Efficient ansvarsstruktur i persondataretten med særlig fokus på ansvarlighedsprincippet

Efficient responsibility structure of GDPR with special focus on the accountability principle

Cand.merc.(jur.)-studiet

4. Semester, Kandidatafhandling

Copenhagen Business School

Afleveringsdato: 14. Maj 2020

Antal sider: 77

Antal anslag: 170.997

Studerende:

Bertram Weihrauch, *Studienummer*: 100937

Specialevejledere:

Henrik Lando (Økonomisk vejleder) og
Camilla Kampmann (Juridisk vejleder)

Indholdsfortegnelse:

Abstract

This thesis analyses the liability of data controllers and data processors under the General Data Protection Regulation.[1] The purpose of the thesis is to investigate whether current legislation is efficient, and to propose solutions to minimize the total cost while maintaining the same level of security. The starting point of the analysis is the requirement of the data controller to be able to demonstrate compliance with GDPR, cf. art. 5, section 2 and art. 24, section 1.

In relation to processing activities that are ongoing the data controller should be able to demonstrate compliance of the data processors. This can be achieved with inspections and audits, cf. art. 28, section 3, point h. The present legal position is not entirely clear, as to when and if a data controller is obligated to initiate an inspection. However, given the present legal sources it is concluded that the data controller is obligated to initiate inspections of the data processors after a period of time – The risk of the processing activity is paramount when assessing, how often inspections should be conducted.

The economic analysis suggests that the current legislation is inefficient as the mandatory inspections do not create deterrence-effect in other games. However, inspection from the national authorities do create such deterrence-effect. It is thus concluded that the data controller should only conduct inspections, when the data controller suspects that the processor is incompliant.

The integrated analysis investigates realistic initiatives that are more efficient than current legislation. There are namely two important aspects in achieving efficiency under the current regulation: Cooperation between the member state countries and implementing a less restrictive audit-rule together with random inspections from the national authorities.

[1] Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Kapitel 1

1.1 Indledning:

Den 25. maj 2018 trådