsynet. Journalnummer 2011-631-0133. Sag mod Irmatorvet A/S

⁴¹ Afgørelse fra Datatilsynet. Journalnummer 2015-631-0108. Sag mod Cure4you ApS

udspring i sikkerhedsbestemmelsen i direktivets art. 17, hvilket Henning Mortensen også påpeger i sin artikel.

Datatilsynets fortolkning af forordningens implementering af princippet forventes at blive klarlagt i den vejledning, som udarbejdes i samarbejde med Justitsministeriet. Vejledningen skulle udkomme i februar 2018, men er nu flere gange blevet udskudt. Det var oprindeligt planen at inddrage vejledningen i nærværende afhandling, men dette blev desværre ikke muligt.

På den anden side er det allerede oplyst, at vejledningen udarbejdes i samarbejde med Justitsministeriet. Det må derfor forventes, at vejledningen i hvert fald ikke vil være i direkte modstrid med det, som allerede fremgår af Justitsministeriets betænkning om begrebet, samt de tidligere gennemgåede ministersvar. Da Justitsministeriet har erkendt i ministersvarene, at begrebet skal fortolkes i overensstemmelse med Ann Cavoukians principper, vil disse højst sandsynligt inddrages. Det vil dog være interessant at se, om de fastholder påstanden i betænkningen om, at art. 25 i forordningen ikke i sig selv etablerer nye krav til de dataansvarlige.

I og med at forordningen skal sikre en fælles europæisk forståelse af begrebet, skal i det følgende ses på, hvordan tilsynsmyndigheder i andre lande, som implementerer forordningen, forholder sig det.

2.10.2. Det britiske datatilsyn

Selv om Storbritannien har valgt at forlade EU, så er de stadigvæk en del af fællesskabet, når forordningen træder i kraft den 25. maj. Storbritannien har også erklæret, at de vil overholde forordningen, og at dette ikke vil blive påvirket af Brexit.⁴² I Storbritannien er det Information Commissioner's Office (ICO), der er tilsynsmyndighed.

ICO har udgivet en oversigt over Persondataforordningen, hvor de også kort kommer ind på kravet om Privacy by Design. I oversigten skriver de, at princippet altid har været et implicit krav af Data

⁴² Vejledning udarbejdet af ICO 20. oktober 2017. *Overview of the General Data Protection Regulation (GDPR)*, s. 3

Protection Act (DPA), som ICO konsekvent har ført tilsyn med.⁴³ DPA er den britiske persondatalov, der implementerer persondatadirektivet.

Oversigten fra ICO ser dermed ud til at nedtone nyskabelsen af begrebet, hvilket Justitsministeriet som nævnt også er beskyldt for. ICO henviser dog i oversigten til en tidligere vejledning, som de har udarbejdet i forbindelse med overholdelse af DPA. Vejledningen er senest opdateret i februar 2018, men selve afsnittet om Privacy by Design er ældre.⁴⁴ I denne vejledning ses der på, hvad Privacy by Design indeholder, og hvordan det kan anvendes. I vejledningen skriver de, i modsætning til den tidligere nævnte oversigt, at kravet om Privacy by Design ikke er et krav efter DPA, men at det kan ses som et redskab til at opfylde andre krav i lovgivningen.⁴⁵ I vejledningen beskrives Privacy by Design som en tilgang til design, hvor både privatliv og databeskyttelse skal indtænkes fra start af, og vejledningen inddrager også Ann Cavoukians syv grundlæggende principper. ICO henviser stadigvæk til denne vejledning på deres hjemmeside, men det oplyses samtidig, at de er i gang med at opdatere vejledningen, så den afspejler bestemmelserne i forordningen.

Det interessante ved ovenstående er, at der ikke er overensstemmelse mellem ICO's egne udlægninger af begrebet. Mens Privacy by Design er meget bredt og omfattende, og ikke en del af gældende persondataret ifølge vejledningen, så har samme begreb pludselig hele tiden været implicit omfattet af gældende ret, når det omtales i oversigten, som er udarbejdet i forbindelse med den nye forordning.

2.10.3. Det norske datatilsyn

Norge er ikke med i EU, men Persondataforordningen vil alligevel gælde i Norge. Tilsynsmyndigheden i Norge er det norske datatilsyn.

Det norske datatilsyn har publiceret en artikel om "Syv steg til innebygd personvern".⁴⁶ Artiklen omhandler netop "De syv stegene (som) er ment for deg som er bestiller, kravstiller, utvikler, leverandør eller på annen måte er involvert i utvikling av IT-verktøy som behandler

⁴³ Vejledning udarbejdet af ICO 20. oktober 2017. *Overview of the General Data Protection Regulation (GDPR)*, s. 30

⁴⁴ Vejledning udarbejdet af ICO 8. februar 2018. *The Guide to Data Protection*.

⁴⁵ Vejledning udarbejdet af ICO 8. februar 2018. *The Guide to Data Protection*., s. 128

⁴⁶ Artikel på det norske datatilsyns hjemmeside. 2017. *Syv steg til innebygd personvern*. <https://www.datatilsynet.no/regelverk-og-skjema/lage-nye-losninger/innebygd-personvern/>

personopplysninger." Datatilsynet skriver, at som dataansvarlig eller databehandler "må du også forholde deg til kravene i personopplysningsloven." (Bemærk at må på norsk, betyder skal).

De syv trin som det norske datatilsyn omtaler, er de syv principper defineret af Ann Cavoukian om Privacy by Design. Det norske datatilsyn laver altså en sammenkobling mellem overholdelse af forordningen og Ann Cavoukians udlægning af Privacy by Design og hendes syv principper.

I artiklen er de syv principper defineret og der er eksempler til alle principperne. Til princip 2 kommer det norske datatilsyn med et eksempel om browsere med "Do Not Track" som standardindstilling, hvilket medfører at browseren automatisk giver besked til de internetsider brugeren besøger, at denne ikke ønsker at blive sporet. Såfremt brugeren rent faktisk ønsker at blive sporet, skal brugeren aktivt selv ændre i indstillinger og godkende sporing. Eksemplet her handler ikke om sikkerhed, men blot om beskyttelse af brugerens privatliv. Til princip 3 kommer tilsynet med et eksempel om at for at undgå unødigt indsamling af data, kan der i et program laves en drop down liste, hvor brugeren kan vælge mellem relevante oplysninger i stedet for et frit tekstfelt, hvor der kan skrives hvad som helst. På den måde sikres det, at der kun er relevant data i feltet og at der ikke indsamles mere data end nødvendigt. Igen ikke et decideret sikkerhedskrav, men blot et tiltag der skal sikre, at der ikke indsamles mere information end nødvendigt - altså dataminimering.

Som Henning Mortensen skriver i sin artikel, ser det umiddelbart ud til, at det norske datatilsyn lægger op til "...et materielt indhold i bestemmelsen, som rækker ud over sikkerhedsbestemmelsen.", og med det mener han, at Privacy by Design indeholder et materielt indhold, der rækker ud over sikkerhedsbestemmelsen i art. 17 i direktivet.

Ifølge det norske datatilsyn er det dermed ikke umiddelbart nok til overholdelse af forordningens art. 25, at sikkerheden er i top og krav hertil i forordningen overholdt. Der skal mere til.

Datatilsynets holdning til begrebet er yderst relevant, da det er deres opgave at håndhæve forordningens bestemmelser og dermed deres holdning til begrebet, der i første omgang bliver gældende.

Dog er det vigtigt at huske på, at Norge ikke er medlem af EU. Dette er relevant, da det dermed ikke er muligt at anlægge sag mod Norge ved EU-domstolen. Norge har altså forpligtet sig til at følge forordningen, men Kommissionen har ikke mulighed for at føre kontrol hermed og kan ikke anlægge sag mod Norge ved EU-domstolen for manglende overholdelse af forordningen, som de normalt kan jf. TEUF art. 258. Norges domstole har heller ikke mulighed for jf. TEUF art. 267 at stille præjudicielle spørgsmål til Domstolen, hvorfor Domstolen ikke har mulighed for at påvirke eller bestemme, hvordan Norge skal fortolke begrebet.

Ovenstående gennemgang af tilsynsmyndighedernes udlægning af begrebet har vist, at selv om der kommer blandede signaler, så inddrages Ann Cavoukians principper i både Storbritanniens og Norges praktiske vejledninger til begrebet. Storbritanniens udlægning er interessant, i og med at de ligesom de danske myndigheder kan anklages for at nedtone nyskabelsen i begrebet i forbindelse med forordningen.

Inden der skal laves en fortolkning af begrebet, skal der i det følgende ses på, hvordan ENISA og Artikel-29 gruppen har forholdt sig til begrebet, da deres fortolkning har betydning og forventes inddraget af EU-Domstolen.

2.11. ENISA

ENISA (The European Union Agency for Network and Information Security) er et center for ekspertise for internetsikkerhed i Europa. ENISA hjælper EU og EU-landene med at være bedre rustet til og forberedt på at forhindre, opdage og imødegå problemer med informationssikkerhed. ENISA er oprindeligt oprettet jf. forordning 460/2004, men er nu reguleret jf. forordning 526/2013. Agenturets mål og opgaver fremgår henholdsvis af forordningens art. 2 og 3. Heraf fremgår det bl.a., at ENISA skal hjælpe EU's institutioner, organer m.m. med at udarbejde politikker inden for ENISAs områdefelt jf. art. 2, stk. 2 og hjælpe til udviklingen af EU's lovgivning ved at bistå og rådgive ved spørgsmål inden for deres område jf. art. 3, stk. 1. ENISAs fortolkning af Privacy by Design er dermed yderst relevant, da det er en del af deres opgaver at bistå med spørgsmål inden for netop dette område og det dermed må forventes, at Domstolen vil tage ENISAs udlægning af begrebet i betragtning, når de senere skal vurdere det i en sag, ligesom de danske myndigheder inddrager ENISA i bl.a. betænkningen.

Agenturet har udarbejdet rapporten "Privacy and Data Protection by Design – from policy to engineering". Rapporten er udarbejdet i 2014.

Vejen til at opnå Privacy by Design er af flere beskrevet som mulig ved indførelse af såkaldte PETs (Privacy Enhancing Technologies). PETs er defineret af Blarkom, Borking og Olk i bogen *Handbook of Privacy and Privacy Enhancing Technologies* som "a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."⁴⁷

Ifølge ENISA er "Privacy by design () a multifaceted concept: in legal documents on one hand, it is generally described in very broad terms as a general principle; by computer scientists and engineers on the other hand it is often equated with the use of specific privacy-enhancing technologies (PETs). However, privacy by design is neither a collection of mere general principles nor can it be reduced to the implementation of PETs."⁴⁸ Indførelse af PETs er således ikke nok til opfyldelse af Privacy by Design. ENISA skriver videre, at det er en proces som ved involvering af forskellige teknologiske og organisatoriske foranstaltninger sikrer privatliv og databeskyttelse. Der er altså tale om en proces, der indeholder elementer af både noget teknisk og noget organisatorisk. Ligesom beskrevet i forordningens art. 25.

ENISA påpeger at privacy- og databeskyttelsesprincipperne kan uddrages af lovgivningen, men som der påpeges er lovgivningen typisk uklar med hensyn til en definition. Privacy by Design handler altså bl.a. om opfyldelse af nogle principper fastsat i lov, men som ENISA dog anerkender, ofte er udefinerede. ENISA påpeger dog, at der kommer hjælp til dette med forordningen, idet de skriver, at forordningen "provides useful indications with regard to objectives and evaluations of a privacy-by-design process, including data protection impact assessment, accountability and privacy seals."⁴⁹

⁴⁷ Van Blarkom, G.W., Borking, JJ og Olk, J.G.E. 2003. *Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents*. College bescherming persoonsgegevens, s. 33

⁴⁸ Rapport udarbejdet af ENISA. 2014/2015. *Privacy and Data Protection by Design – from policy to engineering*, s. 3

⁴⁹ Rapport udarbejdet af ENISA. 2014/2015. *Privacy and Data Protection by Design – from policy to engineering*, s. 3

Privacy by Design omhandler ifølge ENISA klart ikke kun sikkerhed, i det de skriver, at "The concepts of privacy and data protection must not be reduced to protection of data. In fact, the concepts have to be understood more broadly: they address the protection of human beings and their personal rights as well as democratic values of society." ⁵⁰

ENISA anvender Cavoukians principper som grundlag for forståelse af, hvad Privacy by Design indeholder. ENISA påpeger, at der har været en forståelse af, at PETs kunne anvendes som en løsning på problemer med sikring af privatliv ved blot at tilføje PETs på eksisterende systemer. Men som de skriver, er det næppe løsningen. De mener, at Ann Cavoukians syv principper derimod er med til at tydeliggøre, hvordan privatliv kan sikres og hvad Privacy by Design indeholder som begreb. ENISA mener især, at det tydeliggøres ved, at privatliv skal indtænkes i systemer som et forebyggende og proaktiv tiltag, der skal sikre, at der slet ikke opstår problemer med sikring af privatliv. ENISA kritiserer dog Cavoukian for, at de syv principper mere karakteriserer rettigheder, end de giver præcise instruktioner for, hvordan det skal sikres, at princippet overholdes. Som Henning Mortensen også skriver i sin artikel, har Cavoukian dog selv været opmærksom på dette og kommet med sit bud på implementering af Privacy by Design i *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*.

ENISA introducerer otte design strategier, der er afledt af Hoepman⁵¹. De otte design strategier er opdelt i først fire dataorienterede strategier og derefter fire procesorienterede strategier. Strategierne fremgår figur 2.1.

Til de otte strategier kommer ENISA også med eksempler på, hvordan programmer kan designes, så de overholder strategierne.

⁵⁰ Rapport udarbejdet af ENISA. 2014/2015. *Privacy and Data Protection by Design – from policy to engineering*, s. 3.

⁵¹ Hoepman, Jaap-Henk. 2014. Privacy design strategies – (extended abstract). In *ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*, s. 446–459

Figur 2.1.

Strategy #1: MINIMISE

The most basic privacy design strategy is MINIMISE, which states that the amount of personal data that is processed should be restricted to the minimal amount possible.

Strategy #2: HIDE

The second design strategy, HIDE, states that any personal data, and their interrelationships, should be hidden from plain view.

Strategy #3: SEPARATE

The third design strategy, SEPARATE, states that personal data should be processed in a distributed fashion, in separate compartments whenever possible.

Strategy #4: AGGREGATE

The fourth design pattern, AGGREGATE, states that Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.

Strategy #5: INFORM

The INFORM strategy corresponds to the important notion of transparency. Data subjects should be adequately informed whenever personal data is processed.

Strategy #6: CONTROL

The control strategy states that data subjects should be provided agency over the processing of their personal data.

Strategy #7: ENFORCE

The seventh strategy, ENFORCE, states: A privacy policy compatible with legal requirements should be in place and should be enforced.

Strategy #8: DEMONSTRATE

The final strategy, DEMONSTRATE, requires a data controller to be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

Af de otte strategier er der nogen, der har mere med sikkerhed at gøre end andre. F.eks. strategi 5 og 6 der omhandler information og kontrol til den registrerede/brugeren, minder om Cavoukians syvende princip og har umiddelbart intet med sikkerhed at gøre. På den baggrund kan det udledes, at ENISA også plæderer for, at Privacy by Design er mere end blot sikkerhed.

2.12. Artikel 29-gruppen

I medfør af Persondatadirektivets art. 29 er der nedsat en "gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger", den såkaldte "Artikel 29-gruppe".

Artikel 29-gruppen er rådgivende og uafhængig og består af en repræsentant for den eller de tilsynsmyndigheder, som hver medlemsstat har udpeget, og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne, samt af en repræsentant for

Kommissionen. Gruppens opgaver fremgår af art. 30 og omfatter bl.a. sikring af ensartet anvendelse af direktivet jf. art. 30, stk. 1, litra a. Derfor er Artikel 29-gruppens udtalelser relevante, også selvom de ikke længere vil eksistere efter forordningens ikrafttrædelse. Dog vil Det Europæiske Databeskyttelsesråd blive oprettet jf. forordningens art. 68 og artikel 29-Gruppens udtalelser vil fortsat være gældende som udtalelser fra Det Europæiske Databeskyttelsesråd jf. forordningens art. 94, stk. 2. Så alt udarbejdet af Artikel 29-gruppen fastholder sin gyldighed.

Det interessante ved Artikel 29-gruppens udtalelser er, at både Justitsministeriet og Henning Mortensen har inddraget dem i deres analyser af begrebet.

Justitsministeriet inddrager som tidligere nævnt Udtalelse nr. 02/2013 fra Artikel 29-gruppen "om apps i intelligente enheder". Det fremgår af denne, at Privacy by Design er et vigtigt princip, som allerede indirekte blev nævnt i databeskyttelsesdirektivet, navnlig i art. 17 og præambelbetragtning nr. 46.

Det er dermed ingen tvivl om, at selve princippet indirekte blev nævnt i databeskyttelsesdirektivet, og dette er der ikke uenighed om. Spørgsmålet er dog, om Artikel 29-gruppen deler Justitsministeriets opfattelse af, at bestemmelsen i art. 25 ikke i sig selv etablerer selvstændige krav til den dataansvarlige, i og med at princippet allerede følger af gældende databeskyttelsesret.

Som det fremgår af Henning Mortensens artikel, har Artikel 29-gruppen i flere omgange udtalt sig om begrebet. I rapporten "The Future of Privacy" fra 2009, som Justitsministeriet også henviser til i betænkningen, slår Artikel 29-gruppen fast, at databeskyttelsesdirektivets art. 17 sammenholdt præambelbetragtning 46 ikke har vist sig at være tilstrækkeligt til at sikre, at databeskyttelse indlejres i IT-produktet og services.⁵²

Artikel 29-gruppen plæderer derfor i rapporten for, at der introduceret et nyt og bredt Privacy by Design begreb, som ikke blot skal omhandle sikkerhed, men også minimere behandlingen af

⁵² Artikel 29-gruppens udtalelse om "The Future of Privacy", vedtaget den 1. december 2009, (WP 168), s.13, nr. 45.

personoplysninger.⁵³ Denne rapport er som sagt fra 2009, og Artikel 29-gruppen har løbende udtalt sig om og uddybet, hvad de forstår med begrebet Privacy by Design.

Som det også fremgår af Henning Mortensens artikel, anvendes begrebet overordnet i nogle sammenhænge som en del af sikkerhedsbestemmelsen i art. 17 sammenholdt med præambelbetragtning 46, hvilket fokus er på i Justitsministeriets betænkning. Men i andre tilfælde anvendes det også til at fastslå, at der skal implementeres foranstaltninger i hele livscyklussen for et produkt, og derudover anvendes det også som en opsamlingsbestemmelse for en hel række konkrete designtiltag, som skal iværksættes i konkrete sammenhænge, og som går ud over at vedrøre sikkerhed, herunder Internet of Things og droner.

Som det fremgår af ovenstående gennemgang, så er der meget, der taler for, at begrebet databeskyttelse gennem design skal fortolkes bredere, end hvad tilfældet er i betænkningen. Dette kan understøttes ved at se på begrebets oprindelse, samt hvordan det indtil videre er fortolket af bl.a. Artikel 29-gruppen og ENISA. Men i sidste ende er det hverken Artikel 29-gruppen, ENISA, Datatilsynet eller Justitsministeriet, der kommer til at få det afgørende ord, når bestemmelsen skal fortolkes, men EU-domstolen.

2.13. EU-Domstolens hidtidige praksis

Som det fremgår af ovenstående analyse, så er der bred enighed om, at princippet om databeskyttelse gennem design ikke er ukendt i gældende databeskyttelsesret. EU-domstolen har derfor haft mulighed for at tage stilling til begrebet.

Som det fremgår af professor Lee A. Bygrave's publikation i Oslo Law Review, hvor begrebet analyseres, så har EU-Domstolen indtil videre hverken udtalt sig direkte om indholdet af art. 25, eller

⁵³ Artikel 29-gruppens udtalelse om "The Future of Privacy", vedtaget den 1. december 2009, (WP 168), s.13, nr. 43.

afsagt en dom, som de facto kræver databeskyttelse gennem design.⁵⁴ EU-domstolen har dog afsagt nogle domme, som baner vejen for internetrelateret teknologiudvikling.

De første eksempler er to sager fra Belgien.⁵⁵ Her nægtedes Belgien at indføre 'pakkekontrol' på internettet, med det formål at imødegå digital piratkopiering. Selv om domstolen afholdt sig fra aktivt at promovere databeskyttelse gennem design, standsede den i dommene effektivt udbredelsen af privatlivsindtrængende teknologi.

Et andet eksempel er den kendte Google Spain dom⁵⁶, som også skal analyseres nærmere senere. I dommen blev det slået fast, at søgemaskiners aktiviteter skal betragtes som behandling af personoplysninger, og at udbyderen af en søgemaskine derfor skal anses for at være en dataansvarlig. Domstolen afviste dermed Googles argumenter om, at søgemaskiner blot er værdineutrale, robot-applikationer af algoritmer, som falder udenfor anvendelsesområdet for databeskyttelsesretten. Selv om dommen ikke medførte noget væsentligt krav om databeskyttelse gennem design, i og med at Google f.eks. ikke blev pålagt at indføre "hardwiring" af privatlivets interesser i søgemaskinen, så medførte dommen, at Google og andre søgemaskineoperatører måtte genfigurere systematiske aspekter af deres operationer, så de er mere privatlivsvenlige. På den måde blev formålet med art. 25 også i denne dom indirekte promoveret.⁵⁷

Som det fremgår af Lee A. Bygrave's publikation i Oslo Law Review, så har Den Europæiske Menneskerettighedsdomstol (EMD), i modsætning til EU-domstolen mere direkte promoveret databeskyttelse gennem design. Dette skete allerede tilbage i 2008 i sagen I v Finland.⁵⁸

⁵⁴ Bygrave, Lee A. 2017. *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*. Forskningspublikation udgivet i Oslo Law Review. Scandinavian University Press. Volume 4, No. 2-2017, pp. 105–120. ISSN online: 2387-3299. S. 111

⁵⁵ Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Sag C-70/10. EU:C:2011:771 og SABAM v Netlog. Case C-360/10. EU:C:2012:85

⁵⁶ Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González. Sag C-131/12. EU:C:2014:317

⁵⁷ Bygrave, Lee A. 2017. *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*. Forskningspublikation udgivet i Oslo Law Review. Scandinavian University Press. Volume 4, No. 2-2017, pp. 105–120. ISSN online: 2387-3299. S. 111

⁵⁸ Appl. No. 20511/03, Judgment of July 2008

I dommen blev Finland dømt for brud på art. 8 i den europæiske menneskerettighedskonvention (EMRK). Artiklens stk. 1 svarer næsten ord for ord til chartrets art. 7.

EU er ikke medlem i Europarådet og er ikke kontraherende part i EMRK. EU kan derfor ikke direkte blive kontrolleret af EMD. Derimod er alle medlemsstaterne forpligtede af EMRK og som nationalstater underlagt EMD's kontrol.⁵⁹ Med Lissabon-Traktaten fik EU eksplicit hjemmel til at ratificere EMRK, hvilket fremgår af art. 6, stk. 2 TEU. EU-Domstolen havde været af den opfattelse, at EU ikke kunne ratificere EMRK, men EU-Domstolen har alligevel anset EMRK som en integreret del af EU-retten, og den har i de sidste 10-15 år i stigende grad henvist til EMRK i sine afgørelser.⁶⁰ EU-Domstolen har således lært og ladet sig inspirere af EMRK. Det er derfor meget relevant at se på, hvordan EMD har forholdt sig til begrebet databeskyttelse gennem design.

I den nævnte sag blev Finland dømt til at have overtrådt sine forpligtelser efter art. 8 i EMRK til at sikre respekt for privatlivet. Der var ikke gennemført de nødvendige teknologiske og organisatoriske foranstaltninger, til at sikre patientdata på et hospital.

Klageren var en kvinde, der var smittet med HIV, og som havde mistanke om, at tredjepersoner havde fået uautoriseret adgang til hendes lægejournaler. Klagen vedrørte hovedsageligt det forhold, at det pågældende hospital havde et sundhedsregistersystem uden en mekanisme som dokumenterede, hvem der havde fået adgang til oplysningerne, således at det efterfølgende kunne efterprøves, om denne havde behørig tilladelse.

Selv om der efter finsk ret var beskyttelse til patientdata, herunder erstatning til de registrerede for skader, de havde lidt i tilfælde af uautoriseret adgang til oplysningerne, fastslog EMD, at Finland måtte yde mere end databeskyttelse de jure for at opfylde sine positive forpligtelser i henhold til EMRK art. 8.

Det blev slået fast i dommen, at der var krav om en praktisk og effektiv beskyttelse, for at udelukke enhver mulighed for uautoriseret adgang i første omgang. Muligheden for at kræve erstatning for en

⁵⁹ Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, s. 199

⁶⁰ Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, s. 198

påstået ulovlig adgang til personoplysninger efterfølgende, var ikke tilstrækkeligt. En sådan beskyttelse blev ikke givet her, og det var derfor sket brud på EMRK art. 8.

Selvom Domstolen ikke henviste til selve begrebet databeskyttelse gennem design eller lignende i dommen, så er dommen et eksempel på tankegangen, som bærer dette princip. Dog anvendes princippet i forbindelse med beskyttelse mod uautoriseret adgang, som dermed kan siges at omhandle en sikkerhedsforanstaltning.

Ifølge Lee A. Bygrave medfører dommens resultat, at databeskyttelse gennem design er en integreret del af en stats positive forpligtelser til at sikre respekt for de rettigheder, der er fastsat i EMRK art. 8, i hvert fald når det har med personers sundhed at gøre.⁶¹

2.14. EU-domstolens fortolkning

Det er EU-Domstolen, der kommer til at have det sidste ord, når indholdet af Persondataforordningens art. 25 skal afklares. Da bestemmelsen er helt ny, har EU-Domstolen ikke haft mulighed for at tage stilling til dens indhold endnu. Og som det fremgår af ovenstående, så har EU-domstolen heller ikke direkte udtalt sig om begrebet i sin hidtidige praksis. Det vil derfor blive spændende at se, hvordan EU-Domstolen vil forholde sig til bestemmelsens omfang og indhold.

EU-Domstolen har dog en kendt og systematisk fortolkningsstil. Det er derfor muligt at anvende denne fortolkningsstil på et juridisk problem, og på den måde komme frem til en vurdering af, hvordan EU-Domstolen ville håndtere problemet.

Med udgangspunkt i den foregående analyse, skal EU-Domstolens fortolkningsstil i det følgende anvendes på Persondataforordningens art. 25, stk. 1 og begrebet databeskyttelse gennem design.

⁶¹ Bygrave, Lee A. 2017. *Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements*. Forskningspublikation udgivet i Oslo Law Review. Scandinavian University Press. Volume 4, No. 2-2017, pp. 105–120. ISSN online: 2387-3299. S. 110

EU-Domstolen redegjorde for dens fortolkningsstil i CILFIT-sagen.⁶² Fortolkningsstilen begynder med en bestemmelses ordlyd på samtlige autentiske sprog, og hvis denne ikke er klar, gås der videre til sammenhængen, målsætningen og EU-rettens udviklingstrin.⁶³ På persondatarettens område har EU-Domstolen derudover anvendt udtrykket internettets udviklingstrin, hvilket der også skal ses nærmere på.

2.14.1. Ordlyd

Det skal først og fremmest tages hensyn til den omstændighed, at EU-retten er affattet på forskellige sprog, og at alle versioner er autentiske. Udgangspunktet for enhver fortolkning er altid en tekst, og fortolkningen af en EU-bestemmelse kan derfor kun ske efter en sammenligning af de sproglige versioner.⁶⁴ Derudover skal der her tages hensyn til, at EU-retten anvender et særligt sprogbrug, og at indholdet af dette ikke nødvendigvis er det samme som i de nationale retsordener.⁶⁵

Det skal derfor undersøges, om ordlyden af bestemmelsen på de forskellige sprog giver klarhed, eller skaber mere tvivl. EU har for tiden 24 officielle sprog, men det skal i det følgende kun fokuseres på de tre proceduremæssige sprog: Engelsk, fransk og tysk – udover det danske. Det skal her bemærkes, at persondatareglerne generelt er meget bredt formulerede, hvilket er en naturlig følge af, at de regulerer et felt, der konstant er under stor udvikling. Der anvendes brede udtryk, og henvises i flere omgange til "det aktuelle tekniske niveau" mv. Derfor vil det næsten aldrig være tilstrækkeligt kun at se på en bestemmelses rene ordlyd.

Inden hele bestemmelsen skal koges ned og analyseres, skal der først ses på dens overskrift og hovedtræk.

Bestemmelsens overskrift og hovedtræk

Begrebet databeskyttelse gennem design fremgår explicit kun af selve overskriften for art. 25, hvor den danske overskrift er "Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger".

⁶² Srl CILFIT og Lanificio di Gavardo SpA mod Sundhedsministeriet, Sag 283/81, EU:C:1982:335

⁶³ Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, side 136-137

⁶⁴ Srl CILFIT og Lanificio di Gavardo SpA mod Sundhedsministeriet, Sag 283/81, EU:C:1982:335, præmis 18

⁶⁵ Srl CILFIT og Lanificio di Gavardo SpA mod Sundhedsministeriet, Sag 283/81, EU:C:1982:335, præmis 19

Inde i selve bestemmelsen anvendes dette udtryk ikke direkte. I den engelske version hedder overskriften "Data protection by design and by default", i den tyske hedder den "Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" og i den franske lyder den således "Protection des données dès la conception et protection des données par défaut". Det er dermed ikke tvivl om, at selve udtrykket databeskyttelse gennem design er ens i disse fire sproglige definitioner.

Det bemærkes, at der er ikke valgt at anvende det oprindelige udtryk fra Ann Cavoukian. Hun arbejder som tidligere nævnt med udtrykket Privacy by Design, som på dansk kan oversættes til privatliv gennem design. Som tidligere redegjort for, så er Ann Cavoukians version af begrebet bredere end kun omhandlende sikkerhedsforanstaltninger.

Det kan argumenteres for, at fremmelsen af privatliv gennem design er mere omfattende end at fremme databeskyttelse gennem design. Et eksempel er dataminimering, som betyder, at oplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles, og som er et af principperne i forordningens art. 5.

Dataminimering i sig selv går ud over kun at omfavne databeskyttelse, da der sagtens kan være høj grad af databeskyttelse, uden at den indsamlede data bliver slettet, når formålet er bortfaldet, eller hvis der er indsamlet flere data end nødvendigt. Hvis systemet derimod var designet således, at de indsamlede data, udover at være beskyttede mod uønsket adgang, også automatisk blev slettede, når formålet med behandlingen var bortfaldet, så ville systemet være designet til at indeholde både beskyttelse af data, og beskyttelse af individets privatliv. Ud fra en sådan ren ordlydsfortolkning af selve begrebet, kan der argumenteres for, at der bevidst er valgt et mindre omfattende begreb, end det som Ann Cavoukian arbejder med.

I samme retning kan der argumenteres for, at de syv punkter i Ann Cavoukians version ikke skal indfortolkes i EU-begrebet, da der explicit er taget stilling til, præcis hvad er omfattet i art. 25, stk. 1 inde i selve bestemmelsen. I Ann Cavoukians version af begrebet er Privacy by Default f.eks. en integreret del af Privacy by Design, hvorimod databeskyttelse gennem standardindstillinger er en selvstændig tilføjelse til EU-begrebet i forordningens art. 25, stk. 2. Således kan der argumenteres for, at der udtrykkeligt er taget stilling til, hvilke af de syv punkter der er omfattet, og hvilke ikke er.

Med baggrund i ovenstående kan der efter en ordlydsfortolkning af begrebet argumenteres for, at databeskyttelse gennem design er et selvstændigt EU-retligt begreb, der ikke skal holdes op imod Ann Cavoukians Privacy by Design.

På den anden side kan der argumenteres for, at databeskyttelse netop er et meget bredt begreb i EU-retten, og at dette naturligvis også omfatter andet, end kun hvad der fremmer ren beskyttelse af data. Forordningens officielle navn er netop databeskyttelsesforordningen, og forordningen indeholder flere bestemmelser, som går ud over kun at omhandle selve beskyttelsen af de indsamlede data, bl.a. det tidligere nævnte princip om dataminimering i art. 5. Dette taler for, at begrebet databeskyttelse skal anvendes bredt, og derfor er det også naturligt at vælge at anvende udtrykket databeskyttelse gennem design, i stedet for privatliv gennem design, uden at dette skal fortolkes som et fravalg af det sidstnævnte. Derudover bliver dataminimering udtrykkeligt nævnt som et eksempel på databeskyttelse gennem design i forordningens art. 25, stk. 1, hvilket også taler imod, at databeskyttelse gennem design skal betragtes som et smallere begreb end Ann Cavoukians Privacy by Design, selv om det har fået et andet navn i forordningen.

2.14.2. Sammenhæng og helhed

For det andet skal reglerne vurderes i deres rette sammenhæng og fortolkes i lyset af EU-rettens bestemmelser som helhed.

Hvis der ses på, hvor i forordningen begrebet ellers er nævnt, henvises i forordningens præambelbetragtning 78 og 108 til ”*principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger*”. Persondataforordningens art. 47, som omhandler bindende virksomhedsregler, nævner derudover i stk. 2, litra d, anvendelsen af ”generelle databeskyttelses*principper*, navnlig (...) databeskyttelse gennem design og databeskyttelse gennem standardindstillinger”.

Dette taler for, at der i art. 25 henvises til et princip, som er blevet udviklet løbende, og som nu er indarbejdet i forordningen, og ikke et selvstændigt EU-retligt begreb, der skal adskilles fra det oprindelige begreb om Privacy by Design. Det vil derfor give god mening at se nærmere på, hvor dette princip stammer fra, og hvad det indeholder, for at finde ud af, hvad begrebet omfatter, som gjort i

ovenstående analyse. Med andre ord er der brug for at gå udover bestemmelsens ordlyd, når bestemmelsen skal fortolkes.

Selv om der efter en ren ordlydsfortolkning af begrebet kan argumenteres for, at databeskyttelse gennem design er et selvstændigt EU-retligt begreb, der er smallere end det oprindelige Privacy by Design, så er der flere nuancer i ordlyden, der taler for det modsatte, og disse bliver forstærket, når bestemmelsens sammenhæng og helhed bliver inddraget. I og med at art. 25 generelt er formuleret meget bredt, og at forordningen andre steder henviser til et generelt princip om databeskyttelse gennem design, giver dette en stærk opfattelse af, at begrebets udvikling og oprindelse er relevant, når begrebet skal fortolkes, og at det derfor ikke er nok, kun at se på selve ordlyden af bestemmelsen. Som det fremgår af denne afhandlings analyse af begrebets baggrund og hidtidige anvendelse, så anvender både ENISA og Artikel 29-gruppen Ann Cavoukians begreb i deres rapporter og vejledninger, hvilket også taler for, at en ren ordlydsfortolkning af begrebet ikke er tilstrækkelig.

Det er også den generelle opfattelse i teorien, at begrebet Privacy by Design og forordningens udtryk databeskyttelse gennem design på mange måder er synonyme.⁶⁶

Der vil dog alligevel være nogle små forskelle i de to begreber. Som det fremgår af ovenstående analyse, så arbejder Ann Cavoukian med et begreb, der ikke kun omfatter god skik for databeskyttelse, men også går udover det. Princippet skal være med til at "...significantly raise the bar of legal norms". Ann Cavoukian henviser nok her til de love og retningslinjer, der gælder i de nordamerikanske databeskyttelseslovgivninger. På den måde er Ann Cavoukians princip i udgangspunktet noget, der adskiller sig fra lovgivningen. Det er dog intet i vejen for, at princippet i forordningens art. 25, stk. 1 indebærer det samme niveau af Privacy by Design, som Ann Cavoukians version, selvom det nu er indsat i selve lovgivningen. På den anden side kan princippet i forordningen også gå endnu længere end de nordamerikanske opfattelser Privacy by Design, hvor begrebet jo er adskilt fra en lovgivning, der måske ikke kræver et særligt højt niveau af databeskyttelse.⁶⁷

⁶⁶ Rapport udarbejdet af ENISA. 2014/2015. *Privacy and Data Protection by Design – from policy to engineering*

⁶⁷ Bygrave, Lee A. 2017. *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*. Forskningspublikation udgivet i Oslo Law Review. Scandinavian University Press. Volume 4, No. 2-2017, pp. 105–120. ISSN online: 2387-3299. S. 115-116

Ved at have set på ordlyden, og ved at have inddraget sammenhængen og helheden, har vi dermed fået et godt billede af bestemmelsens overskrift og hovedtræk. På baggrund af ovenstående giver det god mening, at EU har valgt at gå med begrebet databeskyttelse gennem design, når princippet indsættes i lovgivningen. Selv om princippet uden tvivl skal læses i sammenhæng med Ann Cavoukians oprindelige begreb, så er der samtidigt ikke risiko for, at begrebet forveksles med eventuelle mindre omfattende, og juridisk ikke-bindende versioner af Privacy by Design.

For at komme nærmere selve indholdet af forordningens princip om databeskyttelse gennem design, skal bestemmelsens nærmere indhold analyseres.

Bestemmelsens nærmere indhold

Der skal i det følgende ses nærmere på både ordlyden af art. 25, stk. 1 og den relevante sammenhæng og helhed.

Bestemmelsen er lang, og det kan være svært at danne sig et overblik. Derfor skal den koges ned, således at de enkelte dele analyseres hver for sig.

Under hensyntagen til det aktuelle tekniske niveau mv.

Første del af bestemmelsen sætter rammerne for, hvad der skal tages hensyn til, når databeskyttelse gennem design skal anvendes. Her nævnes både eksterne og interne faktorer, som påvirker, hvordan princippet skal anvendes. Det afhænger for det første af det aktuelle tekniske niveau, som er en ekstern faktor, der hele tiden vil ændre sig. Derudover afhænger det også af mere interne faktorer, som f.eks. den pågældende handlings karakter, omfang, sammenhæng og formål. Rammerne opstilles dermed således, at kravet om databeskyttelse gennem design bliver dynamisk, og dets indhold vil variere alt efter de konkrete omstændigheder. Selve rammerne siger dog intet om det materielle indhold af kravet.

Passende tekniske og organisatoriske foranstaltninger

Det nærmere indhold af kravet fastlægges derefter ved, at den dataansvarlige skal gennemføre "passende tekniske og organisatoriske foranstaltninger".

Begrebet tekniske og organisatoriske foranstaltninger er bredt, og anvendes flere steder i forordningen. Det betyder dog ikke, at begrebet har det samme indhold i alle sammenhænge, det bliver anvendt. Begrebet anvendes også i sikkerhedsbestemmelsen i persondatadirektivets art. 17, hvor det som tidligere nævnt var anvendt med fokus på sikkerhedsforanstaltninger, i og med at de skulle tilvejebringe et tilstrækkeligt sikkerhedsniveau. I Persondataforordningen anvendes begrebet også i art. 5, stk. 1, litra f og i art. 32 stk. 1, hvor det på samme måde som i Persondatadirektivets art. 17 anvendes i relation til behandlingssikkerhed.

Men begrebet anvendes også i andre sammenhænge, hvor det ikke kun vedrører sikkerhedsforanstaltninger. F.eks. kan nævnes art. 28, stk. 3 litra e, hvor det fremgår, at databehandleren skal bistå den dataansvarlige med passende tekniske og organisatoriske foranstaltninger, med at opfylde den dataansvarliges forpligtelse til at "besvare anmodninger om udøvelse af de registreredes rettigheder".

Efter art. 5, stk. 1, litra e, som fastsætter et princip om opbevaringsbegrænsning, skal der implementeres passende tekniske og organisatoriske foranstaltninger "for at sikre den registreredes rettigheder og frihedsrettigheder". Begrebet anvendes ligeledes i forbindelse med sikring af rettigheder og frihedsrettigheder og generelt at kravene i Persondataforordningen overholdes i art. 24, stk. 1 og art. 28, stk. 1. Begrebet må derfor anses at have et mere vidtgående indhold, når det anvendes til at sikre disse overordnede og brede formål. Det konkrete indhold af de passende tekniske og organisatoriske foranstaltninger vil dermed afhænge af, i hvilken sammenhæng de bliver nævnt.

For at finde ud af, hvad disse foranstaltninger indebærer i forbindelse med databeskyttelse gennem design, er de næste punkter i bestemmelsen derfor særlig relevante.

Implementering af databeskyttelsesprincipper

Det fremgår for det første, at foranstaltningerne skal være designet med henblik på "effektiv implementering af databeskyttelsesprincipper". Det er derfor nødvendigt at se på, hvad implementering af databeskyttelsesprincipper indebærer.

Der gives et konkret eksempel på et databeskyttelsesprincip i bestemmelsen, som er dataminimering. Princippet nævnes også i art. 5, stk. 1, litra c, som et generelt princip, og går ud på, at personoplysningerne skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles. Princippet er gennemgået ovenfor i afsnittet om bestemmelsens overskrift og hovedtræk, hvor der argumenteres for, at princippet omfatter mere end sikkerhed.

Dataminimering er dog kun ét eksempel på de databeskyttelsesprincipper, som bestemmelsen skal sikre effektiv implementering af. I præambelbetragtning 78 nævnes, at sådanne foranstaltninger kan bl.a. bestå af minimering af behandling af personoplysninger (dataminimering), pseudonymisering og "gennemsigtighed for så vidt angår personoplysningers funktion og behandling". Princippet om gennemsigtighed nævnes også i art. 5, stk. 1, litra a, og indebærer, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

Implementering af databeskyttelsesprincipper må derfor også anses som et bredt krav. Databeskyttelse gennem design kræver, at alle databeskyttelsesprincipper i forordningen skal sikres, og det afhænger ikke af, om de relaterer sig til sikkerhedsforanstaltninger eller noget mere end det – f.eks. gennemsigtighed.

Integrering af de fornødne garantier i behandlingen

For det andet, skal foranstaltningerne være designet med henblik på "integrering af de fornødne garantier i behandlingen". Det er dermed ikke nok kun at sikre implementering af selve databeskyttelsesprincipperne. De øvrige fornødne garantier i behandlingen skal også integreres som følge af kravet om databeskyttelse gennem design. Her er det igen relevant at se på, hvad integrering af garantier i behandlingen indebærer.

Der gives hverken i selve bestemmelsen eller i præambelbetragtning 78 eksempler på disse garantier i behandlingen. Ordet garanti er dog ikke ukendt i Persondataforordningen, i og med at det anvendes

flere steder. Som eksempler kan nævnes anvendelse af bindende virksomhedsregler,⁶⁸ kontraktmæssige forpligtelser⁶⁹ samt kryptering og pseudonymisering af oplysninger.⁷⁰ Garantier må derfor opfattes som et meget bredt begreb, som både bliver brugt som supplement til foranstaltninger og inkluderende foranstaltninger.⁷¹

For at opfylde kravene i denne forordning og beskytte de registreredes rettigheder

Til sidst i bestemmelsen fastlægges formålet med det ovenfor forklarede begreb, hvilket både er "...at opfylde kravene i denne forordning og beskytte de registreredes rettigheder". Der er altså tale om et meget bredt formål. Dette er som sagt også formålet med de passende og organisatoriske foranstaltninger, der nævnes i art. 24, stk. 1 og 28, stk. 1. Der er dermed meget, der tyder på, at de tekniske og organisatoriske foranstaltninger i denne sammenhæng skal fortolkes bredere, end det f.eks. skal i sikkerhedsbestemmelsen i Persondatadirektivets art. 17 og Persondataforordningens art. 31, stk. 1. Dette vil derfor blive analyseret nærmere under en formålsfortolkning af bestemmelsen nedenfor.

En ordlydsfortolkning med inddragelsen af den relevante sammenhæng og helhed giver ikke et helt entydigt svar på det materielle indhold af bestemmelsen. Bestemmelsen er meget bredt formuleret og meget tyder på, at begrebet skal fortolkes bredere end kun omhandlende sikkerhedsforanstaltninger.

2.14.3. Formål

For det tredje skal bestemmelsen fortolkes i lysets af det bagvedlæggende formål med reglerne. Dette er et vigtigt element, da EU's formål har stor retlig betydning. Hovedreglen er, at EU-ret fortolkes teleologisk, og EU-Domstolen søger derfor at fortolke en bestemmelse i overensstemmelse med, hvad der mest effektivt kan realisere bestemmelsens målsætning.⁷² Her har EU-Domstolen benyttet

⁶⁸ 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), herefter kaldet Databeskyttelsesforordningen, præambelbetragtning 108

⁶⁹ Databeskyttelsesforordningen, præambelbetragtning 109

⁷⁰ Databeskyttelsesforordningen, art. 6, stk. 4, litra e

⁷¹ Mortensen, Henning. 2017. *Databeskyttelse gennem design – en nyskabelse i databeskyttelsesforordningen?* Artikel fra Karnov Group Denmark. RR.2017.12.0064, s. 5

⁷² Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, s. 139

traktaternes formålsbestemmelser som hjælpemiddel til fortolkning i flere sager.⁷³ Det skal bemærkes, at selvom formålsbestemmelser ikke er direkte anvendelige i medlemsstaterne, så er de forpligtende for alle, der anvender EU-ret, og dette gælder også for nationale myndigheder og domstole, f.eks. når der anvendes EU-konform fortolkning.⁷⁴

2.14.3.1. Overordnet formål med persondatareglerne

Som nævnt i det indledende afsnit om baggrunden for persondatareglerne, så bygger persondatareglerne grundlæggende både på et privatlivs- og et personlighedshensyn, hvor individet er i fokus. Det fremgår også af formålsbestemmelsen i forordningens art. 1, stk. 2, at forordningen ”beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger”. Det er altså først og fremmest fysiske personers grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes.

Når der laves en formålsfortolkning, er det vigtigt også at holde for øje, at persondatabeskyttelse er en grundlæggende rettighed, der er traktatfæstet i chartrets art. 8. Domstolen har konsekvent henvist til denne artikel ved de seneste afgørelser om fortolkning af persondatadirektivet,⁷⁵ hvorfor det også er relevant at se på, hvilke hensyn der inddrages i disse afgørelser, når denne fortolkningsstil skal overføres til art. 25 i Persondataforordningen.

2.14.3.2. Google Spain-dommen

Et godt eksempel på, at EU-Domstolen kan gå langt for at beskytte de registreredes rettigheder, er den tidlige nævnte Google Spain-dom.⁷⁶ I denne dom fik en spansk statsborger medhold i, at Google havde pligt til at slette to links, som blev vist på resultatlisten, når der søgtes på vedkommendes navn. Siderne var fra en spansk avis, og omhandlede en tvangsauktion over fast ejendom i forbindelse med en beslaglæggelse på grund af gæld til den sociale sikringsordning. Det var hverken tale om forkerte eller ulovligt indsamlede oplysninger.

⁷³ Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, s. 139

⁷⁴ Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, s. 140

⁷⁵ Udsen, Henrik. 2016. *IT-ret*. Ex Tuto. 3. udgave, s. 306

⁷⁶ Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González. Sag C-131/12. EU:C:2014:317

Persondatadirektivet indeholder ikke en bestemmelse om retten til at blive glemt, som vi nu kender fra Persondataforordningens art. 17. EU-Domstolen konkluderer i dommen, at de registreredes ret til sletning kunne udledes af en fortolkning af persondatadirektivets art. 12, litra b, og art. 14, stk. 1, litra a.

EU-Domstolen anvender her en udvidende fortolkning af art. 12, litra b, hvor der ses på de lovlighedsbetingelser, som direktivet som helhed pålægger behandlingen af personoplysninger.⁷⁷ Selv om bestemmelsen udtrykkeligt angiver, at oplysningerne kun kan kræves "berigtiget, slettet eller blokeret", hvis de er "ufuldstændige eller urigtige", så skriver EU-Domstolen, at dette blot er et ikke-udtømmende eksempel på ulovlig behandling,⁷⁸ og at "at en sådan uforenelighed ikke kun kan følge af, at personoplysningerne er ukorrekte, men navnlig også af den omstændighed, at de er utilstrækkelige, irrelevante eller omfatter mere end, hvad der er nødvendigt i forhold til formålet med behandlingen, at de ikke er ajourført, eller at de opbevares i et længere tidsrum end det, der er nødvendigt, medmindre de opbevares i historisk, statistisk eller videnskabeligt øjemed".⁷⁹

EU-Domstolen anerkender i dommen, at retten til at blive slettet i dette tilfælde kan stride imod både søgemaskineudbyderens økonomiske interesse, men også for offentlighedens interesse i at få adgang til den nævnte oplysning ved en søgning på personens navn. EU-Domstolen inddrager her chartrets art. 7 og 8 og stadfæster, at den berørte person har nogle grundlæggende databeskyttelsesrettigheder, som går forud for disses øvrige interesser.⁸⁰

Dommen er et godt eksempel på, hvordan EU-domstolen inddrager bestemmelsens helhed og formål, således at den rækker ud over selve ordlyden. Den illustrerer også, hvordan chartrets bestemmelser inddrages, således at eventuelle modstridende interesser bliver afvejet ved, at individets grundlæggende rettigheder vejer tungest.

⁷⁷ Borberg, Vibeke. 2016. *Hovedhensyn bag EU-Domstolens afgørelse i Google Spain-sagen*. Jurist- og Økonomforbundets Forlag, s. 8

⁷⁸ Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González. Sag C-131/12. EU:C:2014:317, præmis 72

⁷⁹ Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González. Sag C-131/12. EU:C:2014:317, præmis 92

⁸⁰ Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González. Sag C-131/12. EU:C:2014:317, præmis 97

2.14.3.3. Formålet med Persondataforordningens art. 25

Vedrørende formålet med den konkrete bestemmelse i forordningens art. 25, fremgår det allerede af selve bestemmelsen, at gennemførelsen af databeskyttelse gennem design, skal sikre opfyldelse af kravene i forordningen og beskytte de registreredes rettigheder, jf. art. 25, stk. 1 in fine.

Det fremgår derudover af præambelbetragtning 78, at bestemmelsen skal sikre beskyttelse af ”fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger”.

Præambelbetragtningen anfører, at foranstaltningerne skal sikre, at hele forordningens krav opfyldes, og at den dataansvarlige skal kunne påvise overholdelse af forordningen, bl.a. ved at gennemføre foranstaltninger, som især lever op til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Det fremgår altså både af selve bestemmelsen, og præambelbetragtning 78, at formålet er meget bredt, da bestemmelsen generelt skal bidrage til, at kravene i forordningen opfyldes og at de registreredes rettigheder skal beskyttes.

2.14.3.4. Formålsfortolkning af databeskyttelse gennem design

Både formålet med reglerne og den konkrete bestemmelse er fastlagt, og ved at tage hensyn til tidligere praksis fra EU-Domstolen, vil det være muligt at give et bud på, hvordan EU-Domstolen vil anvende en formålsfortolkning af databeskyttelse gennem design. I og med at formålet er så bredt, samtidig med at bestemmelsens ordlyd også er bredt formuleret, giver det EU-Domstolen store fortolkningsmuligheder.

Det er ikke nogen tvivl om, at EU-Domstolen vil inddrage formålet med selve bestemmelsen, når den skal fortolkes, og vil se på, hvad der mest effektivt kan realisere bestemmelsens overordnede målsætning. I dette tilfælde er det både at sikre, at alle krav i forordningen opfyldes, og de registreredes rettigheder beskyttes. Da dette er meget bredt, er det dog tvivlsomt, hvor langt EU-Domstolen vil gå med en udvidende formålsfortolkning.

Ved en sådan formålsfortolkning vil bestemmelsen få et materielt indhold, der i hvert fald går ud over kun at omfatte sikkerhedsforanstaltninger. Databeskyttelse gennem design skal sikre, at alle

databeskyttelsesprincipper og garantier i forordningen overholdes, og dette sikres ved, at den dataansvarlige designer passende tekniske og organisatoriske foranstaltninger med dette henblik.

Derudover er det sandsynligt, at EU-Domstolen ikke kun vil se på selve ordlyden og det udtrykkeligt nævnte formål med selve bestemmelsen, men herudover vil inddrage formålet med selve princippet om databeskyttelse gennem design, som er gennemgået tidligere i analysen. Det betyder, at begrebet kan sætte nogle yderligere krav til den dataansvarlige, som ikke fremgår af forordningsteksten, men som er en selvstændig del af princippet om databeskyttelse gennem design, som de registrerede har krav på. Ifølge Ann Cavoukian indeholder princippet som sagt mere end kun at opfylde selve lovgivningen, i og med at der skal tænkes proaktivt for at opfylde normen, som er beskyttelse af privatliv. Princippet er ifølge hende et middel til at undgå at problemer opstår - ikke et middel til at løse dem. Dette kan være nødvendigt, således at "de registreredes rettigheder beskyttes", hvilket er bestemmelsens formål. Der er dog her en udfordring, idet princippet nu er en del af lovgivningen og ikke som oprindeligt et juridisk ikke-bindende princip. Kan en lovgiver kræve, at der skal gøres mere end bare at opfylde lovteksten og at der skal tænkes ud af boksen?

Det største problem ved en sådan udvidende formålsfortolkning af bestemmelsen vil være, at de dataansvarlige på nuværende tidspunkt i så fald ikke kan vide, hvad der præcis ligger i princippet om databeskyttelse gennem design. Det kan være både dyrt og tidskrævende for de dataansvarlige, for det første bare at forstå, hvad princippet indebærer, og herefter at indføre de nødvendige foranstaltninger. Hvis princippet skaber sådanne yderligere selvstændige designkrav, som ikke har nogen tilknytning til forordningens øvrige regler, vil det derfor skabe en stor retsusikkerhed for de dataansvarlige, som vil have svært ved at vide, hvor meget der skal til, for at princippet er overholdt.

Som det blev slået fast i bl.a. Google-Spain dommen, så tager EU-Domstolen de grundlæggende databeskyttelsesrettigheder alvorligt, og er ikke bange for at tilsidesætte kommercielle interesser, for at beskytte de berørte personer. De grundlæggende databeskyttelsesregler i chartrets art. 8, gik i dommen forud for søgemaskinernes økonomiske interesse, og retten til at blive glemt er selvsagt en stor økonomisk byrde at lægge på alle online søgemaskiner. På samme måde kan retten til databeskyttelse gennem design gå forud for private virksomheders økonomiske interesser i, ikke at skulle tænke udover, hvad selve lovteksten kræver, for at overholde princippet om databeskyttelse gennem design.

2.14.4. EU-rettens udviklingstrin

Endelig og for det fjerde skal reglerne fortolkes i lyset af EU-rettens nuværende udviklingstrin, og EU-Domstolen begrundet ofte sine afgørelser med, at noget ikke kan antages på ”fællesskabsrettens nuværende udviklingstrin”.⁸¹ Udtrykket "nuværende udviklingstrin er anvendt over 900 gange.⁸² På denne måde giver EU-Domstolen sig selv en dynamisk og kreativ fortolkningsstil, i og med at den kan anvendes både til at indskrænke eller udvide EU's handling, når omstændighederne taler for det ene eller det andet.

Det må siges at virke noget modsigende, at EU-Domstolen på den ene side søger at fortolke en bestemmelse i overensstemmelse med, hvad der mest effektivt kan realisere bestemmelsens målsætning, men så på den anden side kan begrænse denne målsætning, ved at henvise til EU-rettens nuværende udviklingstrin.⁸³

Det giver også domstolen mulighed for at afsige en dom, og så præcisere i dommen, at den har taget hensyn til EU-rettens nuværende udviklingstrin. På den måde kan dommerne tilkendegive, at de forventer at dette trin vil udvikle sig i fremtiden, og at en eventuel bestemmelse i fremtiden vil få den retsvirkning, som mest effektivt realiserer dens målsætning - tiden er bare ikke moden endnu.

Netop dette fortolkningstrin, kan tænkes at finde relevans på persondatarettens område, når vi har at gøre med bestemmelser, som ellers kan fortolkes vidtgående efter en formålsfortolkning. Dog er dette muligvis alligevel ikke et nødvendigt fortolkningsværktøj, da EU-Domstolen også arbejder med et andet begreb på persondatarettens område, som ligeledes kan begrænse en ellers vidtgående fortolkning – internettets udviklingstrin.

2.14.4.1. Internettets udviklingstrin

På persondatarettens område har EU-Domstolen anvendt udtrykket internettets udviklingstrin. Dette blev anvendt i Lindqvist-sagen,⁸⁴ hvor EU-Domstolen i en præjudiciel afgørelse tog stilling til, om der

⁸¹ Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, s. 141

⁸² Messerschmidt, Morten. 2013. *Intet over og intet ved siden af - EU-Domstolen og dens aktivisme*. People's Press, s. 65

⁸³ Messerschmidt, Morten. 2013. *Intet over og intet ved siden af - EU-Domstolen og dens aktivisme*. People's Press, s. 117-118

⁸⁴ Angående en anmodning, som Göta hovrätt (Sverige) i medfør af artikel 234 EF har indgivet til Domstolen for i den for nævnte ret verserende straffesag mod Bodil Lindqvist. Sag C-101/01. EU:C:2003:596

er tale om en overførsel af personoplysninger til et tredjeland, når en EU-borger, ved hjælp af en computer, lægger personoplysninger ud på en hjemmeside, som er lagret på en server i det pågældende EU-land, men hvorved personoplysningerne bliver tilgængelige for personer i et tredjeland.

Spørgsmålet var altså, om ovenstående var omfattet af persondatadirektivets art. 25. I begrundelsen henviser EU-Domstolen til internettets udviklingstrin på tidspunktet for udarbejdelsen af direktivet, og at der på dette tidspunkt ikke kan formodes, at lovgiver har tilsigtet, at begrebet ”videregivelse til et tredjeland af personoplysninger” fremtidigt skulle omfatte den omstændighed, som den i sagen omhandlede, hvor oplysninger lægges ud på en internetside, selv om disse således er blevet gjort tilgængelige for personer i tredjelande, der har de tekniske muligheder for at få adgang hertil.⁸⁵ Domstolen henviser derudover til de praktiske vanskeligheder den modsatte fortolkning ellers ville føre til, i og med at internettet i så fald reelt ikke kunne anvendes.⁸⁶

Med andre ord begrænsede EU-Domstolen anvendelsesområdet for bestemmelsen ved at lave en rimelighedsvurdering, hvor der både blev set på, hvad lovgiver måtte formodes at have tilsigtet med begrebet, og de praktiske vanskeligheder, som en vidtgående fortolkning ellers ville indebære.

2.14.5. Fortolkningskonklusion

Ovenstående analyse har gennemgået alle EU-Domstolens fortolkningstrin i forbindelse med art. 25, stk. 1 i forordningen. Ved at se på ordlyden af bestemmelsens overskrift og hovedtræk, samt ved at inddrage sammenhængen og helheden, er det konkluderet, at selv om der i forordningen anvendes et andet udtryk end Privacy by Design, så er der ikke nogen tvivl om, at det skal forstås i sammenhæng med Ann Cavoukians oprindelige princip. Ved at anvende udtrykket databeskyttelse gennem design er der ikke risiko for, at begrebet forveksles med eventuelle mindre omfattende, og juridisk ikke-bindende versioner af Privacy by Design, som f.eks. vil findes i Nordamerika.

⁸⁵ Angående en anmodning, som Göta hovrätt (Sverige) i medfør af artikel 234 EF har indgivet til Domstolen for i den for nævnte ret verserende straffesag mod Bodil Lindqvist. Sag C-101/01. EU:C:2003:596, præmis 68

⁸⁶ Angående en anmodning, som Göta hovrätt (Sverige) i medfør af artikel 234 EF har indgivet til Domstolen for i den for nævnte ret verserende straffesag mod Bodil Lindqvist. Sag C-101/01. EU:C:2003:596, præmis 69

Ved at analysere og fortolke de enkelte dele af bestemmelsen, er det konkluderet, at bestemmelsens indhold går ud over kun at omhandle sikkerhedsforanstaltninger. Bestemmelsen er meget bredt formuleret og en ordlydsfortolkning er derfor ikke nok, til at få afklaret dens indhold.

Ved en formålsfortolkning er det konkluderet, at databeskyttelse gennem design skal sikre, at alle databeskyttelsesprincipper og garantier i forordningen overholdes, og dette sikres ved at den dataansvarlige designer de passende tekniske og organisatoriske foranstaltninger med dette henblik.

Det er dog tvivlsomt hvor langt EU-Domstolen vil gå, når det kommer til at inddrage Ann Cavoukians oprindelige princip. At domstolen vil lade sig inspirere af Ann Cavoukians syv grundlæggende principper for Privacy by Design, er der ikke tvivl om, og dette vil også være i overensstemmelse med både ENISA's og Artikel 29-gruppens udtalelser. Derimod vil princippet næppe blive fortolket i overensstemmelse med påstanden om, at virksomheder skal tvinges til at være proaktive, og anvende princippet til at undgå, at problemer overhoved opstår. Derudover er det meget usandsynligt, at et princip, der allerede er inkorporeret i lovgivningen, kan kræve, at virksomheder skal "raise the bar for legal norms", da princippet nu netop er en juridisk norm.

Det forventes, at EU-Domstolen vil lave en formålsfortolkning hvor både selve bestemmelsens udtrykkelige formål, samt baggrunden for det oprindelige princip inddrages. Dog vil denne formålsfortolkning være præget af rimelighedshensyn, således at der tages hensyn til, at det oprindelige princip netop ikke var udarbejdet som en lovbestemmelse, men som noget juridisk ikke-bindende, der supplerede lovregler.

Derudover vil ovenstående formålsfortolkning kunne begrænses af EU-rettens- og internettets udviklingstrin, således at de fulde virkninger af bestemmelsen ikke kommer til sin ret fra den første dag. Dette vil dermed kunne afhjælpe den juridiske usikkerhed, der altid vil være til stede, når der inkorporeres et bredt princip i lovgivningen, som de dataansvarlige må tage stilling til og efterleve. På den anden side er formålet med forordningen at beskytte individers grundlæggende rettigheder, og det kan dermed ikke forventes, at EU-Domstolen vil stå tilbage med at håndhæve princippet, selv om der vil være modstående kommercielle interesser på spil, hvilket Google Spain dommen er et eksempel på. Dette må i hvert fald antages at være tilfældet i fremtiden, når princippet indhold er blevet nærmere defineret gennem EU-Domstolens praksis.

2.15. Konklusion på juridisk analyse

Ved at se på Justitsministeriets udlægning af begrebet databeskyttelse gennem design, og sammenligne denne med bl.a. udlægningen fra Rådet for Digital Sikkerhed er det konstateret, at der er uenighed om fortolkningen af forordningens art. 25, stk. 1. Denne uenighed er vigtig at få afklaret for de dataansvarlige, da overtrædelse af bestemmelsen kan resultere i betydelige bøder.

Justitsministeriet skriver i betænkningen, at princippet allerede indirekte fremgår af direktivets art. 17, sammenholdt med præambelbetragtning nr. 46. Justitsministeriet konkluderer, at art. 25 ikke etablerer nye krav til den dataansvarlige, da de allerede følger af gældende databeskyttelsesret. Formanden for Rådet for Digital Sikkerhed, Henning Mortensen, anerkender, at princippet ikke er ukendt efter gældende ret, men at det kun har fundet anvendelse i forbindelse med sikkerhedsforanstaltninger. Hvis databeskyttelse gennem design allerede er dækket fuldt ud efter gældende ret, så begrænses begrebet derfor til kun at omhandle de sikkerhedsforanstaltninger, som falder ind under anvendelsesområdet for direktivets art. 17.

For at få afklaret om art. 25 omfatter mere end sikkerhedsforanstaltninger, er det for det første konstateret, at dette begreb ikke har en klar definition, men at der ved sikkerhedsforanstaltninger er fokus på beskyttelse mod f.eks. tilintetgørelse, tab, forringelse, udbredelse eller uautoriseret adgang.

Derefter er der gået i dybden med selve princippet om Privacy by Design. Ved at se på hvordan bl.a. Ann Cavoukian, ENISA og Artikel 29-gruppen hidtil har fortolket princippet, er det konkluderet, at princippet går videre end kun at omhandle sikkerhedsforanstaltninger. Ifølge Ann Cavoukian, som introducerede begrebet, er det et meget bredt princip, der omfatter alt fra dataminimering, fuld funktionalitet, transparens og til at brugeren er i centrum. Det er derfor f.eks. muligt at have en høj sikkerhed og opfylde krav til sikkerhedsforanstaltninger, men ikke opfylde princippet om Privacy by Design. Artikel 29-gruppen plæderer ligeledes for et bredt Privacy by Design begreb, som ikke blot skal omhandle sikkerhed, men også minimere behandlingen af personoplysninger.

Det er dog EU-Domstolen, der i sidste ende kommer til at afgøre, hvordan art. 25 skal fortolkes. EU-Domstolen har indtil videre hverken udtalt sig direkte om indholdet af art. 25 eller afsagt en dom, som de facto kræver databeskyttelse gennem design. EU-Domstolen har dog en kendt og systematisk

fortolkningsstil, og med udgangspunkt i afhandlingens analyse af princippet, er denne fortolkningsstil anvendt på forordningens art. 25, stk. 1.

Ved at se på ordlyden af bestemmelsens overskrift og hovedtræk, samt ved at inddrage sammenhængen og helheden, er det konkluderet, at selv om der i forordningen anvendes et andet udtryk end Privacy by Design, så er der ikke nogen tvivl om, at det skal forstås i sammenhæng med Ann Cavoukians oprindelige princip. Ved at lave en formålsfortolkning af bestemmelsen er det konkluderet, at den har et materielt indhold, der i hvert fald går ud over kun at omfatte sikkerhedsforanstaltninger. Dog forventes det, at EU-Domstolens formålsfortolkning vil være præget af rimelighedshensyn, således at der tages hensyn til, at det oprindelige princip netop ikke var udarbejdet som en lovbestemmelse, men som noget juridisk ikke-bindende, der supplerede lovregler. Derudover vil formålsfortolkningen kunne begrænses af EU-rettens- og internettets udviklingstrin, således at de fulde virkninger af bestemmelsen ikke kommer til sin ret fra den første dag. På den anden side er formålet med princippet at beskytte individers grundlæggende rettigheder, og det kan dermed ikke forventes, at EU-Domstolen vil stå tilbage med at håndhæve princippet, selv om der vil være modstående kommercielle interesser på spil, hvilket Google Spain dommen er et eksempel på. Dette må i hvert fald antages at være tilfældet i fremtiden, når princippets indhold er blevet nærmere defineret gennem EU-Domstolens praksis.

Det kan derfor konkluderes, at art. 25 i forordningen medfører en ændring i forhold til gældende ret. Princippet om databeskyttelse gennem design var delvist omfattet af sikkerhedsbestemmelsen i direktivets art. 17 sammenholdt med præambelbetragtning 46, men den fulde virkning af princippet var ikke implementeret i lovgivningen. Dette er nu sket med indførelsen af forordningens art. 25, stk. 1.

Således består ændringen i, at begrebet Privacy by Design omfatter mere end blot sikkerhed og da databeskyttelse gennem design skal fortolkes i overensstemmelse med Privacy by Design, medfører ændringen, at de dataansvarlige skal tænke på mere end blot sikkerhed, når de gennemgår og udvikler deres it-systemer. Dette kan f.eks. være i form af dataminimering ved brug af drop-down menuer i stedet for fritekstfelter, for at sikre at der ikke skrives mere information end nødvendigt. Ligeledes kan det være at sikre, at brugeren er i centrum, når der udvikles. Det vil sige have fokus på, hvad der er bedst for brugeren, i stedet for at have udvikleren/udbyderen i fokus og dermed tænke på, hvad der er bedst for denne.

Kapitel 3: Økonomisk analyse

3.1. Indledning

Der skal i det følgende ses på, om princippet om databeskyttelse gennem design har en økonomisk værdi for virksomheder.

Som det fremgik af den juridiske analyse, så har bl.a. Ann Cavoukian skrevet, at princippet indebærer en positiv ting for alle parter - også de dataansvarlige. Det er i teorien også fremført, at overholdelse af princippet vil give de dataansvarlige en konkurrencefordel på markedet.

Hvorvidt overholdelse af princippet er en gevinst eller en byrde for de dataansvarlige, skal derfor undersøges nærmere, ved at inddrage økonomiske teorier og værktøjer. Derudover skal der ses på, hvordan markedet selv håndterer databeskyttelse, hvis det ikke er lovreguleret.

3.2. Databeskyttelse gennem design – en økonomisk byrde eller en konkurrencefordel?

Der har været meget fokus på de negative konsekvenser, som databeskyttelse gennem design kan have for de dataansvarlige. Det er et komplekst princip, som er dyrt at indføre og overtrædelse kan resultere i store bøder og give negativ omtale. Det er også blevet fremført, at virksomhederne ikke er klare til forordningens krav endnu, hvilket bl.a. bekræftes af en undersøgelse fra juni 2017, som er gennemført af Devoteam.⁸⁷ Devoteam spurgte i undersøgelsen 500 danske offentlige og private virksomheder om deres arbejde med Persondataforordningen, og undersøgelsen viste bl.a. at mere end to tredjedele af de adspurgte stadigvæk ikke havde en plan for dette arbejde.

Men der er også dem, der ser anderledes positivt på princippet. Data er et af de vigtigste aktiver, som virksomheder er i besiddelse af, og privatliv og sikkerhed er samtidigt vigtigt for forbrugerne.

Databeskyttelse skal derfor opfattes som mere end blot et juridisk krav, men derimod som et fundament

⁸⁷ Pressemeddelelse fra Devoteam. 30. maj 2017. *Devoteam lancerer ny markedsundersøgelse for EU persondataforordningen*. Direkte link: <https://dk.devoteam.com/2017/05/30/pressemeddelelse-devoteam-lancerer-ny-markedsundersogelse-eu-persondataforordningen/>

for samarbejdet mellem virksomheden og forbrugerne. Derfor kan kravet om databeskyttelse gennem design også ses som en mulighed for virksomheder til at indføre en ny tilgang til databeskyttelse, således at de måske endda går længere, end kun at opfylde forordningen. På den måde hævdes det, at virksomheden kan vinde forbrugernes tillid, og differentiere sig på markedet.⁸⁸

En konkurrencefordel er kun en konkurrencefordel, såfremt virksomheden har noget, som konkurrenterne ikke er i besiddelse af. Ifølge økonomen Michael Porter kan konkurrencefordele principielt opstå på to måder. Virksomheden kan enten indkøbe, producere og distribuere til de laveste omkostninger i branchen, eller den kan tilbyde et produkt, der er unikt. Porter arbejder med to dimensioner, hvor den ene er, hvilken konkurrencefordel virksomheden besidder, og den anden er, hvilket marked virksomheden ønsker at bearbejde. Ud fra det har Porter udarbejdet fire generiske konkurrencestrategier.⁸⁹

Figur 3.1.⁹⁰

Generiske strategier			
		Konkurrencefordel	
		Lave omkostninger	Unikt produkt
Bearbejdet marked	Stor andel af totalmarked	Omkostningsleder Lav pris	Differentiering Høj pris
	Lille andel af totalmarked	Omkostningsfokus Lav pris	Fokuseret differentiering Høj pris

Virksomheder kan derfor have incitamenter til af egen drift at indføre princippet om databeskyttelse gennem design, hvis den vurderer, at dette giver et unikt produkt og derved en konkurrencefordel på markedet. Selv om selve implementeringen af princippet kan være omkostningsfuldt, så vil virksomheden ved at tilbyde et unikt produkt også kunne kræve en højere pris.

⁸⁸ Artikel af Isaac, Kevin. 10. april 2017. *How to turn GDPR into a competitive advantage with 'privacy by design'*. Direkte link: <http://www.cityam.com/262618/turn-gdpr-into-competitive-advantage-privacy-design->

⁸⁹ Andersen, Finn Rolighed; Jensen, Bjarne Warming; Jepsen, Kurt; Olsen, Mette Risgaard & Schmalz, Peter. 2013. *International markedsføring*. Trojka. 4. udgave, s. 110

⁹⁰ Andersen, Finn Rolighed; Jensen, Bjarne Warming; Jepsen, Kurt; Olsen, Mette Risgaard & Schmalz, Peter. 2013. *International markedsføring*. Trojka. 4. udgave, figur 5.13

En konkurrencefordel er dog kun en konkurrencefordel, såfremt forbrugerne er opmærksomme på fordelene ved databeskyttelse gennem design, og indser at de har et behov for, at dette princip er opfyldt. Det betyder, at virksomheden udover omkostningerne ved at implementere foranstaltningerne, må være i stand til at kommunikere værdien af dette til målgruppen.⁹¹ Det betyder, at der også skal bruges omkostninger på markedsføring, således at forbrugerne bliver gjort opmærksomme på konkurrencefordelen og dermed er villige til at betale for den.

3.3. Produktdifferentiering og Hotelling model

En anden måde at se på produktdifferentiering fra et rent økonomisk synspunkt er ved brug af the Hotelling model.

Vi antager, at der er et marked med fuldkommen konkurrence. Virksomhederne har ens MC, og P er dermed lig MC. En virksomhed på dette marked ønsker nu at indføre PbD. Dette vil alt andet lige medføre øgede omkostninger og dermed en højere MC end de andre virksomheder. Udgangspunktet indenfor den mikroøkonomiske teori er dermed, at de andre aktører på markedet vil tage hele markedet. Dette er dog kun såfremt forbrugerne ser det nye "produkt" som det samme. Hvis omvendt forbrugerne ser, at der er tale om et andet produkt, idet det nye er mere privatlivsfremmende, er kravet om et homogent produkt ikke længere opfyldt og dermed kan virksomheden, der ønsker at indføre PbD sagtens overleve, idet der i så fald er tale om et selvstændigt produkt, som ikke længere kan sammenlignes med de andre aktørers.

Inden for produktdifferentiering findes der to former – horisontal- og vertikal produktdifferentiering. Vertikal omhandler de situationer hvor alle forbrugere er enige om, at produkt A er bedre end produkt B. Horisontal, som vil blive anvendt her, er den situation, hvor ikke alle er enige. Nogle vil altså foretrække produkt A fremfor B og andre B fremfor A.

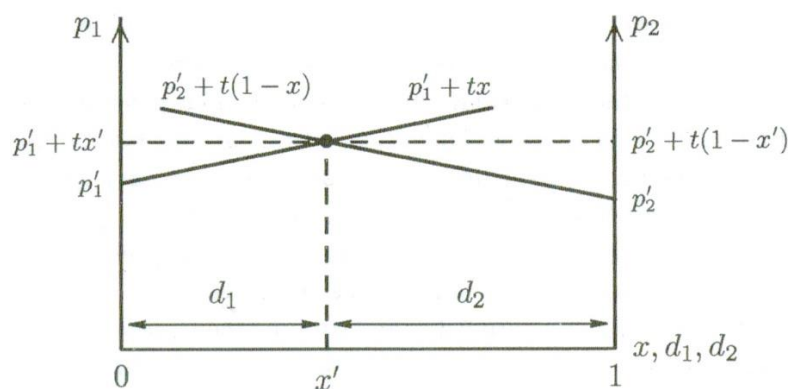
Det kommer f.eks. til udtryk ved, at der kan vælges mellem to apps til brug som lommelygte på telefonen. Den ene er "gratis" og den anden koster penge. Til den der er "gratis" betaler vi med deling

⁹¹ Andersen, Finn Rolighed; Jensen, Bjarne Warming; Jepsen, Kurt; Olsen, Mette Risgaard & Schmalz, Peter. 2013. *International markedsføring*. Trojka. 4. udgave, s. 112

af persondata og får dermed appen uden betaling af penge. Til den der koster penge, skal vi ikke dele vores persondata. I denne situation kan der argumenteres for, at der er tale om to forskellige produkter. Den ene deler overhoved ikke data og den anden gør. Selvom alle er bevidste om dette, vil nogen alligevel foretrække den, der deler data fremfor den anden og nogle andre omvendt.

Dette kan forklares ved at inddrage the Hotelling model. Det er en model, der bruges til at beskrive, hvordan det kan være, at to virksomheder der sælger et ens produkt, alligevel kan tage en differentieret pris for varen, idet der skal tillægges transportomkostninger til prisen, for at afgøre den reelle omkostning for forbrugeren, og dermed er den rene pris for varen ikke den udslagsgivende. Derudover kan modellen også bruges i situationer, hvor der ikke er tale om præcis det samme produkt. Transportomkostningen bliver her forbrugers aversion mod ikke at få præcis det ønskede produkt.

Figur 3.2.⁹²



I ovenstående model viser y-akserne priserne på to produkter. X-aksen beskriver ens omkostning for at transporterer sig. Det vil sige, at en person der befinder sig på punkt x' , skal transportere sig fra x' til 0 og dermed rykke distancen x til transportomkostningen t per enhed distance. Dermed skal en person, der befinder sig på punkt x' betale prisen $p_1' + tx'$ for at købe fra virksomhed 1. Ligeledes vil personen der befinder sig på punkt x' , skulle transportere sig fra x til 1 for at købe fra virksomhed 2 og dermed rykke sig distancen $1 - x$. Prisen for at købe hos virksomhed 2, hvis man befinder sig på punkt x' altså $p_2' + t(1 - x')$.

⁹² Cabral, Luis M. B. 2000. *Introduction to Industrial Organization*. The MIT Press, s. 212, figur 12.1

Ud fra modellen ses det, at hvis man befinder sig på punkt x' , er man indifferent mellem at købe hos virksomhed 1 og 2, mens alle der befinder sig til venstre for dette punkt, vil handle hos virksomhed 1 og til højre for dette punkt vil handle hos virksomhed 2.

Selvom de to priser ikke er ens, vil begge virksomheder altså kunne overleve ifølge Hotelling model, også selvom udgangspunktet inden for økonomien er, at virksomheden med den laveste pris vil tage hele markedet. I denne situation er det virksomhed 2 med prisen $p'2$, som er lavere end $p'1$. Men tages transportomkostningen med, er der et marked for begge virksomheder.

Modellen kan udover at beskrive, hvordan to virksomheder godt kan tage en differentieret pris også beskrive, hvordan to differentierede produkter kan tage en del af markedet hver.

Transportomkostningen kan konverteres til at beskrives forbrugerens aversion mod ikke at få det ønskede produkt.

Modellen kan altså bruges til at beskrive situationen med de to lygteapps. Lad os nu antage for nemheds skyld, at de begge koster penge, dog er appen fra virksomheden der sælger brugerens data lidt billigere. Transportomkostningen bliver her brugerens aversion mod dette salg. Lad os antage at virksomhed 2 sælger ens data, hvormed prisen $p'2$ er lidt billigere end $p'1$. Selvom man har en aversion mod salget af ens data, vil dem, der befinder sig til højre for x' , alligevel købe appen der sælger ens data, da deres aversion ikke er stor nok til at kompensere for den højere pris for virksomhed 1 app.

Det kan dermed både ud fra the Hotelling model og Porters generiske konkurrencestrategier argumenteres for, at databeskyttelse gennem design økonomisk set kan udgøre en konkurrencefordel på markedet, selv om dette medfører en højere pris. Virksomheder kan derfor have incitamenter til at indføre det, selv om dette ikke er lovkrævet.

Selv om databeskyttelse gennem design ifølge økonomisk teori kan udgøre en konkurrencefordel, så ændrer dette ikke på, at en stor del af virksomhederne indtil videre ikke har indarbejdet princippet i sine it-systemer. Virksomhederne er som tidligere nævnt på nuværende tidspunkt ikke klar til forordningens nye krav, og det kan på den baggrund konstateres, at værdien – og den eventuelle konkurrencefordel – af princippet ikke genspejles, når der ses på virksomhederne på markedet.

Det er dermed noget, der tyder på, at den økonomiske værdi ved at indsamle og profitere på persondata, er højere for de fleste virksomheder på markedet, end gevinsten er ved at satse på høj databeskyttelse. Den økonomiske værdi af persondata skal derfor undersøges nærmere, inden der skal ses på, om forbrugernes efterspørgslen efter databeskyttelse svarer til denne værdi.

3.4. Den økonomiske værdi af persondata

Det er allerede nævnt et par gange, at persondata har en økonomisk værdi, og at forbrugere i stedet for penge kan betale med at udlevere deres persondata. Den økonomiske værdi er det maksimale, en forbruger er villig til at betale for et produkt i et frit marked. Et produkt kan have en brugsværdi og en bytteværdi, og mønter er blot et kvantitativt mål for produktets bytteværdi, uanset produktets karakter. Men den økonomiske værdi kan også komme til udtryk gennem andet end mønter. I socialistisk økonomi kommer den økonomiske værdi af et produkt til udtryk, gennem den tid forbrugeren vil ofre, for at få hænderne i det statsproducerede produkt.⁹³

Det er dermed ikke ukendt indenfor den økonomiske teori, at værdi kan udgøres i andet end penge. De fleste økonomiske teorier og modeller er mange år gamle, og er derfor udviklet langt inden internettet og de muligheder, som persondata indebærer, var blevet en virkelighed. Det som adskiller persondata fra penge, er, at værdien af persondata er meget forskellig fra person til person, mens en krone altid er en krone værd, uanset hvem der besidder den.

Værdien af data kan dog være meget svær at definere. Både for virksomheder og for forbrugere. En virksomhed kan have fået noget information fra en forbruger, men hvad er denne information egentlig værd? Hvis en virksomhed der sælger fortrydelsespiller mod uønsket graviditet, ønsker at markedsføre produktet, kan det have en stor værdi for virksomheden at vide, hvis en forbruger f.eks. har søgt på graviditetstest på google, da man dermed må antage at personen tror, at hun måske er gravid. Det kan derfor være en stor fordel at markedsføre sit produkt til denne forbruger, da der er en stor mulighed for, at forbrugeren ikke ønsker et barn. Værdien af denne information kan være svær at gøre op i penge, men at den har en værdi, er indiskutabelt. På denne måde kan virksomheder opnå store salgsmuligheder

⁹³ Artikel om definition på økonomisk værdi. *Economic Value*. <https://www.investopedia.com/terms/e/economic-value.asp>

og derved øge deres indtjeningsevne markant, hvis de får hænderne i de relevante personoplysninger. Det kan derfor betale sig for virksomheder at bruge penge på at købe sig til persondata, da værdien af denne data hurtigt kan overstige de kroner, de giver for det.

Dog er der heller ingen tvivl om, at værdien er mindre eller ingen, hvis det nu viser sig, at forbrugeren der søgte på en graviditetstest, ikke gjorde det for sig selv, men for en veninde. Så vil markedsføringen af fortrydelsespiller mod denne forbruger ikke have nogen, eller i hvert fald en væsentlig mindre værdi.

På individplan kan værdien af data altså være svær at værdiansætte, men at den i store mængder har en værdi, er der ingen tvivl om. F.eks. vil det for virksomheden der sælger fortrydelsespiller være værdifuld information at vide, hvem der har søgt på graviditetstest på f.eks. google, da chancen for at få solgt sit produkt til denne gruppe nok er større, end hvis der bare markedsføres bredt.

Når persondata kan have en så stor værdi, burde forbrugerne også kræve sig godt betalt for at udlevere det, samt kræve at det ikke videregives. Når forbrugerne er i besiddelse af noget så værdifuldt, burde efterspørgslen efter databeskyttelse dermed også svare til dette. Efterspørgslen efter databeskyttelse skal derfor undersøges nærmere, for at finde frem til hvad den økonomiske årsag er, til at virksomheder ikke af egen drift har mere fokus på databeskyttelse, f.eks. databeskyttelse gennem design.

3.5. Efterspørgsel på databeskyttelse

Påstanden flere steder er, at vi som mennesker ønsker mest muligt privatliv. Vi ønsker ikke at dele vores data. Men er det nu også sådan, det i virkeligheden er? Eller er det kun ud fra et teoretisk synspunkt?

Det har en omkostning for os at dele vores persondata. Men at begrænse deling af vores persondata kan ligeledes have en omkostning for os. Det kommer f.eks. til udtryk ved den førnævnte lygteapp. Som nævnt er den ene "gratis" og den anden koster penge. Til den der koster penge, skal vi ikke dele vores persondata. Mange vælger den "gratis" app og betaler således i stedet med deres personlige data. Er det så fordi, at de er ligeglade med at skulle dele deres data, ikke kan overskue/forstå det, de accepterer, eller er det fordi, at de bare vurderer, at det har en mindre omkostning for dem, end rent faktisk at skulle betale for appen med penge?

Som nævnt til den økonomiske metode er det inden for den neoklassiske økonomi udgangspunktet, at mennesker er rationelle og der er perfekt information. Ud fra denne økonomiske teori, må det altså antages, at folk godt ved, hvad de foretager sig og på baggrund af deres rationalitet gør det, der er bedst for dem selv. Og der er perfekt information, så folks beslutninger bliver taget på et oplyst grundlag. Dette er den optimale verden, men som nævnt i metodeafsnittet nok heller ikke den realistiske.

Modsat indenfor den neoklassiske økonomi er der inden for den nyinstitutionelle økonomi ikke perfekt information og folk er kun begrænset rationelle. Det vil sige, at vi som mennesker har en begrænset beregningskapacitet, hukommelse og opmærksomhed. Det medfører, at vi ikke kan overskue vores beslutninger og dermed træffer de beslutninger, som vi umiddelbart tror, er de bedste for os. Vi har altså ikke evnen til at maksimere, som egentlig er vores ønske og det vi tror, at vi gør. Vi tilfredsstiller, snarere end vi maksimerer.

Vi vælger måske at acceptere at dele vores data med lygteappen, fordi vi er begrænset rationelle og ikke kan overskue konsekvenserne af vores beslutning og ikke kan regne ud, at omkostningen herved måske er større for os, end at betale et lille beløb for den anden app. Også fordi vi som mennesker har svært ved at forholde os til en ”fiktiv” omkostning modsat en reel omkostning i form af penge – noget fysisk.

Beslutningen om hvilken app man skal downloade, tages måske også ud fra et forkert økonomisk synspunkt. Økonomiske beslutninger skal tages ud fra en betragtning om økonomiske omkostninger og disse er ikke det samme som reelle udgifter. Økonomiske omkostninger indeholder mulige omkostninger som ikke er lig med reelle omkostninger og udelukker omkostninger der er "sunk". Sunk costs er omkostninger, der allerede er afholdte og som dermed ikke skal medregnes i en omkostningsberegning. En omkostning kan derfor være reel at medregne, hvis der tages udgangspunkt i en dag, men derimod sunk, hvis der tages udgangspunkt i en anden dag.⁹⁴

Der tages udgangspunkt i eksemplet med de to lygteapps. Hvis man skal lave en økonomisk beregning den dag, hvor man ønsker at downloade appen, skal man altså se på omkostningen til betaling for den

⁹⁴ Cabral, Luis M. B. 2000. *Introduction to Industrial Organization*. The MIT Press, s. 23

app, der koster penge. Til sammenligning skal man ved "gratis" appen se på de omkostninger, man har ved at dele sine data. Selvom en forbruger måske er rationel og kan overskue og beregne sin reelle omkostning ved deling af sine data og måske vurdere dette til at være lavere end udgiften til indkøb af den anden app, er det interessante, om forbrugeren er klar over, at denne udgift dagen efter ville være sunk og derfor slet ikke skal med i en økonomisk beregning, hvis denne foretages dagen efter. Det vil sige, at den økonomiske omkostning dagen efter ville være 0, da der ikke er nogen AC ved brug af appen, der koster penge. Modsat ved "gratis"-app'en vil der være en konstant AC, da ens data vil blive solgt konstant og brugt til f.eks. marketing tilpasset lige præcis dig og som dermed vil have en løbende omkostning for dig.

Der kan dermed argumenteres for, at på grund af menneskers begrænsede rationalitet, som medfører, at vi ikke kan overskue den sande omkostning ved at dele vores persondata, og som også forøger risikoen for, at der tages forkerte beslutninger set fra et økonomisk synspunkt, er efterspørgslen på databeskyttelse ikke så stor, som den ellers ville være, hvis mennesker var fuldkommen rationelle.

Ligesom deling af persondata har en omkostning for os, vil det medføre en omkostning for virksomheder at begrænse indsamling af persondata, da dataene som nævnt har en stor økonomisk værdi for virksomhederne. Derudover kan det være omkostningsfuldt at indføre de relevante databeskyttelsesteknologier.

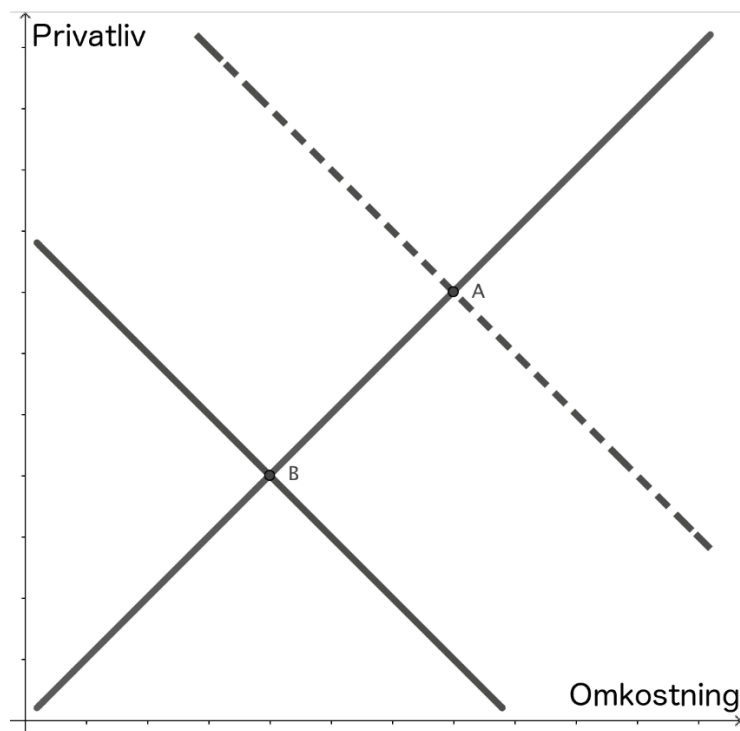
Det kan dermed slås fast, at persondata har stor værdi for virksomhederne, selv om det ikke nemt kan sættes et konkret tal på, hvad denne værdi er. Derudover er der meget der tyder på, at forbrugerne på grund af deres begrænsede rationalitet ikke kender den sande omkostning af, at deres persondata bliver indsamlet. Dette kan medføre, at efterspørgslen på databeskyttelse ikke er så stor, som den ville være, hvis forbrugerne var fuldt rationelle, hvilket resulterer i, at virksomhederne ikke udbyder et særligt højt databeskyttelsesniveau. For at undersøge dette nærmere, skal der ses nærmere på, hvordan markedet finder et databeskyttelsesniveau, hvis dette ikke er lovreguleret.

3.6. Hvordan markedet finder et databeskyttelsesniveau

Inden for den mikroøkonomiske teori arbejdes der med udbud og efterspørgselskurven. Denne kan bruges til at finde det optimale punkt i et marked med fuldkommen konkurrence, idet skæringen

mellem de to grafer definerer markedsligevægten. Denne figur kan ændres lidt og bruges til at beskrive sammenhængen mellem ønsket privatliv i forhold til prisen herfor og virksomhedernes omkostning ved begrænsning af indsamling af data. Grafen for ønsket privatliv falder med omkostningen herfor og udgiften for virksomhederne stiger med den ønskede mængde privatliv.

Figur 3.3. (Egen tilvirkning)



Ligevægtpunktet på markedet er der, hvor de to grafer skærer hinanden. Det er umiddelbart der, hvor der er ligevægt mellem ønsket databeskyttelse og omkostningen herfor. Ud fra den mikroøkonomiske teori er det der, hvor "markedet" vil ende. Altså markedet vil selv finde denne ligevægt, fordi der her er en overensstemmelse mellem ønsket privatliv i forhold til omkostningen herfor.

Udbud og efterspørgselskurven har sin oprindelse i mikroøkonomien, som befinder sig inden for den neoklassiske økonomi. Hvis forbrugerne er rationelle, og der er fuldkommen information, så vil markedet altid finde den optimale løsning, og der ville ikke opstå markedsfejl.

Som det fremgår af ovennævnte kan der dog argumenteres for, at når det kommer til markedet for databeskyttelse, så er forbrugerne netop ikke rationelle, og deres efterspørgsel efter databeskyttelse er

derfor lavere, end den ville være, hvis de var fuldkommen rationelle. Dette kommer som nævnt til udtryk ved, at mange i det tidligere nævnte eksempel med lygteappen, alligevel vælger "gratis"-appen, selv om denne i virkeligheden er dyrere. Dermed ender vi ikke i skæringspunktet A, men skæringspunktet B, da efterspørgselskurven ikke er som den burde på grund af folks irrationalitet.

3.7. Adam Smith's model for sikkerhed på arbejdsmarkedet

En passende og lidt anderledes måde at tegne markedet for databeskyttelse på, er ved at anvende Adam Smith's model for sikkerhed på arbejdsmarkedet⁹⁵, da dette på mange måder kan sammenlignes med markedet for datasikkerhed. Smith observerede, at arbejdere krævede kompensation i form af højere løn for arbejde, som efter deres opfattelse var mere risikofyldt.⁹⁶

Modellen viser hvordan forskellige kræfter påvirker niveauet for sikkerhed. Niveauet for sikkerhed fremgår efter den vandrette linje, mens omkostningen for sikkerhed fremgår efter den lodrette linje.

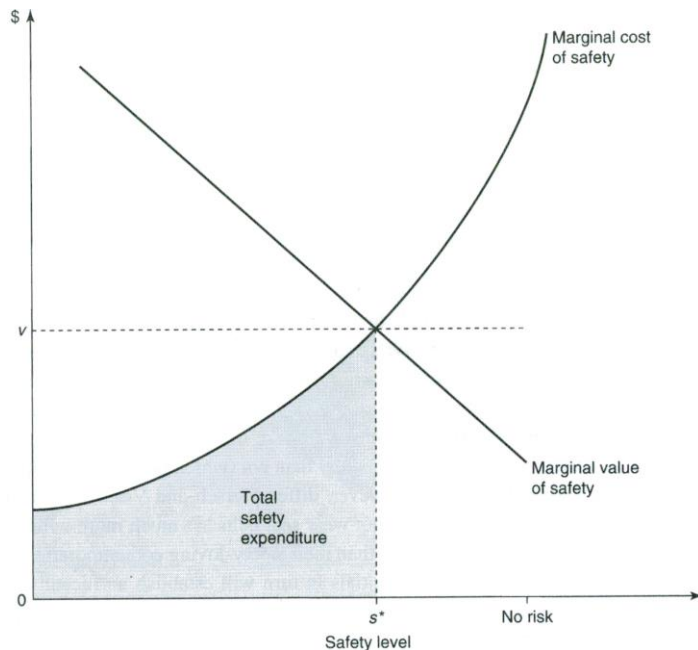
Den marginale værdi af sikkerhed er en nedadgående graf, da de indledende trin har størst værdi for forbrugerne, mens værdien af yderlige sikkerhed ikke har lige så stor værdi.

Virksomhederne kan tilbyde mere sikkerhed, men dette medfører også større marginale omkostninger. De første sikkerhedstrin kan måske klares ved at indføre mindre modifikationer, men hvis sikkerheden skal forbedres markant, så skal der større investeringer til. Dette medfører, at grafen for den marginale omkostning ved ekstra sikkerhed ikke er flad, men stigende.

⁹⁵ Smith, Adam. *The Wealth of Nations*. (New York: Modern Library, 1937)

⁹⁶ Viscusi, W. Kip; Harrington, Joseph E. and Vernon, John M. 2005. *Economics of regulation and antitrust*. The MIT Press. 4. udgave, s. 831

Figur 3.4.⁹⁷



Det optimale sikkerhedsniveau fra et markedssynspunkt er så der, hvor de to grafer møder hinanden, dvs. skæringspunktet hvor grafen for den marginale værdi af ekstra sikkerhed møder grafen for den marginale omkostning ved ekstra sikkerhed. Det valgte sikkerhedsniveau, bliver dog ikke helt uden risiko, fordi det ville være for dyrt. Det bliver derfor et trade-off mellem værdien af nedsat risiko og værdien af andre værdsatte egenskaber.⁹⁸

Modellen er som sagt udarbejdet i forbindelse med sikkerhed på arbejdsmarkedet. En forudsætning for at markedet finder det optimale sikkerhedsniveau på arbejdspladsen, er, at arbejderne er bevidste om, hvilke risici de møder på arbejdspladsen. Hvis dette ikke er tilfældet, vil arbejderen ikke kræve kompensation for det farlige arbejde. På arbejdspladsen kan det være nemt at regne risikoen ud, når det drejer sig om åbenlyse farer på arbejdspladsen, f.eks. hvis arbejdet udføres højt oppe, og der er risiko for at falde ned. Hvis der derimod er tale om helbredsmæssige farer, der kan vise sig langt ude i fremtiden, er det derimod sværere for arbejderne at indregne denne risiko. Det bliver dermed

⁹⁷ Viscusi, W. Kip; Harrington, Joseph E. and Vernon, John M. 2005. *Economics of regulation and antitrust*. The MIT Press. 4. udgave, s. 832, figure 23.2

⁹⁸ Viscusi, W. Kip; Harrington, Joseph E. and Vernon, John M. 2005. *Economics of regulation and antitrust*. The MIT Press. 4. udgave, s. 833

afgørende, om arbejderen for det første besidder den nødvendige information om arbejdspladsen, og for det andet, om arbejderen er rationel nok til at indregne denne risiko i sin beslutningstagen. Hvis dette ikke er tilfældet, er der ineffektivitet på markedet - altså en markedsfejl.

Der kan argumenteres for, at de er de samme markeds kræfter på spil, når vi ser på markedet for databeskyttelse, som i ovenstående model for sikkerhed på arbejdspladsen. Markedet vil sætte et databeskyttelsesniveau i skæringspunktet, hvor grafen for den marginale værdi af ekstra datasikkerhed møder grafen for den marginale omkostning ved ekstra datasikkerhed. I modsætning til modellen for sikkerhed på arbejdspladsen, så er der ikke tale fysiske og helbredsmæssige risici på databeskyttelsesområdet. Men det kan dog argumenteres for, at forbrugerne på samme måde som ved helbredsfarer på arbejdspladsen, ikke er bevidste om risikoen ved manglende databeskyttelse og om værdien af ens persondata, og at der derfor også kan opstå markedsfejl på databeskyttelsesområdet. Disse markedsfejl skal derfor analyseres nærmere.

3.8. Markedsfejl

Hvis markedet for databeskyttelse var efficient set fra lovgivers side, ville der ikke være nødvendigt at regulere området. Så ville markedet selv finde det optimale databeskyttelsesniveau. Men der er noget, der taler for, at der er nogle væsentlige fejl på markedet, som begrænser det effektive marked, og som medfører, at markedet ikke opnår det optimale databeskyttelsesniveau.

Det skal derfor i det følgende analyseres, om markedet for databeskyttelse er underlagt markedsfejl. Den økonomiske teori om markedsfejl siger, at hvis markedet i sig selv ikke frembringer en efficient ligevægt, så kan dette skyldes en markedsfejl – som regulator derfor kan komme ind og afhjælpe i form af regulering.

Markedsfejl opstår generelt, når markedet ikke formår at opnå økonomisk efficiens, dvs. at den sociale velfærd (målt som summen af forbrugervelfærd og industriens profit) ikke er maximeret.⁹⁹ Selv om

⁹⁹ Ølykke, Grith Skovgaard & Møllgaard, Peter. 2013. *What is a Service of General Economic Interest?* Tidsskriftsartikel, s. 219

nærværende afhandling har virksomhederne i fokus, må den samlede sociale velfærd inddrages, for at forstå, hvorfor lovgiver vælger at regulere markedet.

I teorien er der anerkendt flere forskellige markedsfejl. Som eksempel kan nævnes markedsmagt, som vil opstå, når der ikke er fuldkommen konkurrence på markedet. I denne situation vil producenten sætte udbuddet ned, således at prisen bliver højere, hvilket resulterer i, at velfærden rykker fra forbrugerne over til producenten. Derudover vil der opstå et dødvægtstab som følge af, at flere forbrugere nu ikke længere vil købe produktet, selv om de værdsætter det højere end markedsprisen under fuldkommen konkurrence.¹⁰⁰ Andre anerkendte markedsfejl er eksternaliteter, offentlige goder og informationsfejl (asymmetrisk information). Her skal den sidstnævnte analyseres nærmere i forbindelse med markedet for databeskyttelse.

3.8.1. Adfærdsmæssige antagelser

Informationsfejl og asymmetrisk information på markedet har nær sammenhæng med de adfærdsmæssige antagelser, som blev introduceret i kapitel 1. Disse skal derfor uddybes her, inden de potentielle markedsfejl analyseres nærmere.

Vi befinder os som nævnt indenfor den nyinstitutionelle økonomi, hvor aktørerne er begrænset rationelle og der ikke er fuldkommen information. Det antages, at aktørerne har nogle interesser, som opfattes økonomisk. Aktørerne tilstræber så at handle rationelt, hvor de forsøger så vidt muligt at træffe de valg, der skaber de størst mulige fordele i forhold omkostningerne. Der er dog ingen garanti for, at denne handlen i virkeligheden maksimerer deres nytte. Dette er en følge af, at aktørernes kognitive egenskaber er for begrænsede, til at de kan overskue alle tænkelige handlemuligheder og deres konsekvenser. Verden er altså for kompleks til, at aktørerne er i stand til at træffe de valg, der i virkeligheden ville optimere deres nytte.¹⁰¹

¹⁰⁰ Paccès, Alessio M. & Visscher, Louis T. 2013. *Methodology of Law and Economics*. Artikel, afsnit 3.2

¹⁰¹ Hansen, Anders Christian. 2007. *Uden for hovedstrømmen - Alternative strømninger i økonomisk teori*. Roskilde Universitetsforlag, s. 48

Derudover vil aktørerne som tidligere nævnt have en opportunistisk adfærd. Dette er også en af adfærdsantagelserne i Williamsons transaktionsomkostningsteori. Williamson definerer opportunistisme som "... self-interest seeking with guile". Dette er en lidt kontroversiel antagelse, og der er også senere kommet blødere versioner af begrebet.¹⁰² Ved opportunistisme tages der i denne afhandling udgangspunkt i Carstens A. Koch's version, hvor aktørerne er villige til at fremme deres egeninteresse, selv om dette sker på bekostning af de andre parter i transaktionen, eller at det fører til en aftale, som de andre parter ikke ville acceptere, hvis de havde fuld forståelse for situationen.¹⁰³ Det er desuden ikke nødvendigt, at alle aktører på markedet er opportunistiske, for at nedenstående analyse holder. Det antages at tilstrækkeligt mange er det.¹⁰⁴ At aktørerne på markedet både er begrænset rationelle og opportunistiske gør, at der er stor mulighed for, at der opstår informationsfejl.

3.8.2. Informationsfejl

At der foreligger en informationsfejl (information failure) betyder, at markedsfejlen kommer til udtryk ved, at en eller begge parter i transaktionen ikke har fuld information, når der tages en økonomisk beslutning.

Informationsfejl findes i mange former, hvor den mest almindelige er, at den ene part har mere information end den anden. Det kan være en sælger, som kender den reelle værdi af en vare, uden at fortælle dette til køberen, som værdsætter varen højere.

Men informationsfejl kan også komme til udtryk ved, at det er svært at vurdere omkostningerne og fordelene ved en transaktion. Dette kan f.eks. skyldes manglende oplysning eller opmærksomhed, således at forbrugeren ikke er klar over den sande personlige omkostning ved transaktionen. Eksempler på det er de dårlige effekter, som tobak og sukker har på vores helbred.

¹⁰² Hansen, Anders Christian. 2007. *Uden for hovedstrømmen - Alternative strømninger i økonomisk teori*. Roskilde Universitetsforlag, s. 66-67

¹⁰³ Koch, C.A. *Trust, Opportunism, Protective Mechanisms and Institutions*. I Nielsen, K., red.: *Social Capital, Trust and Networks*. Publiceret af Edward Elgar i 2006

¹⁰⁴ Hansen, Anders Christian. 2007. *Uden for hovedstrømmen - Alternative strømninger i økonomisk teori*. Roskilde Universitetsforlag, s. 66-67

Med anerkendelsen af, at individer er begrænset rationelle, og at de ikke besidder fuldkommen information, er der dermed en risiko for, at den sande værdi af en vare eller tjeneste ikke bliver taget i betragtning. Netop på persondatarettens område er denne risiko stor, da dette er et felt, som har været og er i rivende udvikling. En almindelig borger er derfor ofte ikke klar over, hvor meget vedkommendes persondata er værd for virksomhederne.

Der er f.eks. flere eksempler på, at folk frivilligt betaler med deres persondata, for at få apps på telefonen, selv om den samme app kan fås for nogle få kroner, og hvor persondata ikke bliver en del af transaktionen. Det betyder, at den reelle værdi af persondata, og dermed databeskyttelse, ikke indregnes i beslutningstagningen, hvilket så gør, at efterspørgslen på databeskyttelse falder på et niveau, der ikke er optimalt. Altså gør den asymmetriske information og individets begrænsede rationalitet, at der indgås transaktioner, som i virkeligheden ikke maksimerer individets nytte. Der er altså tale om en informationsfejl på markedet.

3.8.3. Hvordan markedet reagerer på informationsfejl

At der konstateres en markedsfejl, er dog ikke i sig selv grund til, at lovgiver skal ind og regulere. Når der er tale om en informationsfejl som den ovenstående, kan markedet også rette sig selv.

Som tidligere nævnt, så kan fokus på datasikkerhed, herunder databeskyttelse gennem design, også være en konkurrencefordel. Leverandører af datasikkerhedsløsninger kan markedsføre vigtigheden af datasikkerhed, og således oplyse borgerne om værdien af deres persondata. Virksomheder kan differentiere sig på markedet ved at have større fokus på datasikkerhed, således at brugerne vælger dem foran de billigere løsninger, hvor de derimod enten skal betale med persondata, eller bare generelt ikke får den samme datasikkerhed. På den måde vil efterspørgslen efter databeskyttelse rykke sig til det optimale niveau, ved at markedet selv retter op på den informationsfejl, der er opstået.

Men denne effekt modsvares af de økonomiske aktørers opportunisme på databeskyttelsesområdet, som derfor skal analyseres nærmere.

3.8.4. Opportunisme

Når aktørerne på markedet er opportunistiske, så betyder det, at virksomhederne kan udnytte en eventuel markedsfejl til egen fordel. Når markedsfejlen er, at en virksomhed har fået for stor markedsmagt, så udnytter denne virksomhed markedsmagt – og derved markedsfejlen – til at maksimere egen nytte ved at sætte priserne op. Dette går ud over brugerne, men virksomhedens opportunisme gør, at velfærdstab for borgerne ikke tages i betragtning.

På samme måde kan en informationsfejl på markedet for persondata udnyttes af virksomhederne. Virksomhederne ved, at informationsfejlen er til stede. De ved, at borgerne ikke er rationelle, og at de ikke kender den sande værdi af deres persondata. Dette kan opportunistiske virksomheder udnytte, ved at indsamle persondata og bruge det kommercielt. Når en app-udvikler f.eks. kræver irrelevante og unødvendige personoplysninger fra borgeren, for at en app kan hentes gratis, er dette et fint eksempel på opportunisme. App-udvikleren er klar over, at persondata ikke værdsættes højt nok af forbrugerne på grund af deres begrænsede rationalitet, og dette udnyttes til at maksimere egen nytte – hvilket så resulterer i et velfærdstab.

3.9. Spilteori med to spil

For at illustrere hvordan virksomhedernes opportunisme og forbrugernes begrænsede rationalitet påvirker markedsligevægten, skal spilteorien anvendes.

Der skal i det følgende præsenteres to spil, hvor der tages udgangspunkt i eksemplet med de to lommelygteapps. Den ene er gratis at hente, men den skal have adgang til forbrugerens persondata, som så bliver videresolgt kommercielt. I det første spil, har forbrugeren ikke den opfattelse, at det koster ham noget, at virksomheden får adgang til vedkommendes persondata.

Vi antager, at appen giver en nytte for forbrugeren på 10, uanset om den er gratis eller der skal betales for den. Derudover antages at virksomheden får en nytte på 10 for at få adgang til forbrugerens persondata. Betalingsappen koster 7 kroner at downloade, og det koster virksomheden 3 kroner at udvikle appen, uanset om det er en betalingsversion eller det er en gratisapp.

Det antages for at simplificere, at virksomheden må vælge enten at udvikle betalingsappen, eller gratisappen. Den kan ikke udvikle begge.

Virksomheden får dermed et overskud på 4 (7-3), hvis forbrugeren vælger at købe betalingsappen, og et overskud på 7 (10-3), hvis forbrugeren henter gratisappen. Virksomheden får et underskud på -3, hvis den udvikler en app, som forbrugeren ikke downloader. Forbrugeren får en nytte på 10 (10-0) ved at hente gratisappen, og en nytte på 3 (10-7) ved at hente betalingsappen.

Figur 3.5. Spil 1: Når forbrugeren ikke inddrager omkostningerne ved at udlevere persondata (Egen tilvirkning)

Virksomhed / Forbruger	Henter gratisapp	Henter betalingsapp
Udvikler gratis-app	7, 10	-3, 3
Udvikler betalingsapp	-3, 10	4, 3

Når de økonomiske aktører nyttemaksimerer, vælger de altid den løsning, som maksimerer deres egen nytte, uanset hvad den anden person får ud af transaktionen. Der er i ovenstående spil kun én Nash-ligevægt, og den er, at virksomheden udvikler en gratisapp, og at forbrugeren downloader denne. Virksomhederne har dermed ikke noget incitament til at udvikle sikre betalingsapps, da de ved, at de får mere ud af, at lave gratisapps, hvor de får adgang til forbrugernes persondata.

Det antages nu, at borgeren ser det som en omkostning på 8 at udlevere sine persondata. De øvrige antagelser er de samme.

Virksomheden får dermed stadigvæk et overskud på 4 (7-3), hvis forbrugeren vælger at købe betalingsappen, og et overskud på 7 (10-3) hvis forbrugeren henter gratisappen. Virksomheden får et underskud på -3, hvis den udvikler en app, som forbrugeren ikke henter. Forbrugeren får en nytte på 2 (10-8) ved at hente gratisappen, og en nytte på 3 (10-7) ved at hente betalingsappen.

Figur 3.6. Spil 2: Når forbrugeren inddrager omkostningerne ved at udlevere persondata (Egen tilvirkning)

Virksomhed / Forbruger	Henter gratisapp	Henter betalingsapp
Udvikler gratis-app	7, 2	-3, 3
Udvikler betalingsapp	-3, 2	4, 3

Igen er der kun én Nash-ligevægt, men den har rykket sig og er nu, at virksomheden udvikler en betalingsapp, og at forbrugeren downloader denne. Virksomhederne har nu incitament til at udvikle sikre betalingsapps, da de ved, at forbrugerne værdsætter deres persondata, og ikke vil downloade gratis-appen, hvis de har et alternativ, hvor deres nytte er større.

Selv om gratisappen kan give virksomheden en nytte på 7, som er større end de 4, som fås gennem betalingsappen, så er det urealistisk at virksomheden realiserer denne nytte. En konkurrent kan nemt udvikle en betalingsapp, og derved snuppe hele markedet, således at den første virksomhed i stedet står med et underskud på -3.

Ovenstående to spil viser hvordan forbrugernes opfattelse af deres omkostning ved at dele persondata, kan have væsentlig betydning for deres beslutningstagning – og derved på virksomhedernes incitament til at udvikle sikre apps. Spillene viser også, at virksomhederne får 3 mindre i overskud, når forbrugerne er bevidste om omkostningen ved at dele persondata. Det betyder, at virksomhederne i dette eksempel er bedre stillede, hvis forbrugerne ikke er rationelle, da dette kan udnyttes til virksomhedernes fordel.

I en verden, hvor forbrugerne er fuldt rationelle, ville nyttemaksimeringen ligne spil 2, og i dette tilfælde vil virksomhederne have en klar konkurrencefordel på markedet, hvis de udbyder et produkt, hvor databeskyttelse er i fokus. Forbrugerne kender værdien af deres persondata, og ville indregne prisen for manglende databeskyttelse i deres nyttemaksimering.

Hvis verden derimod ligner spil 1, hvor forbrugerne slet ikke indregner prisen for den manglende databeskyttelse i deres nyttemaksimering, vil virksomhederne ikke have nogen konkurrencefordel ved at satse på databeskyttelse. I og med at virksomhedernes overskud i dette spil er højere (7), end det er i det andet spil (4), har virksomhederne heller ikke noget incitament til at oplyse forbrugerne om, hvilke fordele forbrugerne kan få ved databeskyttelse, da denne fordel ikke kommer virksomhederne til gode. Virksomhederne er med andre ord godt tilfredse, hvis verden ligner Spil 1, og har intet ønske om, at den skal ændre sig.

Det skal bemærkes, at selv om der kun er én Nash-ligevægt i spil 2, og at dette punkt er Pareto-efficient, så er det ikke Kaldor-Hicks-efficient. Punktet er Pareto-efficient, i og med at ingen kan stilles

bedre, uden at det går ud over den anden part. Punktet er derimod ikke Kaldor-Hicks-efficient, i og med at den samlede nytte ville være større, hvis gratis-appen blev udviklet og downloadet. Det ville betyde at den samlede nytte var 9 ($7+2$) i stedet for 7 ($4+3$). Det betyder, at selv om markedet nu har valgt en løsning, hvor databeskyttelse er værdsat, så er det i dette eksempel ikke det optimale fra set et samfundssynspunkt. Dette er en følge af, at i dette tilfælde er værdien af persondata højere for virksomhederne (10), end omkostning ved at betale med persondata er for forbrugeren (8).

I teorien kan virksomheden derfor kompensere forbrugeren, for at få forbrugeren til at vælge gratisappen. Det kan resultere i en mellemløsning, hvor virksomheden gennem gratisappen blot indsamler mindre persondata, således at noget af nytten bliver rykket over til forbrugeren.

Virksomheden kan dermed få en nytte af det indsamlede persondata på 8 i stedet for 10, mens forbrugeren får en omkostning på 6 i stedet for 8. Dette ville betyde en samlet nytte på 5 til virksomheden og 4 til forbrugeren, som er både Pareto- og Kaldor-Hicks-efficient. Dette spil illustreres nedenfor.

Figur 3.7. Udvidelse til spil 2: Når virksomheden kan kompensere forbrugeren (Egen tilvirkning)

Virksomhed / Forbruger	Henter gratis-app	Henter betalingsapp
Udvikler gratis-app	[7-2], [2+2]	-3, 3
Udvikler betalingsapp	-3, 2	4, 3

Under disse forudsætninger ville markedet således lande på en løsning, der både er Kaldor/Hicks og Pareto efficient. I og med at persondata har så stor en værdi for virksomhederne, vil der stadigvæk blive indsamlet og profiteret på forbrugers persondata, men det ville ikke gå ud over, hvad forbrugerne anså som rimeligt. At forbrugeren er bevidst om omkostningen ved at dele persondata, og derved efterspørger et databeskyttelsesniveau, der svarer til det, gør derved, at markedet lander på det punkt, som maksimerer den sociale velfærd. Virksomhederne mister dog stadigvæk en nytte på 2 i forhold til Spil 1, da de nu skal kompensere forbrugeren ved ikke at indsamle så meget persondata, som ellers ønsket.

Ovenstående spil har illustreret, for det første hvordan virksomhedernes opportuniste kan hindre markedet i at rette op på eventuelle markedsfejl, og derved lande i det punkt, som maksimerer den sociale velfærd. For det andet at værdien af at indsamle og profitere på persondata kan være højere for

virksomhederne, end eventuelle fordele ved at tilbyde lignende løsninger, hvor databeskyttelse er i fokus.

3.10. Konklusion på økonomisk analyse

Databeskyttelse gennem design kan ifølge den økonomiske teori udgøre en konkurrencefordel på markedet, og nogle virksomheder vil måske af egen drift implementere princippet. Dette er vist ved brug af både Porters konkurrencestrategier og the Hotelling model.

Selv om der ikke kan sættes et konkret tal på, har persondata en stor værdi for virksomhederne. Der er dog meget, der tyder på, at forbrugerne ikke efterspørger en databeskyttelse, der svarer til denne høje værdi. Med udgangspunkt i Adam Smith's model for sikkerhed på arbejdsmarkedet er det vist, at der er en stor risiko for, at der opstår markedsfejl på markedet for databeskyttelse. Forbrugere er ikke bevidste om den høje værdi af deres persondata samt risikoen ved manglende databeskyttelse, hvilket negativt påvirker efterspørgslen på databeskyttelse.

Det er konkluderet, at markedet for databeskyttelse er underlagt markedsfejl i form af informationsfejl. Den asymmetriske information og individets begrænsede rationalitet gør, at der indgås transaktioner, som i virkeligheden ikke maksimerer individets nytte.

Når der er tale om en informationsfejl, kan markedet dog også rettes op af sig selv. Ved brug af spilteorien er det konkluderet, at markedsfejlen ikke bliver rettet op, da virksomheder er opportunistiske, og udnytter forbrugernes begrænsede rationalitet. Dette medfører at markedet lander i et punkt, som ikke maksimerer den sociale velfærd.

Det kan dermed konkluderes, at selv om indførelse af princippet om databeskyttelse gennem design kan have en økonomisk værdi fra et virksomhedssynspunkt, så er værdien af at indsamle persondata og at profitere på dette endnu større. Dette har medført, at der nu er indført strikse krav om databeskyttelse i lovgivningen, herunder kravet om databeskyttelse gennem design. Virkningerne af dette krav skal derfor undersøges i den integrerede analyse.

Kapitel 4: Integreret analyse

4.1. Indledning

I den økonomiske analyse blev markedet for databeskyttelse analyseret, og det blev konkluderet, at markedet var underlagt en markedsfejl i form af en informationsfejl. Individets begrænsede rationalitet sammenholdt med den asymmetriske information på markedet medfører, at der indgås transaktioner, som i virkeligheden ikke maksimerer individets nytte. Denne markedsfejl gør, at det optimale databeskyttelsesniveau set fra lovgivers side, ikke opnås. Det kan dermed ud fra økonomiske teorier retfærdiggøres, at lovgiver regulerer markedet for databeskyttelse.

Det skal derfor i det følgende analyseres, hvordan kravet om databeskyttelse gennem design, som blev analyseret i den juridiske analyse, påvirker markedet for databeskyttelse, herunder markedsfejlen, der blev introduceret i den økonomiske analyse. Overordnet skal der i det følgende laves en efficiensanalyse af Persondataforordningens art. 25, stk. 1, hvor virksomhederne er i fokus.

Som nævnt i den økonomiske analyse, så er der tale om økonomisk efficiens fra lovgivers synsvinkel, når den sociale velfærd (målt som summen af forbrugervelfærd og industriens profit) er maximeret. I og med at det er lovgivning, der analyseres, og at formålet med denne lovgivning først og fremmest er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, er det naturligt også at inddrage samfundet som helhed. Analysen vil derfor tage udgangspunkt i ovennævnte efficiensbegreb, blot med særlig fokus på virksomhederne.

Bestemmelsens efficiens afhænger for det første af, om markedsfejlen effektivt bliver rettet op. Her opstilles to betingelser. Det er for det første afgørende, at lovgiver har valgt det optimale databeskyttelsesniveau, hvilket svarer til, hvad rationelle individer med fuldkommen information ville efterspørge. For det andet skal der være effektiv håndhævelse, således at de dataansvarlige overholder bestemmelsen.

Men bestemmelsens efficiens afhænger derudover af, om den er efficient i forhold til lovgivningens formål, samt hvilke øvrige effekter den har på virksomhederne og dermed samfundet. Selv om en regel kan rette op på noget, så vil der ofte være en bagside af medaljen, hvilket skal undersøges nærmere.

Ovenstående tre betingelser skal derfor undersøges i det følgende.

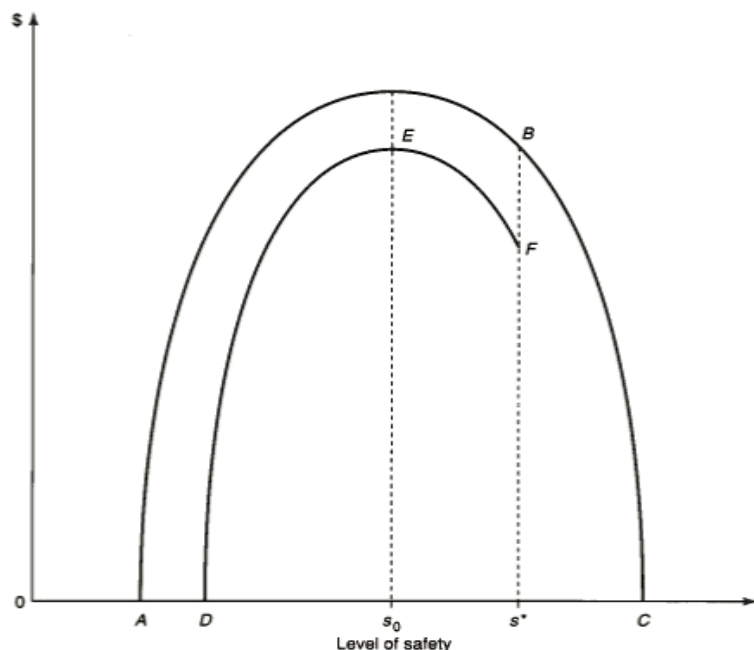
4.2. Bestemmelsens efficiens i forhold til markedsfejlen

Som det fremgår af den juridiske analyse, så har EU med Persondataforordningen med princippet om databeskyttelse gennem design indført et meget vidtgående begreb, som ikke tidligere har været en del af persondatalovgivningen i samme omfang. I den økonomiske analyse blev der set på, hvordan markedet selv finder et databeskyttelsesniveau, hvis der ikke er regulering. Det skal derfor i det følgende analyseres, hvordan lovgivers konkrete krav om databeskyttelse gennem design påvirker virksomhederne, og herunder om det løser markedsfejlen, der blev introduceret i den økonomiske analyse.

Af nedenstående model fremgår en virksomheds mulige profit ved forskellige grader af databeskyttelse indbygget i deres it-system. Denne er først tiltagende, da indtjeningen overstiger udgiften til et vist punkt. Herefter er den nedadgående, da udgiften pludselig bliver større end indtjeningen ved den øgede mængde databeskyttelse. I nedenstående model er det optimale punkt for virksomheden S_0 . Det er her, at profitten for virksomheden er størst. Det er dermed dette punkt, som markedet ville vælge, hvis der ikke var nogen regulering på markedet. Dette punkt svarer dermed til det optimale punkt i Adam Smith's model for sikkerhed på arbejdsmarkedet, som blev introduceret i den økonomiske analyse.

Denne model har fokus på virksomhedernes profit ved at indarbejde databeskyttelse i deres systemer. Modellen giver også mulighed for at se, hvad der sker med virksomhedernes profit, hvis lovgiver kræver et højere niveau af databeskyttelse, end hvad markedet selv ville komme frem til. Det antages her i overensstemmelse med resultaterne fra den økonomiske analyse, at de fleste virksomheder på markedet ikke indfører databeskyttelse gennem design, når dette ikke er lovkrævet.

Figur 4.1.¹⁰⁵



Ved indførelse af forordningens krav om databeskyttelse gennem design sker det, at den krævede databeskyttelse rykkes fra det optimale punkt set fra virksomhedssynspunkt, over til et nyt punkt længere til højre. Samtidigt indføres en bøde for manglende overholdelse af bestemmelsen. Om virksomheden vil overholde denne, afhænger af, om det kan betale sig for virksomheden.

Virksomhedens mulige profit ved manglende overholdelse af loven rykker nedad grundet indførelse af bøden for manglende overholdelse. Afstanden mellem de to grafer i ovenstående model symboliserer den forventede bøde ved overtrædelse. Rykket nedad i kurven gælder op til punktet for den krævede mængde databeskyttelse. Herefter vil virksomheden ikke kunne få en bøde, da den fra dette punkt opfylder loven og derfor er dens mulige profit den samme, som inden indførelsen af kravet om databeskyttelse gennem design.

I ovenstående model antages det, at den ønskede mængde databeskyttelse sættes af lovgiver til S^* . Den højest mulige profit, som virksomheden kan opnå, hvis denne skal overholde kravet, er ved punkt B.

¹⁰⁵ Viscusi, W. Kip; Harrington, Joseph E. and Vernon, John M. 2005. *Economics of regulation and antitrust*. The MIT Press. 4. udgave, s. 852, figure 23.4

Hvis virksomheden ikke overholder og sikrer højere databeskyttelse, men bliver på samme punkt som inden indførelsen af lovgivningen, vil virksomheden kun opnå profitten E. Dette grundet indførelsen af bøden for manglende overholdelse.

Det elementære set fra virksomhedens synspunkt, når den skal vælge, om den skal overholde, er altså om punkt B er større end punkt E. I ovennævnte situation er punkt B højere end E og virksomheden vælger derfor den fra lovgivers side ønskede mængde sikkerhed, da profitten her er højere, end hvis den vælger at blive på det tidligere punkt, hvor den kun kan opnå profitten E. Men selv om dette måske er tilfældet for én virksomhed på markedet, så er det ikke nødvendigvis tilfældet for alle. Da virksomheder er forskellige, vil de også påvirkes forskelligt, når lovgiver sætter et databeskyttelsesniveau. For at analysere hvordan dette påvirker virksomhederne på markedet, skal modellen udvides med eksempler på tre forskellige virksomheder.

4.2.1. Forskel på virksomheder

For nogle virksomheder vil det måske være helt urealistisk at skulle overholde lovgivningen. Dette understøttes også af den tidligere nævnte undersøgelse fra Devoteam, hvoraf det fremgik, at de fleste virksomhederne ikke har en plan for overholdelse af Persondataforordningen. Selvom der kan være stor forskel på virksomhederne, som rammes af kravet, så er kravet det samme for alle. Princippet om databeskyttelse gennem design skal overholdes, uanset hvilken type virksomhed der er tale om. Dog skal det bemærkes, at bestemmelsen også tager hensyn til implementeringsomkostningerne, og disse kan selvsagt være forskellige, alt efter hvilken virksomhed der er tale om.

Ud fra den tidligere model om én virksomheds mulige profit, kan der identificeres tre typer virksomheder, således at modellen udvides. Disse tre virksomheder rammes på forskellig måde af kravet om databeskyttelse gennem design. Disse tre typer vil generelt opstå, når der indføres nye krav.¹⁰⁶ Men hvor mange af hver type virksomhed afhænger derimod af, hvor omfattende kravet er.

¹⁰⁶ Viscusi, W. Kip; Harrington, Joseph E. and Vernon, John M. 2005. *Economics of regulation and antitrust*. The MIT Press. 4. udgave, s. 853

For det første har vi en virksomhed, hvor det vil være helt urealistisk at overholde lovgivningen, for det andet har vi en virksomhed, hvor det kan betale sig at indføre databeskyttelse gennem design, og for det tredje en virksomhed, som allerede opfylder kravet. Den tredje type er der dog næppe mange af på nuværende tidspunkt.

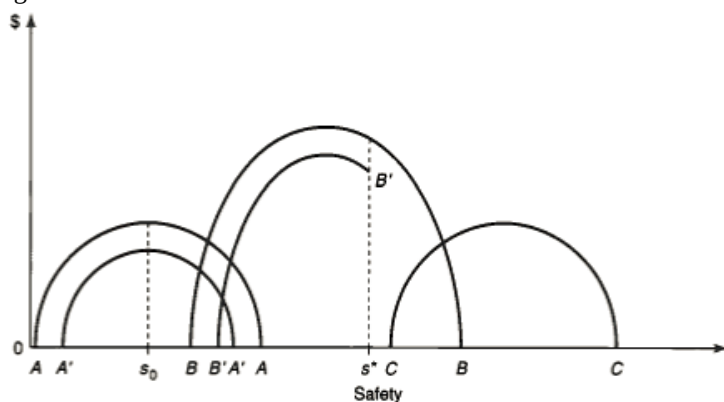
Af nedenstående model fremgår de tre eksempler på virksomheder, der rammes af kravet om databeskyttelse gennem design. Den første virksomhed har profitmuligheden AA inden ny lovgivning og herefter A'A'. Virksomheden har inden indførsel af ny lovgivning en databeskyttelse på S_0 . Hvis kravet efter indførsel af ny lovgivning er S^* , vil virksomheden alligevel ikke ændre på mængden af databeskyttelse, da det ikke kan betale sig for virksomheden. Det er slet ikke muligt for virksomheden at komme helt derop. Virksomheden har ikke råd til at indføre den fra lovgivers side ønskede mængde af databeskyttelse, og må derfor vælge at indregne den forventede bøde i sin profitmaksimering. Det betyder, at databeskyttelsen bliver den samme på punktet S_0 , men profitten falder med den forventede bøde, hvilket fremgår af forskellen på de to grafer (AA og A'A').

For den anden virksomhed, der har profitmuligheden BB inden ny lovgivning og B'B' efter, vil det derimod kunne betale sig at opfylde loven og øge mængden af databeskyttelse til S^* . Dette svarer dermed til virksomheden, som fremgik af den tidligere model.

For den tredje virksomhed, der har profitmuligheden CC, ændrer den nye lovgivning intet, da virksomheden allerede inden den nye lovgivning er over punktet S^* , da dens optimale punkt er til højre for dette punkt. Dette er dermed en virksomhed, som allerede har differentieret sig, og satset på databeskyttelse. Denne vil heller ikke sætte databeskyttelsesniveauet ned, i og med at virksomhedens profit allerede er maksimeret ved at have en databeskyttelse, der går langt ud over kravet.

Nedenstående model viser altså, at lovgiver kan risikere, at ny lovgivning sætter baren så højt, at det ikke kan betale sig for virksomhederne at overholde den. Dette er tilfældet, hvis de fleste virksomheder svarer til den første type i nedenstående model. Det ændrer intet selvom bødeniveauet sættes højt, da bødeniveauet netop ikke ændrer på grafens brede, eller hvor på x-aksen den befinder sig, men kun på hvor langt ned den rykker under den tidligere. Uanset hvor langt ned den nye graf (A'A') sættes på grund af en høj bøde, så vil virksomheden aldrig kunne overholde lovgivningens krav, og den vil derfor ikke ændre sit databeskyttelsesniveau – den vil kun miste størstedelen af sin profit.

Figur 4.2.¹⁰⁷



Lovgiver har dog forsøgt at afhjælpe dette problem ved at indføre en begrænsning af kravet i forordningens art. 25, stk. 1, således at virksomhederne også kan tage hensyn til implementeringsomkostningerne, når de implementerer princippet. Kravet bliver på den måde lidt forskelligt fra virksomhed til virksomhed, i og med at de forholdsmæssige implementeringsomkostninger kan variere meget. Det bliver dog ikke uddybet, hvad en rimelig implementeringsomkostning er, og det bliver dermed meget usikkert for en lille virksomhed, at køre med den argumentation, hvis den vælger at slække på implementeringen af princippet. Som det fremgår af den juridiske analyse, har EU-Domstolen tidligere tilsidesat kommercielle interesser, når grundlæggende databeskyttelsesrettigheder skal beskyttes.

Pointen med ovenstående modeller er at vise, at det har meget stor betydning for virksomhederne, hvor omfattende et nyt lovkrav er, samt hvor effektiv håndhævelsen af kravet er, når de afgør, om de vil indrettet sig efter kravet.

4.2.2. EU's valg af databeskyttelsesniveau

Med udgangspunkt i de to foregående analyser, kan der argumenteres for, at EU med kravet om databeskyttelse gennem design netop kræver et databeskyttelsesniveau, der klart overgår det niveau, som markedet ellers ville ende på.

¹⁰⁷ Viscusi, W. Kip; Harrington, Joseph E. and Vernon, John M. 2005. *Economics of regulation and antitrust*. The MIT Press. 4. udgave, s. 853, figure 23.5

Spørgsmålet er dog, om dette punkt svarer til, hvad rationelle forbrugere med fuldstændig information ville efterspørge, hvilket er første betingelse for, at markedsfejlen effektivt rettes op, eller om lovgiver har valgt et inefficiant niveau af databeskyttelse. Dette kan ovenstående analyse ikke give et klart svar på, da denne efterspørgsel ikke kan defineres nøjagtigt.

Ved at der nu i punkt S* kræves et højere niveau af databeskyttelse, har lovgiver med indførelsen af kravet om databeskyttelse gennem design dog under alle omstændigheder rettet op på den lave efterspørgsel efter databeskyttelse. Derudover har forordningen generelt sat et øget fokus på databeskyttelse, hvilket også er med til at rette op på markedets informationsfejl, i og med at folk bliver mere oplyst om værdien af deres data.

Det skal i det følgende undersøges, om virksomhederne overhoved vil overholde bestemmelsen, hvilket er den anden betingelse for, at markedsfejlen effektivt bliver rettet op.

4.2.3. Overholdelse af forordningen

Virksomhederne bliver nødt til at tage stilling til, om de vil overholde bestemmelsen, og lige gyldigt om de gør eller ej, kan det have store økonomiske konsekvenser for dem.

Som det fremgår af ovennævnte modeller, vil virksomheders opfyldelse af kravet afhænge af, om den forventede omkostning til overholdelse er mindre end den forventede omkostning ved ikke at opfylde kravet. Til det sidstnævnte skal medregnes sandsynligheden for at blive opdaget. Det vil sige, at:

Omkostning til overholdelse < sandsynligheden for at blive opdaget x bøden for overtrædelse af bestemmelsen

Når virksomheder skal beslutte, om de skal bruge udgifter på at ændre på deres it-systemer, kræver det altså, at ovenstående ligning er opfyldt. Inden der skal gås i dybden med den første del af ligningen *omkostning til overholdelse*, skal de to andre dele gennemgås.

4.2.3.1. Bøden for overtrædelse af bestemmelsen

Som tidligere nævnt i den juridiske analyse, er der i Persondataforordningen introduceret langt højere bødestørrelser end tidligere.

Den høje mulige bødestørrelse skal afskrække bl.a. virksomhederne fra at overtræde kravet om databaseskyttelse gennem design. At bødeniveauet er steget fra det, som indtil videre højst har været på 25.000 kr., til bøder helt op til 10.000.000 EUR, hvilket svarer til over 74 mio. danske kroner, har uden tvivl en afskrækkende virkning. Det skal dog bemærkes, at forordningen blot angiver et maksimum beløb, og de konkrete bødestørrelser er stadigvæk ukendte. Men der er dog ingen tvivl om, at bødeniveauet vil blive hævet betydeligt.

Når Persondataforordningen har været i kraft i en tid, og der er udstedt et par bøder, vil "bøden for overtrædelse af bestemmelsen" i ovenstående ligning kunne klarlægges mere præcist, og i stedet blive til "gennemsnitlig bøde for overtrædelse af bestemmelsen". Indtil dette er tilfældet, afgøres "bøden for overtrædelse af bestemmelsen" ud fra, hvad virksomhederne forventer, at bøden bliver, hvis de bliver fanget i at overtræde bestemmelsen.

Virksomhederne kender til de historiske data for bødeniveau for overtrædelse af lovgivningen, som har været på et meget lavt niveau, og det må derfor forventes, at virksomhederne også ser på sandsynligheden for, at vi i Danmark overhoved vil give så store bøder, som forordningen lægger op til. Juraprofessor fra KU, Henrik Udsen har udtalt, at han ikke finder det realistisk, at der skulle blive udskrevet bøder i den størrelse, som forordningen lægger op til, i hvert fald ikke i starten.¹⁰⁸ Derudover har direktør i Datatilsynet Christina Gulisano udtalt, at Datatilsynet mangler ressourcer for at kunne håndhæve forordningen, hvilket analyseres nærmere nedenfor, når der ses på Datatilsynets forventede tilsyn.¹⁰⁹

Der er altså to faktorer - historiske bøder og forventningen til bødeniveauet, som dermed kan påvirke virksomhederne, når de skal vurdere deres omkostninger til henholdsvis overholdelse/ikkeoverholdelse af bestemmelsen. Det betyder, at hvis virksomhederne ikke forventer, at der nogensinde vil blive givet

¹⁰⁸ Villadsen, Steffen. 19. juni 2017. *Professor: Minimal risiko for kæmpebøder til virksomheder når EU-persondataforordningen træder i kraft*. Artikel udgivet på Computerworld.dk. Direkte link: <https://www.computerworld.dk/art/240309/professor-minimal-risiko-for-kaempeboeder-til-virksomheder-naar-eu-persondataforordningen-traeder-i-kraft>

¹⁰⁹ Fribo, Adam. 13. juni 2017. *Datatilsynet 11 måneder før persondataforordningen: "Vi kan ikke håndhæve loven med de nuværende ressourcer"*. Artikel udgivet på Computerworld.dk. Direkte link: <https://www.computerworld.dk/art/240265/datatilsynet-11-maaneder-foer-persondataforordningen-vi-kan-ikke-haandhaeve-loven-med-de-nuvaerende-ressourcer#O3zY1ifKoT4wyB1E.99>

en bøde på over 10 mio., så ville beregningen i nedenstående afsnit kun blive lavet med sandsynligheden for at blive opdaget ganget med 10 mio., og ikke med 74 mio.

Der er dermed meget, der taler for, at virksomhederne ikke forventer, at bøderne bliver så høje, som forordningen lægger op til – i hvert fald i starten.

Som det fremgår af ovenstående ligning, så udgør selve bødestørrelsen også kun en tredjedel af ligningen, når virksomhederne overvejer, om de vil overholde kravet. Bødestørrelsen skal for det første ganges med sandsynligheden for at blive opdaget, og derefter holdes op imod omkostningen ved at overholde kravet.

4.2.3.2. Sandsynligheden for at blive opdaget

Vi antager nu, at en virksomhed regner med at skulle betale hele 74 mio. kr., hvis den bliver opdaget i at overtræde bestemmelsen. Virksomheden forventer dog kun at sandsynligheden for at blive opdaget i overtrædelsen er 5 %. Det betyder, at den forventede bøde for virksomheden ved at overtræde bestemmelsen er på $0,05 \times 74 = 3,75$ mio. kr. Det er derfor dette tal, og ikke de 74 mio. som virksomheden holder op imod omkostningen ved at overholde bestemmelsen om databeskyttelse gennem design. Hvis implementeringen af princippet i dette tilfælde har en omkostning for virksomheden, der overstiger 3,75 mio. kr., vil det ikke betale sig for virksomheden at overholde kravet, medmindre den også inddrager andre ting i sin nyttemaksimering, som f.eks. risikoen for dårlig medieomtale og tab af kunder. Hvis virksomheden derimod først er blevet opdaget i overtrædelse en gang, er risikoen nok nærmere 100 % for, at der bliver fulgt op fra tilsynsmyndighedernes side, og så er det forventede bødeniveau fremover steget til de 74 mio. kr.

Sandsynligheden for at blive opdaget afhænger naturligvis af, hvilken grad af tilsyn der vil blive ført med reglerne. Den forventede grad af tilsyn fra tilsynsmyndighederne, vil derfor have en helt afgørende betydning for virksomhedernes forventede bøde ved overtrædelse, og dermed også deres incitamenter til at overholde lovgivningen.

Her er det relevant at se på, hvordan tilsynsopgaven forventes udført i Danmark, hvor det er Datatilsynet, der er tilsynsmyndighed. Datatilsynets nuværende organisation og opgaver fremgår af Persondatalovens kapitel 55. Det fremgår af forslaget til den nye databeskyttelseslov, at Datatilsynets

organisation og opgaver fremover vil fremgå af Databeskyttelseslovens kapitel 10. Det fremgår af lovforslagets § 27, at Datatilsynet i overensstemmelse med forordningens kapitel VI-VII fører tilsyn med enhver behandling, der omfattes af Databeskyttelsesloven, forordningen og anden lovgivning, som ligger inden for forordningens rammer for særregler om behandling af personoplysninger.

Tilsynenes kompetence fremgår af Persondataforordningens art. 55-56, mens tilsynenes beføjelser fremgår af art. 58, stk. 1-3. Det fremgår endvidere af lovforslagets § 35, at Justitsministeren kan fastsætte nærmere regler om, at Datatilsynet og Domstolsstyrelsen har yderligere beføjelser end dem, der er omhandlet i forordningens art. 58, stk. 1, 2 og 3. Udgangspunktet er, at disse beføjelser skal udøves af en tilsynsmyndighed på dens eget territorium, jf. forordningens art. 55, stk. 1. Overordnet giver art. 58, stk. 1-3 tilsynene undersøgelsesbeføjelser, korrigerede beføjelser, samt godkendelses- og rådgivningsbeføjelser.

Mange af disse beføjelser har Datatilsynet allerede efter gældende ret. Men som det også fremgår af Justitsministeriets betænkning, så gælder dette dog ikke fuldt ud for art. 58, stk. 2, litra c-g om påbud og forbud. Datatilsynet har efter forordningen beføjelse til at pålægge modtageren af et påbud eller forbud at foretage noget aktivt i forhold til en given behandling af personoplysninger, hvilket indebærer en betydelig udvidelse af tilsynets beføjelser.¹¹⁰ Selv om Datatilsynet derved har flere håndhævelsesbeføjelser, så siger dette ikke noget om, i hvilken grad disse vil blive udnyttet, da dette afhænger af, om Datatilsynet får de nødvendige ressourcer til effektiv håndhævelse af forordningen.

Direktør i Datatilsynet, Christina Gulisano, har som nævnt udtalt, at Datatilsynet mangler ressourcer for at kunne håndhæve forordningen. Det har regeringen dog forsøgt at råde bod på ved at tilføre flere penge til Datatilsynet fra 2018 og fremover. Det er dog tvivlsomt, om dette styrker Datatilsynet i den grad, som der er behov for. Datatilsynets direktør Christina Gulisano har udtalt, at med de midler der tilføres, er det kun lige præcis muligt at leve op til EU's krav.¹¹¹

¹¹⁰ Betænkning nr. 1565/2017. *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, s. 799

¹¹¹ Ritzau. 2. september 2017. *Regeringen vil styrke Datatilsynet med flere penge*. Artikel udgivet på dr.dk. Direkte link: <https://www.dr.dk/nyheder/politik/regeringen-vil-styrke-datatilsynet-med-flere-penge>

I forbindelse med lovforslaget til den nye databeskyttelseslov, har folketingets retsudvalg efter ønske fra folketingspolitikere fra Alternativet Josephine Fock stillet to spørgsmål til Justitsministeren, der omhandler Datatilsynets budget.¹¹² Spørgsmålene omfatter det danske Datatilsyns budget holdt op imod andre europæiske landes budgetter på nuværende tidspunkt og fremadrettet. I svaret fra Justitsministeriet er som ønsket budgetter for flere europæiske lande for 2017, 2018 og 2019 – opgjort på tre måder, efter reel bevilling, på baggrund af indbyggertal og på baggrund af landenes BNP. Det første tal siger ikke meget, da bevillingen i sig selv ikke beskriver meget, da det er logisk, at større lande bruger flere penge end mindre lande. Det er dermed ikke så relevant, at Frankrig jf. svaret fra Justitsministeriet bruger 129 mio. i 2017 mod Danmarks 23,7 mio. Derimod bliver det mere relevant, når budgettet opgøres i henhold til befolkningens størrelse. Her ses det, at Danmark, ud af de lande der sammenlignes med, er et af de lande, der fremadrettet bruger flest penge pr. indbygger. I sammenligning med andre EU-lande ligger vi derfor højt på listen, men det er dog ikke lig med, at vi bruger nok penge på det. Derudover kan det diskuteres, om det er den bedste metode at sammenligne på baggrund af indbyggertal. Da Datatilsynet typisk skal føre tilsyn med virksomheder, både i form af private og det offentlige, ville det måske være mere relevant at sammenligne budgetter på baggrund af antallet af virksomheder i landet. Men det er der ikke spurgt til og dermed ikke svaret på fra Justitsministeriet. Hvis der i stedet ses på sammenligningen på baggrund af BNP, er Danmark ikke længere i toppen af listen, men faktisk i bunden.

Det er derfor ikke muligt på baggrund af svaret fra Justitsministeriet at drage nogen konklusion om budgetternes størrelse og dermed afgøre, om de er høje nok til, at Datatilsynet kan udføre sin opgave, eller om de mangler ressourcer som udtalt af Datatilsynets direktør Christina Gulisano. Der hersker dermed stadigvæk usikkerhed omkring Datatilsynets forventede tilsyn.

Når forordningen derimod har været i kraft i et par år, og når der er udstedt nogle bøder, vil virksomhederne derimod have fået et bedre billede af både bødernes gennemsnitsstørrelse, og Datatilsynets grad af tilsyn.

¹¹² Spørgsmål 60 og 61 til L 68 Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, som sambehandles med L 69 Forslag til lov om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love

Denne usikkerhed på nuværende tidspunkt omkring både *bøden for overtrædelse af bestemmelsen* og *sandsynligheden for at blive opdaget*, gør, at den forventede omkostning ved at overtræde bestemmelsen falder. Virksomhederne indregner derfor ikke en omkostning, der svarer til de høje bødestørrelser i forordningen, når de overvejer om det betaler sig at bruge mange omkostninger til overholdelse af princippet om databeskyttelse gennem design, hvilket er den tredje og sidste del af ovenstående ligning.

4.2.3.3. Omkostning til overholdelse

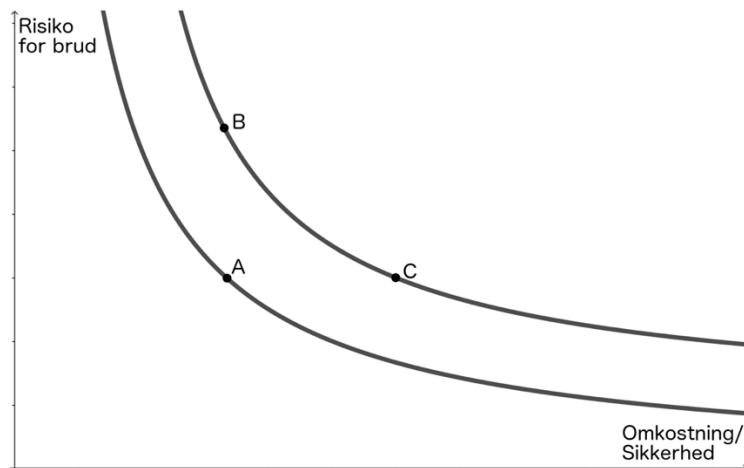
Som nævnt skal bødestørrelsen ganges med sandsynligheden for at blive opdaget, og dette beløb skal så være højere end omkostningen til overholdelse af kravet. Hvis dette er opfyldt, har bøderne en afskrækkende effekt, og giver dermed incitamenter til overholdelse. Der skal derfor i det følgende gås i dybden med, hvilke omkostninger overholdelse af bestemmelsen har for de dataansvarlige. Inden der skal ses på de konkrete omkostninger ved at implementere databeskyttelse gennem design, skal de stigende omkostninger for databeskyttelse generelt kort gennemgås.

4.2.3.3.1. Stigende omkostninger for databeskyttelse

Vi lever i en verden, der bliver mere og mere digitaliseret. Vores afhængighed af velfungerende IT med høj sikkerhed stiger derfor. Samtidig med at vores brug af digitale løsninger stiger, bliver det også mere og mere interessant for hackere at bryde ind i vores systemer og stjæle data. Både til videresalg, da data stor værdi, og for at kunne bruge data som gidsel og dermed kræve løsesum fra virksomhederne for at levere deres data tilbage. Dette er desværre set et stigende antal gange i den senere tid.

I nedenstående model er der to grafer. De viser sammenhængen mellem sikkerhed og omkostningen herfor og forventede sikkerhedsbrud. Der kan argumenteres for, at grafen er blevet skubbet op, idet der er brug for mere sikkerhed for at opnå den samme lave risiko for sikkerhedsbrud. Den nederste graf viser derfor, hvordan det tidligere så ud og den øverste graf viser den nuværende situation. I det udviklingen er dynamisk vil grafen forventeligt også i fremtiden blive skubbet længere og længere op. Forskydningen skyldes som nævnt, at hackere er blevet meget dygtigere til at bryde ind og det er blevet meget mere værdifuldt for dem, idet dataene er blevet mere værdifulde for virksomhederne. Det kræver dermed en øget mængde sikkerhed at undgå hacking.

Figur 4.3. (Egen tilvirkning)



Det er dyrt at have maksimal sikkerhed, hvorfor dette ikke har været det optimale punkt for virksomhederne. Det optimale punkt har derfor måske tidligere været A, som har sikret en forholdsvis lille risiko for brud, men acceptabel i forhold til den krævede mængde sikkerhed og omkostningen hertil. Efter udviklingen er grafen blevet skubbet op og det har derfor ændret på vilkårene. For at sikre den samme lille risiko for brud på sikkerheden, kræves der nu mere sikkerhed til en større omkostning, da det nu kræver mængden C af sikkerhed for at have den samme lave risiko for brud på sikkerheden. Alternativt kan virksomheden benytte samme mængde sikkerhed og dermed ikke øge sin omkostning hertil, men det vil medføre en øget risiko for brud på sikkerheden, idet der så sker en ændring på y-aksen fra punktet A til punktet B.

Omkostningen for virksomhederne er altså blevet større, såfremt de vil sikre optimal sikkerhed. Om virksomhederne vil bruge øgede omkostninger på sikkerhed, afhænger som nævnt overordnet af, om de ser deres investering i dette som værende mindre end udgiften ved ikke at øge sikkerheden. Udgiften kan f.eks. være bøder for brud på sikkerheden, betaling af løsesum for data og brud på tilliden til virksomheden med dalende omsætning til følge.

Som det fremgår af ovenstående, er det generelt dyrt at indføre databeskyttelse, og at omkostningerne til dette er stigende. Der skal i det følgende ses nærmere på de konkrete omkostninger ved at indføre princippet om databeskyttelse gennem design.

4.2.3.3.2. Omkostninger til overholdelse af databeskyttelse gennem design

Det er indtil videre slået fast, at selv om der er lagt op til store bøder i forordningen, så er der både tvivl om, om bøderne overhoved vil blive så store i Danmark og om Datatilsynets grad af tilsyn. Hvis danske virksomheder både forventer lavere bøder, og at der er en lav risiko for at blive opdaget i at overtræde lovgivningen, er det ikke så mærkeligt, at flere danske virksomheder indtil videre ikke har forberedt sig til forordningens krav, specielt hvis indførelse af bl.a. databeskyttelse gennem design vurderes at være meget omkostningsfuldt. Dette skal derfor analyseres nærmere.

Udfordringen for mange virksomheder er, at de ikke selv ejer deres it-systemer, men blot leaser/lejer dem af store it-virksomheder. De fleste virksomheder, har dermed hverken penge eller kompetencer til at udvikle egne it-systemer, der overholder kravet om databeskyttelse gennem design.

Den enkelte virksomhed har derfor svært ved at påvirke, hvordan dens system skal udvikles/ændres. Som det fremgår af den juridiske analyse, er definitionen på databeskyttelse gennem design umiddelbart meget uklar og kan tolkes på flere måder. Kravet til indholdet er i hvert fald ikke klart for virksomhederne på nuværende tidspunkt. It-leverandørerne, der udvikler systemerne, vil umiddelbart af egen vilje forsøge at få deres systemer til at leve op til forordningen, men det må forventes, at de vil antage den mest lempelige fortolkning af databeskyttelse gennem design, så de skal bruge færrest mulige omkostninger på ændring/udvikling af deres systemer.

Udfordringen her er ligeledes, at it-leverandørerne ikke vil kunne blive mødt med bøder for manglende overholdelse, så de har intet incitament til at bruge flere omkostninger end hvad det kræver, for at fastholde kunderne. Og kunderne har svært ved at overskue, hvad der kræves til it-systemerne, da de hverken har kendskab eller indblik i det bagvedliggende i deres it-system, og heller ikke kender det nøjagtige indhold af databeskyttelse gennem design. Brugere af it-systemerne, vil antageligt anlægge en strengere fortolkning af begrebet end it-leverandørerne, da det er brugerne, der risikerer bøder ved manglende overholdelse af forordningen.

Brugere kan derfor vælge blot at anvende systemet, som leveret af it-leverandøren, eller de kan vælge at betale denne for udvikling af systemet, så det overholder brugerens egen definition af databeskyttelse gennem design. Udfordringen herved er, at it-leverandøren så kan give denne udvikling til alle sine

brugere og dermed har virksomheden betalt for udvikling af systemet, som kommer alle til gavn. Virksomheden kan så vælge at lave en aftale om, at udviklingen kun er til virksomheden selv, og ikke må gives til andre brugere, men dette vil it-virksomheden typisk tage sig meget dyrt betalt for. Nogle af de udfordringer der udspringer af ovennævnte, kan tydeliggøres ved principal-agent-teorien samt Coase teoremet.

4.2.3.3.3. Principal-agent-teorien

Teorien beskriver de problemer, der opstår ved kontrahering/samarbejde mellem to parter. På den ene side principalen og på den anden side agenten. Principalen er den part, der vil have agenten til at udføre en opgave. Efter indgåelse af en kontrakt udarbejdet af principalen, vælger agenten sit ydelses eller investeringsniveau.¹¹³

En typisk principal-agent situation indeholder følgende: En mulighed for et overskud, en interessekonflikt og asymmetrisk information.

Muligheden for overskud findes, når principalen er villig til at betale agenten mere end dennes omkostning ved udførelsen. Interessekonflikten kan f.eks. være, at principalen ønsker et høj kvalitetsprodukt, men prisen er aftalt på forhånd, så agenten vil få mere ud af at levere dårligere kvalitet, da kvalitet har en omkostning. Og jo lavere omkostning for agenten, jo mere overskud. Asymmetrisk information består i, at agenten besidder en viden, som ikke er tilgængelig for principalen.¹¹⁴ Adfærdssantagelserne er de samme som i den økonomiske analyse, hvor aktørerne er opportunistiske og begrænset rationelle.¹¹⁵

I situationen med en it-leverandør og en bruger af it-udstyret, kan der være et ønske fra brugeren om udvikling af systemet. I den situation vil virksomheden, der ønsker at få udviklet på systemet, være principal og it-leverandøren agenten. For at it-leverandøren skal være villig til udvikle sit system, skal principalen ønske at betale mere for denne udvikling, end det koster agenten at udvikle. Dette giver god

¹¹³ Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education, s. 90

¹¹⁴ Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education, s. 91

¹¹⁵ Den oprindelige PA-teori byggede dog på fuldstændig rationalitet og muligheden for fuldstændige kontrakter, jf. Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education, s. 93

mening, da it-leverandøren ikke vil udvikle, hvis de ikke kan tjene penge herpå. Interessekonflikten er også til stede, da principalen vil ønske at få udviklet et høj kvalitetssystem, men agenten har interesse i at bruge så få omkostninger som muligt på udviklingen og dermed opnå det højeste mulige overskud. Den asymmetriske information består i, at agenten har meget større viden om sit system og kender til den bagvedliggende programmering. Ligeledes har denne en langt større viden om it-systemer generelt og ved, hvad der kræves for udvikling og er dermed principalen langt overlegen. Derudover er det kun agenten, der kender til den bagvedliggende programmering. Principalen kan kun se det umiddelbare og har derfor svært ved at teste og validere systemet.

Der er inden for modellen to forskellige former for asymmetrisk information. Der er "hidden action" og "hidden characteristic", som beskriver problemet og tilhørende "moral hazard" og "adverse selection" som beskriver agentens adfærd. Ved "hidden action" har principalen og agenten symmetrisk information under forhandlingen, men efterfølgende er det kun agenten, der har information om f.eks. ydelsesniveau. Principalen kan kun observere resultatet. Der opstår altså asymmetrisk information efter indgåelsen af kontrakten og der er dermed tale om en ex-post asymmetrisk information.¹¹⁶ Ved "hidden characteristic" er der asymmetrisk information fra starten og der er dermed tale om en ex-ante asymmetrisk information.¹¹⁷

I den opstillede situation vil der være tale om et "hidden characteristic" problem. Agenten vil besidde en stor mængde information, som hverken er tilgængelig eller forståelig for principalen, da denne typisk ikke vil have viden om og dermed forståelse for it-programmering. Problemet udmønter sig altså ved, at principalen indgår en aftale med en agent om at levere it-systemer, som principalen kræver, skal overholde hele forordningens krav, men i og med at principalen ikke har de nødvendige tekniske kompetencer, risikerer han at indgå et samarbejde med en it-leverandør, hvor løsningen i virkeligheden ikke opfylder princippet om databeskyttelse gennem design.

Ud fra ovenstående må det konkluderes, at virksomheder under alle omstændigheder vil have store omkostninger ved at implementere databeskyttelse gennem design i alle deres systemer. De må vælge

¹¹⁶ Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education, s. 95

¹¹⁷ Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education, s. 96

mellem enten at udvikle dem selv, eller købe dem fra en ekstern it-leverandør. De fleste små og mellemstore virksomheder vil ikke have muligheder for at udvikle dem selv, og vil derfor blive nødt til at købe dem udefra. Dette kan skabe ovenstående principal/agent problemer, hvilket også øger de samlede omkostninger ved implementeringen.

4.2.3.3.4. Coase-teoremet

Ovenstående forhandling mellem it-leverandøren på den ene side, og virksomheden der ønsker at få udviklet it-udstyr, på den anden side, kan også belyses med udgangspunkt i Coase-teoremet. Det fremgår af den stærke version af Coase-teoremet, at hvis ejendomsrettigheder er veldefinerede og transaktionsomkostningerne er nul, så vil parterne, i enhver forhandlingssituation opnå et Pareto-optimalt resultat.¹¹⁸ Selve teoremet kommer i forskellige udgaver, da ovenstående ikke er direkte udarbejdet af Coase, men en udledning af hans analyser.¹¹⁹ Betingelsen om, at transaktionsomkostningerne skal være lig nul, er blevet kritiseret, fordi at selvom alle juridiske hindringer for at indgå aftaler fjernes, så vil der altid opstå transaktionsomkostninger.¹²⁰ Denne betingelse bliver også i litteraturen justeret lidt, således at den passer bedre til den virkelige verden. Betingelsen er f.eks. formuleret som et krav om *efficient bargaining*, hvilket betyder, at transaktionsomkostningerne er så lave, at forhandling kan foregå uden problemer.¹²¹

Coase-teoremet opstiller dermed tre betingelser for, at der kan opnås Pareto-optimale resultater. Der skal være tale om en forhandlingssituation, ejendomsrettighederne skal være veldefinerede og transaktionsomkostningerne skal være lig nul (eller meget lave).

Der er ingen tvivl om, at vi er i en forhandlingssituation i ovenstående eksempel. Men som det fremgår af de nævnte principal-agent-problemer, så vil der altid opstå transaktionsomkostninger mellem it-udvikleren og virksomheden. Der er som sagt en interessekonflikt og asymmetrisk information, hvilket fører til, at forhandlingen ikke bliver fri for transaktionsomkostninger. Spørgsmålet er om de høje

¹¹⁸ Eide, Erling & Stavang, Endre. 2014, Rettsøkonomi. Cappelen Akademisk Forlag, s.137

¹¹⁹ Eide, Erling & Stavang, Endre. 2014, Rettsøkonomi. Cappelen Akademisk Forlag, s.137

¹²⁰ Eide, Erling & Stavang, Endre. 2014, Rettsøkonomi. Cappelen Akademisk Forlag, s.138

¹²¹ Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education, s. 76

transaktionsomkostninger netop opstår, fordi at den tredje – og i dette tilfælde den mest interessante betingelse – ikke er opfyldt. Den kræver, at rettighederne skal være veldefinerede.

Ejendomsrettigheder opdeles normalt i afgørelses- og indtægtsrettigheder, hvor afgørelsesrettigheder omhandler brugen af et aktiv, og indtægtsrettigheder omhandler rettigheden til at modtage overskud, og betale eventuelle omkostninger vedrørende aktivet.¹²² Normalt er der derfor kun tvivl om rettighederne, når der er tale om forurening, luft, jord og lignende. Coase-teoremet blev dog udarbejdet, inden de problemer som den teknologiske udvikling har medført, var en realitet, herunder spørgsmålet om persondatarettigheder. Spørgsmålet er derfor, om netop denne betingelse ikke er ekstra relevant, når der skal ses på kravet om databaseskyttelse gennem design. Som det fremgår af den juridiske analyse, er det netop et uklart krav, og virksomhederne har derfor svært ved at vide, hvad de har ret til, hvilke systemer de kan anvende, og hvilket system ikke opfylder betingelserne i bestemmelsen.

Ved at have en bestemmelse i forordningen, hvor rettighederne ikke kan betragtes som veldefinerede overfor virksomhederne, øger usikkerheden på markedet, forstærker principal-agent-problemerne, samt transaktionsomkostningerne i forhandlingen mellem it-leverandører og virksomheder. Virksomhederne står dermed i en forhandlingssituation, hvor rettighederne ikke er veldefinerede, og transaktionsomkostningerne er høje. Dette medfører ifølge Coase-teoremet, at resultatet ikke bliver Pareto-optimalt.

Det kan dermed både ud fra principal-agent-teorien og med inddragelse af Coase-teoremet argumenteres for, at overholdelse af forordningens krav om databaseskyttelse gennem design indebærer væsentlige omkostninger for virksomhederne.

Hvor store omkostningerne er, afhænger dog både af, hvilken slags virksomhed der rammes, og af hvordan begrebet databaseskyttelse gennem design bliver fortolket. Større virksomheder har selvsagt mindre vanskeligheder med at implementere reglerne, mens mindre virksomheder får større

¹²² Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education, s. 74

udfordringer. Og desto mere begrebet omfatter, desto flere omkostninger vil det have for virksomhederne.

4.2.4. Konklusion på efficiens i forhold til markedsfejlen

Sammenfattende er det konstateret, at EU med kravet om databeskyttelse gennem design har sat et databeskyttelsesniveau, der klart overgår det niveau, som markedet ellers ville ende på. Det er dog usikkert, om dette punkt svarer til, hvad rationelle forbrugere med fuldstændig information ville efterspørge.

Det er derudover konstateret, at overholdelse af kravet om databeskyttelse gennem design indebærer høje omkostninger for virksomhederne, samtidig med at der er usikkerhed både omkring bødestørrelse og den forventede håndhævelse. Dette medfører, at kravet om databeskyttelse gennem design mister noget af den afskrækkende effekt, og virksomhederne har derved mindre incitament til at overholde bestemmelsen. På den måde er det tvivlsomt, om virksomhederne vil tilpasse sig det omfattende databeskyttelsesniveau, som lovgiver har sat, uanset om dette svarer til det niveau af databeskyttelse, som rationelle og fuldt oplyste forbrugere ville have efterspurgt.

Bestemmelsen vurderes dog til delvis at rette op på markedsfejlen, da databeskyttelsesniveauet under alle omstændigheder stiger, samtidigt med at forbrugerne som følge af forordningen bliver mere oplyste om værdien af deres data.

Spørgsmålet er herudover, om det meget strikse krav om databeskyttelse gennem design overhoved er efficient i forhold til formålet med lovgivningen, og om det måske strider imod andre overordnede formål, som EU arbejder for, herunder formålet med det indre marked.

4.3. Bestemmelsens efficiens i forhold til forordningens og EU's formål

Som det fremgår af den juridiske analyse, så bygger persondataretten overordnet på privatlivs- og personlighedshensyn, hvor det er individet, der er i fokus. Formålet med selve Persondataforordningen er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder. Det er nemt at argumentere for, at indførelsen af databeskyttelse gennem design går langt i denne retning, og at det er

i overensstemmelse med forordningens formål. Princippet har netop fokus på individers rettigheder, og at de dataansvarlige skal designe alle deres it-systemer således, at disse rettigheder bliver beskyttet.

Som det fremgik af Google-Spain dommen, så går EU-Domstolen langt i dette henseende, og er ikke bange for at tilsidesætte eventuelle kommercielle interesser. Spørgsmålet er dog, hvor meget skal til, før de kommercielle interesser bliver så store eller påvirkede, at der skal lægges vægt herpå. I sidste ende kan det også gå ud over forbrugerne, hvis lovgivningen har for store negative konsekvenser for de dataansvarlige, f.eks. hvis det påvirker den økonomiske vækst i samfundet.

Det er i den forbindelse relevant at inddrage EU's overordnede mål. Det Europæiske Fællesskab (EF) blev oprettet tilbage i 1958, oprindeligt som et økonomisk fællesskab. I perioden fra EF's oprettelse og frem til Maastricht-Traktatens ikrafttræden og Unionens oprettelse i 1993, var det indre marked det helt dominerende projekt i EF/EU. Projektet er stadigvæk meget vigtigt, men står ikke længere alene.¹²³

Unionens overordnede mål fremgår i dag af TEU art. 3. Her er stk. 3 særlig interessant fra et virksomhedssynspunkt, da målet med det indre marked klarlægges. Det fremgår her, at unionen opretter et indre marked, og at den arbejder for en bæredygtig udvikling i Europa, der er baseret på en afbalanceret økonomisk vækst og prisstabilitet, en social markedsøkonomi med høj konkurrenceevne, hvor der tilstræbes fuld beskæftigelse og sociale fremskridt, og et højt niveau for beskyttelse og forbedring af miljøkvaliteten. Den skal derudover bl.a. fremme videnskabelige og teknologiske fremskridt.

Det overordnede formål med det indre marked er dermed bl.a. at skabe økonomisk vækst, en høj konkurrenceevne, samt at fremme videnskabelige og teknologiske fremskridt. Det skal derfor undersøges nærmere, om kravet om databeskyttelse gennem design påvirker virksomhedernes muligheder for at skabe økonomisk vækst i samfundet, og om kravet på den måde hindrer nogle af de overordnede formål med det indre marked.

¹²³ Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group, s. 39

4.3.1. Økonomisk vækst i samfundet

For at undersøge om kravet om databeskyttelse gennem design påvirker virksomhedernes muligheder for at skabe økonomisk vækst i samfundet, skal des nærmere på, hvad økonomisk vækst er. Økonomisk vækst er et upræcist begreb, i og med at det kan opgøres i flere forskellige økonomiske størrelser.

Normalt defineres økonomisk vækst som en forøgelse af samfundets produktion og indkomst, hvilket som oftest måles i den årlige ændring i bruttonationalproduktet. På kort sigt vil konjunkturudsving påvirke den økonomiske vækst både den ene og den anden vej, men når der tales om økonomisk vækst på længere sigt, vil den være påvirket af forskellige økonomiske faktorer, f.eks. ændringer i produktionsteknologi, arbejdskraft, kapital og råvareforbrug. Dette er faktorer, som virksomhederne på markedet har en stor indflydelse på, og det bliver dermed vigtigt, at de både har mulighed og incitamenter til at fremme den økonomiske vækst i samfundet.

Det skal i det følgende undersøges, hvordan økonomisk vækst opstår, og hvilken sammenhæng der er mellem økonomisk vækst og innovation. Indenfor økonomisk teori er Joseph Schumpeter faderen der søgte at beskrive innovation og iværksætter i starten af 1900-tallet, og hans teorier er derfor meget relevante at inddrage i analysen.

4.3.2. Schumpeters teori om innovatøren

Joseph A. Schumpeter har analyseret samspeilet mellem innovatøren og det økonomiske system. Schumpeters teori bygger videre på Léon Walras teori om innovatøren. Walras teori er dog bygget på den neoklassiske teori og dermed ud fra tankegangen om, at hvis der sker en ændring i ligevægten skyldes det udefrakommende påvirkninger, såsom smagsændringer og ny teknologi. I Walras teori er det økonomiske system derfor passivt og det er denne passivitet, som Schumpeter ikke er enig i.¹²⁴

Det er ifølge Schumpeter ikke en ekstern faktor, der påvirker det økonomiske system og skaber en ændring i ligevægten, men en ændring inde i systemet. Det er Schumpeters innovatør, der skaber denne ændring i ligevægten og det er dermed en ændring, der sker indefra og ikke via en ekstern faktor.

¹²⁴ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 30 ff.

Forskellen på Walras og Schumpeters teori er, at i Walras teori er der i ligevægten indført alle innovationer og alle økonomiske aktører er tilfredse med tilstanden. Det er derfor, der ikke sker en ændring indefra, men kræves en ekstern faktor til påvirkning af det økonomiske system.¹²⁵

Schumpeter gjorde op med den neoklassiske tankegang, om at alle aktører er rationelle og fuldkommen informerede, ligesom Schumpeter antager, at ikke alle aktører tænker og handler ens. De fleste aktører vil være tilfredse med tingenes tilstand, som vil være præget af rutine for at opnå ligevægten. Enkelte vil dog ikke kunne tilpasse sig den stationære økonomi med faste rutiner og de vil have behov for at gennemføre fornyelser. Og det er disse mennesker, der er innovatører i Schumpeters teori. Det er altså personer, der bryder med de faste rutiner og skaber fornyelser.¹²⁶

Ligevægten vil altså blive brudt ved at en innovatør skaber f.eks. et nyt produkt. I Walras teori vil en ændring i ligevægten hurtig blive udlignet, hvorimod Schumpeter arbejder med en meget mere langsom og markedsstilpasning, som let kan tage et årti, da de andre aktører i markedet er rutinepræget og kun langsomt ændre deres rutiner. Det er grundet denne langsomme tilpasning, at innovatøren har mulighed for at opnå en profit, som giver mulighed for at tilbagebetale lånet, som han har taget for at kunne innovere. Innovatøren er nemlig nødt til at låne penge til sin innovation, idet der inden er ligevægt i markedet og dermed ikke er overskud til finansieringen af innovationen.¹²⁷ Denne antagelse om at pengene til innovation skal lånes, ændres dog senere af Schumpeter, så det f.eks. er muligt for innovatøren at udvikle ud fra tidligere opnåede midler ved innovation.¹²⁸ Efter innovationen er udført vil de andre aktører enten gå konkurs eller tilpasse sig og herefter vil en ny ligevægt opstå.

Innovationen er altså årsagen til konjunkturer i økonomien. I starten vil der ske en opsving i økonomien bl.a. grundet de penge, der bliver skudt ind i systemet i form af innovatørens lån. Efter afslutningen på innovationen bliver disse penge tilbagebetalt og der er færre penge i systemet, hvilket starter en

¹²⁵ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 34 ff.

¹²⁶ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 37 ff.

¹²⁷ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 38 ff.

¹²⁸ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 102+107

tilbagegang i økonomien. Påvirkningen på makroøkonomisk plan er mulig, da innovation sker i sværme af mange innovatører og der dermed er stor påvirkning af det økonomiske system.¹²⁹

Schumpeter så derfor konjunkturer som en nødvendighed i det økonomiske system, idet disse var grundet i innovation. Opture som følge af udviklingen af nye tiltag og nedturen som følge af afslutningen herpå. Nedturen og den nye tilpasning af økonomien til et nyt ligevægtspunkt er nødvendig for muliggørelse af ny innovation, da innovatøren bedst kan innovere, når der er ligevægt, da det er her, det er lettest at få øje på muligheder og beregne omkostninger og mulige indtjeninger.¹³⁰

I en situation med tilbagegang i økonomien kan der let opstå ønsket om at forsøge at undgå dette ved forskellige økonomiske og politiske tiltag. Schumpeter mener dog ikke, at dette er frugtbart, da nedgangen er nødvendig. Ved indblanding opnås der fordele på kort sigt, men ikke på lang sigt, da det undergraver innovationsprojekterne og viser en negativ indstilling til innovation. Dog anerkender Schumpeter, at der kan være situationer, hvor det er nødvendigt at påvirke økonomien ved brug af økonomiske/politiske tiltag.¹³¹

Ifølge Schumpeter er der dermed en direkte sammenhæng mellem virksomhedernes innovation og vækst i samfundet. Konjunkturerne i økonomien er direkte begrundet i virksomhedernes innovation. Hvis virksomhederne ikke har mulighed for at innovere, vil der simpelthen ikke blive skabt vækst. Spørgsmålet er herefter om Persondataforordningens art. 25, stk. 1 om databeskyttelse gennem design hindrer virksomhedernes innovationsmuligheder og kan være en medvirkende årsag til at økonomien stagnerer.

4.3.3. Big data er fremtiden

På engelsk bruges tre V-ord til at beskrive big data, og de er volume, velocity og variety. Det er altså tale om flere data, flere datakilder og højere hastighed. Big data beskrives som "high-volume, high-velocity and/or high-variety" informationsaktiver, der kræver omkostningseffektive og innovative

¹²⁹ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 78 ff.

¹³⁰ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 81 ff.

¹³¹ Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag, s. 91 ff.

former for informationsbehandling, der muliggør en øget indsigt, beslutningstagning og procesautomatisering.

Det er flere steder fra påstået, at big data er fremtiden. I rapporten "Big Data: Fremtidens digitale råstof" udarbejdet af Mandag Morgen i samarbejde med Google, er det også konklusionen.¹³² Som det skrives i rapporten bliver "(big data)...krumtappen i informationsalderens næste fase, og vil skabe vækst og innovation i erhvervslivet og løse nogle af samfundets største udfordringer.". Data er ikke længere blot en nødvendig del af en handelstransaktion, det er selve handelsvaren.

USAs tidligere præsident, Barack Obama, udsendte i 2013 en ordre til hele det offentlige apparat om, at al offentlige data skulle gøres tilgængelig, så private kunne gøre brug heraf. Obamas beslutning var med den viden, at al den data har en stor værdi og måske kunne åbne op for nye iværksættere, der kunne se muligheder heri. Barack Obama henviste til den vækst, der blev skabt i forbindelse med Ronald Reagans åbning af det private adgang til GPS-data, som i dag bruges af mange og som dermed har skabt udvikling og nye muligheder.

Påstanden er, at big data vil øge produktiviteten, skabe nye jobs og fungere som en katalysator for vækst. Hvis der ses på big data som en innovation er påstanden i tråd med Schumpeters analyse af, hvordan innovation påvirker økonomien. Produktiviteten stiger som følge af, at innovatøren presser de andre aktører til at tilpasse sig. Ved innovationen skabes der nye jobs, idet innovatøren har brug for arbejdskraft. Væksten vil bl.a. ske som følge af nye muligheder, der opstår som følge af den nye innovation og væksten vil skabe en optur i økonomien, som følger i kølvandet på en innovation.

Ifølge professor ved MIT Sloan School of Management, Andrew McAfee vil virksomheder, der benytter sig af big data have en højere omsætning, end virksomheder der ikke benytter sig heraf. Studier viser, at indtjeningen faktisk vil være 5-6 % højere. Så det er helt klart et parameter, der er vigtigt i en verden med stor global konkurrence. Den øgede indtjening er på linje med Schumpeters teori, da innovationen netop medfører monopollignende profit. Dette er dog i Schumpeters teori

¹³² Rostgaard, Anders. 2013. *Big Data Fremtidens Digitale Råstof*. Rapport udarbejdet af Mandag Morgen i samarbejde med Google. Afsnit 4.3.3. om Big Data samt underafsnit bygger på viden fra denne rapport s. 60-86

begrænset til en periode, da de andre aktører på markedet vil følge med og en ny ligevægt på markedet vil opstå og dermed er det ikke længere muligt for innovatøren at opnå større profit.

Der er dermed meget, der tyder på, at big data er et område, som der skal satses på fra virksomheders side, og at dette kan skabe store muligheder for innovation. Det har derfor betydning, at lovgivning ikke sætter hindringer i vejen, således at mulighederne med big data ikke kan udnyttes.

4.3.3.1. Big data i Danmark

I en undersøgelse foretaget af Vanson Bourne viste det sig, at vi i Danmark halter langt bagefter, når det handler om big data og udnyttelsen heraf. I undersøgelsen var der 60 % af it-virksomhederne i Danmark og Sverige, der ikke havde undersøgt, om brug af big data kunne gavne forretningen. I resten af Europa var dette tal kun 35 %. Og i en global verden med konkurrence på tværs af landegrænserne, er det et stort problem. De danske virksomheder risikerer simpelthen at blive udkonkurreret, da beslutninger bedre kan træffes på baggrund af kvalificeret data i form af big data end alternativet som er mavefornemmelse og intuition. Ifølge Schumpeter er der stor risiko for, at virksomheder der halter bagud, vil blive udkonkurreret, hvis de ikke kan følge med den nye udvikling. Det er faktisk et vilkår, at nogle virksomheder vil gå konkurs, da der ikke længere er brug for dem. Det er dermed ikke ligegyldigt, hvem der er med på udviklingen og hvem der er først. Især da dem der er først, som nævnt har muligheden for monopollignende profit.

4.3.3.2. Forsigtighed med deling af persondata

En af årsagerne til, at vi i Danmark er bagud, kan skyldes, at der fortsat er en stor forsigtighed med deling af data. Herunder især persondata. Jørgen Elgaard Larsen fra IT-Politisk Forening har udtalt, at det er en illusion, at man kan dele data og tro, at det er anonymiseret. Han ser derfor, at der er stor risiko for, at deling af data kan blive misbrugt og er derfor negativt indstillet på deling af data og brugen heraf. Hvis denne holdning afspejler, hvordan danske virksomheder ser på deling af data, er det ikke mærkeligt, at Danmark halter bagefter, når det kommer til at udnytte mulighederne ved big data.

Anders Sparre fra Dansk IT er dog positivt indstillet og han mener, at vi skal være mere villige til at se muligheder og ikke være så nervøse, for så mister vi chancen for at få gang i noget nyt.

Digitaliseringsstyrelsen har kørt en kampagne for åbning af offentlige data¹³³, men det omhandler kun data, der ikke er persondata og som derfor ikke er omfattet af Persondataloven. Det viser, at selv med den nuværende lovgivning, er vi i Danmark bange for, at vi skal komme i konflikt med lovgivningen. Der er en berøringsangst, når det kommer til persondata. Spørgsmålet er derefter, hvordan Persondataforordningen og herunder kravet om databeskyttelse gennem design påvirker denne tilbageholdende tilgang til persondata i Danmark.

4.3.4. Innovationshæmmende forordning?

Der kan argumenteres for, at denne berøringsangst overfor persondata kun er blevet forstærket i forbindelse med den nye forordning. Virksomhederne er især blevet skræmt af de store bøder, som forordningen giver mulighed for. Derudover er der meget misinformation og dermed generelt meget forvirring om reglerne i den nye forordning. Ifølge Schumpeter er en af kravene til at innovation opstår, at der er ligevægt i markedet, så innovatøren har mulighed for at beregne mulig indtjening og omkostninger. Usikkerhed er med andre ord ikke positivt for innovation og det er netop usikkerhed, der er opstået i forbindelse med forordningen.

Som det fremgår af rapporten, så plæderer Viktor Mayer-Schönberger, Professor fra Oxford University, for et helt nyt mindset, når det omhandler persondata. Han mener, at fokus skal være på høj og etisk korrekt dataansvarlighed i virksomhederne i stedet for beskyttelse af individet, som er fokus i forordningen. Ifølge Mayer-Schönberger vil det gavne alle, både forbrugere og virksomheder, da virksomhederne vil have bredere mulighed for brug af data til gode formål, som er i forbrugers interesse. Han påpeger udfordringen ved, at virksomheder ved ændring af formål for behandling af persondata, jf. lovgivningen, skal indhente nyt samtykke fra forbrugerne. Og dette er både besværligt for virksomhederne og for forbrugerne og kan derfor medføre, at virksomhederne ikke får udnyttet potentialet i nye muligheder og forbrugerne heller ikke får glæde heraf.

Mayer-Schönberger udtaler ikke direkte, at forordningen kan være innovationshæmmende, men det kan godt sammenfattes ud fra hans udtalelser. Bl.a. ved at han kommer med et eksempel på, hvordan en

¹³³ Digitaliseringsstyrelsens Open government-handlingsplan 2013-2016. <https://digst.dk/strategier/internationalt-samarbejde/open-government/open-government-handlingsplan-2013-2016/>

virksomhed der sælger anti-tyveriudstyr, bruger førerens siddeposition til at afgøre, om det er rette ejer, der sidder i bilen, senere kan videreudvikle på den indsamlede data til f.eks. at vurdere førerens opmærksomhedsniveau og bruge dette til at sende advarsler. Det vil kræve et nyt samtykke fra føreren at bruge den indsamlede data til at vurdere førerens opmærksomhedsniveau og sende advarsler, da der er tale om et nyt formål med den indsamlede data. Et nyt samtykke kan være svært for virksomheden at indhente og det kan være, at forbrugeren finder det for besværligt at give og dermed får ingen glæde af den nyudviklede funktion. Det kan også være, at den måske slet ikke udvikles, da virksomheden ikke innoverer, fordi den ved, at det er for besværligt at få gevinst af innovationen. På den måde bliver forordningen innovationshæmmende.

Af rapporten fremgår yderligere, på baggrund af de eksperter Mandag Morgen har talt med, fem punkter som er vigtige områder til revision, hvis Danmark og virksomhederne skal få del i gevinsterne fra mulighederne ved brug af big data. Her nævnes også lovgivning som en mulig innovationshæmmende faktor.

Det første punkt er nytænkning af rettighedslove. Essensen af big data omhandler værdiskabelse ved deling, kopiering og udveksling af data. En række undersøgelser fra andre lande har ifølge rapporten vist, at der er lovgivning i form af bl.a. copyright regler, der blokerer for muligheden for brug af big data og dermed for vækst. Lovene fungerer altså som en innovationshæmmende faktor.

Det femte punkt omhandler netop Persondataforordningen. Som det fremgår af den juridiske analyse, er målet med forordningen at sikre personers data. Og som rapporten fastslår, er der lagt op til en langt striksere beskyttelse end tidligere og det kan være et problem. Problemet opstår som følge af, at reglerne i f.eks. USA er langt lempeligere og da vi lever i en globaliseret verden, skal virksomheder i EU også konkurrere med virksomheder uden for EU. Det kan skabe en situation, hvor det bliver svært for virksomhederne i EU at konkurrere med virksomhederne uden for EU. Dog er dette problem måske delvist løst ved, at alle virksomheder der opererer inden for EU, er underlagt forordningen, ligegyldigt hvor de hører hjemme.

Der er dermed flere, der argumenterer for, at forordningen generelt sætter hindringer i vejen for virksomheders innovationsmuligheder, og dermed også for vækst i samfundet. Men det er ikke alle, der deler denne opfattelse.

I en artikel¹³⁴ fra IT-Universitetet i Danmark udtaler lektor Thomas Hildebrandt fra IT-universitetet, at virksomheder ikke skal se forordningen som pisk, men som en mulighed for at få styr på arbejdsgangene i virksomheden og komme i gang med at bruge virksomhedens data til eventuelle nye indtjeningsmuligheder, som kan opstå i forbindelse med, at man får styr på sin data. Der kan også være besparelser i gennemgangen af processer, idet virksomheden måske identificere unyttige steps i arbejdsgangen. Hildebrandt mener derfor ikke, at der er nogen grund til at se på forordningen som noget negativt. Det er bare at komme i gang. Og som han nævner, er der ingen grund til at vente med at implementere reglerne i virksomheden, heller ikke selvom forordningen indeholder, hvad han kalder en gummiparagraf, hvormed han henviser til, at virksomheden kan se på risici holdt op i mod omkostninger, når de skal vurdere, hvor langt de skal gå for overholdelse. For som Hildebrandt udtaler, vil det på sigt blive billigere og billigere at overholde reglerne, i takt med at der kommer it-systemer, som kan hjælpe hermed. På sigt vil gummiparagraffen derfor ikke have nogen betydning, og virksomheden vil ikke kunne slippe udenom. Hildebrandt ser dermed forordningen som en mulighed for, at virksomheder får styr på deres datapolitikker, og forordningen generelt kan blive en innovationsskabende faktor.

4.3.5. Innovation i forbindelse med databeskyttelse gennem design

Som det fremgår af ovenstående, er der blandede meninger om forordningen generelt er positiv eller negativ for virksomhedernes innovationsmuligheder. På den ene side siger Viktor Mayer-Schönberger, at forordningen overordnet er bygget på et small data-mindset, og dermed sætter hindringer i vejen for virksomheder, der ser muligheder i en bredere anvendelse af det indsamlede data. På den anden side siger Thomas Hildebrandt, at forordningen netop sætter virksomhederne i gang med at få styr på deres datapolitikker, og at dette vil skabe forretningsmuligheder. Der er dog intet til hinder for, at begge parter kan have ret, i og med at forordningen er på 99 artikler, og der sagtens både kan være innovationshæmmende og innovationsskabende virkninger af den. Derfor bliver det nødvendigt at se på den konkrete bestemmelse.

¹³⁴ Arildsen, Vibeke. 11. september 2017. *ITU-forsker: Brug persondataforordningen til at styrke forretningen*. Artikel udgivet på ITU i Københavns hjemmeside. Direkte link: <https://www.itu.dk/om-itu/presse/nyheder/2017/itu-forsker-brug-persondataforordningen-til-at-styrke-forretningen>

Som det også fremgår af den juridiske analyse, så ser Ann Cavoukian netop princippet om databeskyttelse gennem design som noget, der kræver innovation fra virksomhederne, og hun påstår, at det er en myte, at privatliv kvæler innovationen. Dette er dermed i overensstemmelse med, hvordan Thomas Hildebrandt ser på, hvordan forordningen kan skabe muligheder. Virksomhederne tvinges til at tænke innovativt, for at overholde princippet.

Men dette er derimod ikke i overensstemmelse med, hvordan innovation opstår i forhold til Schumpeters teori om innovatøren. Her er innovation for det første ikke noget, som bliver pålagt virksomhederne udefra. Som nævnt siger Schumpeter, at innovation ikke er en ekstern faktor, der påvirker det økonomiske system og skaber en ændring i ligevægten, men en ændring inde i systemet. Det er altså personer, der bryder med de faste rutiner og selv skaber fornyelser. Det er dermed ikke en ekstern faktor, i form af lovgivning, der tvinger alle aktører til at tænke innovativt, det er derimod en enkelt aktør, der bryder, og på den måde opnår monopolprofit i en periode, indtil markedet har tilpasset sig.

Der kan for det andet argumenteres for, at princippet netop kan afholde virksomheder fra at innovere på andre områder, som f.eks. big data. Innovation opstår i udgangspunktet kun, hvis virksomheden ser forretningsmuligheder ved at innovere.

Som det fremgår af den økonomiske analyse, så gør den lave efterspørgsel efter databeskyttelse og den høje værdi af persondata, at virksomhederne ikke af egen drift vil indføre princippet. Virksomhederne ser umiddelbart større forretningsmuligheder ved at indsamle og profitere på persondata, end ved at satse på databeskyttelse. Ved at indføre kravet om databeskyttelse gennem design i lovgivningen, bliver virksomhederne som nævnt tvunget til enten at overholde kravet, eller betale den forventede bøde ved at overtræde. Som tidligere illustreret vil overholdelse indeholde væsentlige omkostninger, hvilket gør, at der selvsagt vil være mindre penge til at innovere på andre områder, og som det også fremgår af Schumpeters teori om innovatøren, så har virksomhederne brug for penge til at innovere.

Som det fremgår af den juridiske analyse, skal princippet om databeskyttelse gennem design beskytte individers grundlæggende rettigheder. Dette indebærer at alle it-systemer skal udvikles med fokus på it-sikkerhed og designes således, at alle forordningens krav overholdes allerede i designfasen. Dette kan medføre, at virksomhederne har mindre muligheder for at tænke innovativt i forhold andre potentielle

muligheder for brug af data til gode formål, som kan være i forbrugerens interesse. På den måde kan bestemmelsens formål om at beskytte individers grundlæggende rettigheder være hæmmende for virksomhedernes innovation, hvilket Viktor Mayer-Schönberger også påpeger.

På den måde kan der argumenteres for, at indførelsen af kravet om databeskyttelse gennem design både gør, at der er mindre midler til innovation på andre områder, som f.eks. big data, samtidig med at bestemmelsens fokus på beskyttelse af individet tilbageholder virksomheder fra at tænke innovativt i forhold andre potentielle muligheder for brug af persondata.

Et tredje problem ved at lave krav om innovation eller proaktivitet i lovgivning, hvilket princippet om databeskyttelse gennem design kan ses som et forsøg på, er, at det samtidigt fjerner mulighed for en længerevarende monopolprofit ved innovationen. Som det fremgår af den økonomiske analyse, så har virksomhederne på nuværende tidspunkt ikke incitamenter til at satse på databeskyttelse gennem design. Men dette kan i teorien ændre sig, hvis efterspørgslen efter databeskyttelse i fremtiden vil rykke sig, f.eks. hvis folk bliver mere oplyste om værdien af deres persondata. I så fald vil der være store muligheder for innovation på databeskyttelsesområdet, herunder databeskyttelse gennem design, da virksomhederne vil se forretningsmulighederne i det.

Dette belyses f.eks. gennem Blue Ocean Strategien, udviklet af W. Chan Kim og Renée Mauborgne. I modsætning til Michael Porters konkurrencestrategier, hvor der er fokus på virksomhedens konkurrencefordel, så er strategien her netop at være innovativ og skabe et helt nyt marked. Red Ocean er det eksisterende marked i branchen, hvor konkurrencen er hård, konkurrenterne kender hinandens styrker og alle kender konkurrencebetingelserne. Blue Ocean er derimod et marked, som ikke eksisterer i dag. Efterspørgslen bliver skabt af innovatøren, og der er derfor ingen konkurrence om den. Dette giver gode muligheder for stor og hurtig vækst, og efter Schumpeters teori vil der kunne tjenes monopolprofit i længere tid. Men ved at lave lovgivning, som kræver, at alle skal innovere, mindskes mulighederne for at skabe et helt nyt marked, hvor efterspørgslen bliver skabt. Dette er derimod et krav, som alle alligevel skal opfylde. Det nye Blue Ocean bliver i hvert fald hurtigt rødt igen, og derved er incitamenterne også mindre til at komme med en nytænkende innovation.

Et fjerde problem ved bestemmelsen om databeskyttelse gennem design er, at den ikke skaber klarhed eller tryghed. Som allerede nævnt er et af kravene til, at innovation har gode muligheder for at opstå er,

at der er ligevægt på markedet, så innovatøren har mulighed for at beregne mulig indtjening og omkostninger. Forordningen har generelt medført noget usikkerhed, og art. 25 er bestemt ikke en undtagelse, hvilket fremgår af den juridiske analyse. Denne usikkerhed medfører også øgede omkostninger for de dataansvarlige, hvilket tidligere blev illustreret ved brug af både principal/agent teorien og Coase-teoremet.

Der er dermed meget der taler for, at kravet om databeskyttelse gennem design er innovationshæmmende for virksomhederne, hvilket ifølge Schumpeter har en direkte sammenhæng med den økonomiske vækst. På baggrund af dette kan det konkluderes, at bestemmelsen er hæmmende for nogle af de overordnede formål med det indre marked.

4.4. Konklusion på integreret analyse

Der er lavet en efficiensanalyse af bestemmelsen om databeskyttelse gennem design. Der er for det første undersøgt, om den effektivt retter op på markedsfejlen, der blev introduceret i den økonomiske analyse, hvilket både afhænger af, om lovgiver har sat et efficient databeskyttelsesniveau, og om de dataansvarlige vil indrette sig efter kravet.

Det er konstateret, at kravet om databeskyttelse gennem design og indførelsen af de høje bøder for overtrædelse, påvirker markedets optimale databeskyttelsesniveau. Det kan dog ikke siges, om dette punkt svarer til, hvad rationelle forbrugere med fuldstændig information ville efterspørge. Med indførelsen af kravet om databeskyttelse gennem design er der dog under alle omstændigheder rettet op på den lave efterspørgsel efter databeskyttelse, og derudover har forordningen generelt sat et øget fokus på databeskyttelse, hvilket også er med til at rette op på markedets informationsfejl.

Overordnet vil en dataansvarlig kun overholde kravet, hvis omkostningen til overholdelse er mindre end sandsynligheden for at blive opdaget gange bøden for overtrædelse af bestemmelsen. Det er konstateret, at selv om forordningen introducerer meget høje bøder, så er det meget tvivlsomt, både hvor effektiv håndhævelsen vil være, og om der vil blive udstedt så store bøder, som forordningen lægger op til. Derudover er det påvist, at overholdelse af forordningen har væsentlige omkostninger for virksomhederne. Den høje omkostning ved overholdelse sammenholdt med usikkerheden omkring både bødestørrelse og håndhævelse medfører, at kravet om databeskyttelse gennem design mister noget

af den afskrækkende effekt, og virksomhederne har derved færre incitamenter til at overholde bestemmelsen. På den måde er det tvivlsomt, om virksomhederne vil tilpasse sig det omfattende databeskyttelsesniveau, som lovgiver har sat, uanset om dette viser sig at være det optimale niveau.

Derefter er det undersøgt, om bestemmelsen er efficient i forhold til lovgivningens og EU's overordnede formål. Formålet med selve Persondataforordningen er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, og det er nemt at argumentere for, at indførelsen af databeskyttelse gennem design går langt i denne retning. Det overordnede formål med det indre marked er derimod bl.a. at skabe økonomisk vækst, en høj konkurrenceevne, samt at fremme videnskabelige og teknologiske fremskridt. Det er derfor undersøgt, hvordan økonomisk vækst opstår, og hvilken sammenhæng der er mellem økonomisk vækst og innovation. Der er flere argumenter for og imod om forordningen som helhed, samt art. 25 er innovationsskabende eller ej. Ved at inddrage Joseph Schumpeter grundlæggende teori om innovatøren, er der argumenteret for, at kravet om databeskyttelse gennem design kan have negative konsekvenser for virksomhedernes innovation. Indførelsen af kravet om databeskyttelse gennem design gør både, at der er færre midler til innovation på andre områder, som f.eks. big data, samtidig med at bestemmelsens fokus på beskyttelse af individet tilbageholder virksomheder fra at tænke innovativt i forhold til potentielle muligheder for brug af persondata.

Der er bred enighed om, at big data bliver centralt i informationsalderens næste fase, og at dette vil skabe vækst og innovation i erhvervslivet. Der er også ifølge Joseph Schumpeter en direkte sammenhæng mellem innovation og økonomisk vækst. På baggrund af dette er det konkluderet, at bestemmelsen er hæmmende for nogle af de overordnede formål med det indre marked.

Selv om bestemmelsen må antages delvist at rette op på markedsfejlen, vurderes den derfor ikke til at være efficient i forhold til EU's overordnede formål, da den vil hæmme den økonomiske vækst. På den måde kan formålet med selve bestemmelsen, som er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, gå ud over de selvsamme personers velstand, i og med at den manglende økonomiske vækst i sidste ende også vil ramme dem.

Kapitel 5: Samlet konklusion

Det er i den juridiske analyse forsøgt at klarlægge det materielle indhold af bestemmelsen om databeskyttelse gennem design. Justitsministeriets udlægning har i betænkningen været, at begrebet ikke var nyt og allerede var omfattet af art. 17 i det nuværende direktiv. Det er flere enige i, men mener samtidig, at bestemmelsen nu vil være bredere, da det ikke længere kun vil omfatte sikkerhedsforanstaltninger. På baggrund af analysen kan det konkluderes, at begrebet omhandler mere end sikkerhed – især når det skal tolkes i overensstemmelse med Ann Cavoukians Privacy by Design begreb.

Det er dog ikke muligt at konkludere endeligt på, hvor bredt bestemmelsen vil blive tolket, idet dette endeligt vil blive afklaret af EU-domstolen, som endnu ikke har haft mulighed for at tage stilling til begrebets indhold. EU-domstolen har dog en kendt fortolkningsstil, som i analysen er anvendt på art. 25, stk. 1. Ved at se på bestemmelsens ordlyd og formål er det konkluderet, at bestemmelsen i hvert fald går ud over kun at omfatte sikkerhedsforanstaltninger. Databeskyttelse gennem designs formål er at sikre, at alle databeskyttelsesprincipper og garantier i forordningen skal overholdes, og dette sikres ved at den dataansvarlige designer de passende tekniske og organisatoriske foranstaltninger med dette henblik. Der er dog inddraget rimelighedshensyn, som EU-domstolen også anvender, og på den baggrund set på, at begrebet oprindeligt ikke var lovfæstet, men var et supplerende ikke-juridisk bindende begreb. Ydermere er inddraget EU-rettens- og internettets udviklingstrin. Dette kan medføre, at bestemmelsens indhold ikke bliver så bredt til at starte med, men kan udvikle sig over tid.

Da det således kan konkluderes, at begrebet indeholder mere end blot sikkerhedsforanstaltninger, er det en ændring i forhold til gældende ret. De dataansvarlige skal tænke bredere end blot sikkerhed, når de skal opfylde bestemmelsen. Det kan f.eks. være i form af dataminimering ved brug af drop-down menuer i stedet for fritekstfelter, for at sikre, at der ikke skrives mere information end nødvendigt.

I den økonomiske analyse er der set på, om databeskyttelse gennem design har en økonomisk værdi for virksomhederne, og om de vil implementere princippet af egen drift. Med muligheden for at have en konkurrencefordel, kan det ifølge den økonomiske teori være en fordel at implementere princippet. Dette er vist med Porters konkurrencestrategier og Hotelling model.

Derefter er der set på, hvorfor virksomheder alligevel ikke har incitamenter til at implementere princippet. Forbrugere er ikke bevidste om den høje værdi af deres persondata samt risikoen ved manglende databeskyttelse, hvilket negativt påvirker efterspørgslen på databeskyttelse. Det er konkluderet, at markedet for databeskyttelse er underlagt markedsfejl i form af informationsfejl. Den asymmetriske information og individets begrænsede rationalitet gør, at der indgås transaktioner, som i virkeligheden ikke maksimerer individets nytte.

Når der er tale om en informationsfejl, kan markedet dog også rettes op af sig selv. Ved brug af spilteorien er det konkluderet, at markedsfejlen ikke bliver rettet op, da virksomheder er opportunistiske, og udnytter forbrugernes begrænsede rationalitet. Dette medfører at markedet lander i et punkt, som ikke maksimerer den sociale velfærd.

Det kan derefter konkluderes, at selv om indførelse af princippet om databeskyttelse gennem design kan have en økonomisk værdi fra et virksomhedssynspunkt, så er værdien af at indsamle persondata og at profitere på dette endnu større.

I den integrerede analyse er der lavet en efficiensanalyse af bestemmelsen om databeskyttelse gennem design. Det er for det første undersøgt, om den effektivt retter op på markedsfejlen, der blev introduceret i den økonomiske analyse, hvilket både afhænger af, om lovgiver har sat et efficient databeskyttelsesniveau, og om de dataansvarlige vil indrette sig efter kravet. Det er her konstateret, at kravet om databeskyttelse gennem design og indførelsen af de høje bøder for overtrædelse, påvirker markedets optimale databeskyttelsesniveau. Det kan dog ikke siges, om dette punkt svarer til, hvad rationelle forbrugere med fuldstændig information ville efterspørge.

Den høje omkostning ved overholdelse sammenholdt med usikkerheden omkring både bødestørrelse og håndhævelse medfører derudover, at kravet mister noget af den afskrækkende effekt, og virksomhedernes incitament til at overholde bestemmelsen mindskes. Det er på denne baggrund konkluderet, at det er tvivlsomt, om virksomhederne vil tilpasse sig det omfattende databeskyttelsesniveau, som lovgiver har sat, uanset om dette viser sig at være det optimale niveau. Dog var forbrugernes manglende oplysning ligeledes en del af markedsfejlen og dette er der i hvert fald sket en forbedring af, da forordningen har virket som en oplysningskampagne for vigtigheden af databeskyttelse og værdien heraf.

Ydermere er der set på bestemmelsens efficiens i forhold til forordningens og EU's overordnede formål. Forordningens formål er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder og art. 25 er klart med til at sikre dette. Dog kan der være en koalition med det indre markedes formål, som bl.a. er at skabe økonomisk vækst. Ved brug af Joseph Schumpeters teori om innovation er det vist, at databeskyttelse gennem design kan have negative konsekvenser for innovationen og da dette er katalysatoren for økonomisk vækst jf. Schumpeters teori, kan der argumenteres for, at bestemmelsen kan være decideret innovationshæmmende og dermed strider mod formålet med det indre marked. Omvendt ser Lektor Thomas Hildebrandt forordningen som en mulighed for virksomhederne til at få styr på deres processer og i den forbindelse måske finde områder, der ikke giver værdi og dermed kan fjernes. Derudover har Ann Cavoukian udtalt, at det er en myte, at innovationen skulle blive kvalt på baggrund af krav om Privacy by Design.

Der kan dermed argumenteres både for innovationshæmmende og -skabende virkninger af forordningen, men når der ses isoleret på bestemmelsen om databeskyttelse gennem design, er der mest der taler for det første. Dette set i forhold til den store værdi der er i big data og innovationsmulighederne på dette område. Bestemmelsens fokus på beskyttelse af individet tilbageholder virksomheder fra at tænke innovativt i forhold til potentielle muligheder for brug af persondata. På baggrund af dette konkluderes det, at bestemmelsen er hæmmende for nogle af de overordnede formål med det indre marked.

Selv om bestemmelsen må antages delvis at rette op på markedesfejlen, vurderes den derfor ikke til at være efficient i forhold til EU's overordnede formål, da den vil hæmme den økonomiske vækst.

Litteraturliste

Bøger:

- Andersen, Esben Sloth. 2004. *Økonomiens konger – Joseph A. Schumpeter*. Jurist- og Økonomforbundets Forlag.
- Andersen, Finn Rolighed; Jensen, Bjarne Warming; Jepsen, Kurt; Olsen, Mette Risgaard & Schmalz, Peter. 2013. *International markedsføring*. Trojka. 4. udgave.
- Cabral, Luis M. B. 2000. *Introduction to Industrial Organization*. The MIT Press.
- Eide, Erling & Stavang, Endre. 2014. *Rettsøkonomi*. Cappelen Akademisk Forlag.
- Hansen, Anders Christian. 2007. *Uden for hovedstrømmen - Alternative strømninger i økonomisk teori*. Roskilde Universitetsforlag.
- Hendrikse, George. 2003. *Economics and Management of Organizations: Co-ordination, Motivation and Strategy*. McGraw-Hill Education.
- Knudsen, Christian. 1997. *Økonomisk Metodologi Bind 2 – Virksomhedsteori & Industriøkonomi*. Jurist- og Økonomforbundets Forlag.
- Messerschmidt, Morten. 2013. *Intet over og intet ved siden af - EU-Domstolen og dens aktivisme*. People's Press.
- Neergaard, Ulla & Nielsen, Ruth. 2016. *EU-ret*. Karnov Group.
- Tvarnø, Christina & Nielsen, Ruth. 2017. *Retskilder & Retsteorier*. Jurist- og Økonomforbundets Forlag.
- Udsen, Henrik. 2016. *IT-ret*. Ex Tuto. 3. udgave.
- Van Blarckom, G.W., Borking, JJ og Olk, J.G.E. 2003. *Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents*. College bescherming persoonsgegevens.
- Viscusi, W. Kip; Harrington, Joseph E. and Vernon, John M. 2005. *Economics of regulation and antitrust*. The MIT Press. 4. udgave.
- Østergaard, Kim. 2003. *Metode på cand. merc. jur. studiet. Julebog 2003*.

Artikler:

- Arildsen, Vibeke. 11. september 2017. *ITU-forsker: Brug persondataforordningen til at styrke forretningen*. Artikel udgivet på ITU i Københavns hjemmeside.
- Borberg, Vibeke. 2016. *Hovedhensyn bag EU-Domstolens afgørelse i Google Spain-sagen*. Jurist- og Økonomforbundets Forlag
- Bygrave, Lee A. 2017. *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*. Forskningspublikation udgivet i Oslo Law Review. Scandinavian University Press. Volume 4, No. 2-2017, pp. 105–120. ISSN online: 2387-3299.

Datatilsynet i Norge. Artikel på det norske datatilsyns hjemmeside. 2017. *Syv steg til innebygd personvern*.

Fribo, Adam. 13. juni 2017. Datatilsynet 11 måneder før persondataforordningen: "Vi kan ikke håndhæve loven med de nuværende ressourcer". Artikel udgivet på Computerworld.dk.

Hoepman, Jaap-Henk. 2014. Privacy design strategies – (extended abstract). In *ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014*.

Isaac, Kevin. 10. april 2017. *How to turn GDPR into a competitive advantage with 'privacy by design'*.

Jørgensen, Rikke Frank og Pedersen, Anja Møller. 2017. *Grib chancen for at styrke databeskyttelsen*.

Koch, C.A. *Trust, Opportunism, Protective Mechanisms and Institutions*. I Nielsen, K., red.: *Social Capital, Trust and Networks*. Publiceret af Edward Elgar i 2006.

Mortensen, Henning. 2017. *Databeskyttelse gennem design – en nyskabelse i databeskyttelsesforordningen?* Artikel fra Karnov Group Denmark. RR.2017.12.0064

Paccès, Alessio M. & Visscher, Louis T. 2013. *Methodology of Law and Economics*.

Ritzau. 2. september 2017. *Regeringen vil styrke Datatilsynet med flere penge*. Artikel udgivet på dr.dk.

Villadsen, Steffen. 19. juni 2017. *Professor: Minimal risiko for kæmpebøder til virksomheder når EU-persondataforordningen træder i kraft*. Artikel udgivet på Computerworld.dk.

Ølykke, Grith Skovgaard & Møllgaard, Peter. 2013. *What is a Service of General Economic Interest?*

Hjemmesider:

Information om Rådet for Digital sikkerhed fra deres hjemmeside. <http://www.digitalsikkerhed.dk/>

Pressemeddelelse fra Devoteam. 30. maj 2017. *Devoteam lancerer ny markedsundersøgelse for EU persondataforordningen*. Direkte link: <https://dk.devoteam.com/2017/05/30/pressemeddelelse-devoteam-lancerer-ny-markedsundersogelse-eu-persondataforordningen/>

Definition på økonomisk værdi. *Economic Value*. <https://www.investopedia.com/terms/e/economic-value.asp>

Digitaliseringsstyrelsens Open government-handlingsplan 2013-2016.

<https://digst.dk/strategier/internationalt-samarbejde/open-government/open-government-handlingsplan-2013-2016/>

Vejledning og rapporter:

Artikel 29-gruppens udtalelse om "The Future of Privacy", vedtaget den 1. december 2009, (WP 168)

Cavoukian, Ann. 2010. *Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices*.

Cavoukian, Ann. 2011. *Privacy by Design, Strong Privacy Protection – Now, and Well into the Future, A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners*.

ENISA. Rapport udarbejdet af ENISA. 2014/2015. *Privacy and Data Protection by Design – from policy to engineering*.

Information Commissioner's Office. Vejledning udarbejdet af ICO 20. oktober 2017. *Overview of the General Data Protection Regulation (GDPR)*.

Information Commissioner's Office. Vejledning udarbejdet af ICO 8. februar 2018. *The Guide to Data Protection*.

Rostgaard, Anders. 2013. *Big Data Fremtidens Digitale Råstof*. Rapport udarbejdet af Mandag Morgen i samarbejde med Google.

Rådet for Digital Sikkerheds vejledning om Databeskyttelse gennem Design. Udarbejdet af Rådet for Digital Sikkerhed. 2017.

Smith, Adam. *The Wealth of Nations* (New York: Modern Library, 1937).

Betænkning:

Betænkning nr. 1565/2017. *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*.

Lovforslag:

L 68 Forslag til 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).

Lov:

Lov 2000-05-31 nr. 429 om behandling af personoplysninger (Persondataloven), senest ændret ved L 2017-05-03 nr. 426.

Direktiv og forordning:

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 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).

Udvalgsspørgsmål:

Udvalgsspørgsmål fra Retsudvalget til L 68 Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, som sambehandles med L 69 Forslag til lov om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love, spørgsmål 8, 9, 10, 12, 60 og 61.

Afgørelser:

Afgørelse fra Datatilsynet. Journalnummer 2015-631-0108. Sag mod Cure4you ApS.

Afgørelse fra Datatilsynet. Journalnummer 2011-631-0133. Sag mod Irmatorvet A/S.

EU-domme:

Angående en anmodning, som Göta hovrätt (Sverige) i medfør af artikel 234 EF har indgivet til Domstolen for i den for nævnte ret verserende straffesag mod Bodil Lindqvist. Sag C-101/01. EU:C:2003:596.

Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González. Sag C-131/12. EU:C:2014:317.

SABAM v Netlog. Case C-360/10. EU:C:2012:85.

Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Sag C-70/10. EU:C:2011:771.

Srl CILFIT og Lanificio di Gavardo SpA mod Sundhedsministeriet, Sag 283/81, EU:C:1982:335.

Dom fra Den Europæiske Menneskerettighedsdomstol:

I v Finland. Appl. No. 20511/03, Judgment of 17 July 2008.

Diverse:

Datatilsynets j.nr. 2013-112-0268, Datatilsynets høringssvar vedrørende høring over lovforslag om "bølge 3", 17. december 2013.

Datatilsynets j.nr. 2013-112-0252, Udtalelse over lovforslag om digitale vælgererklæringer.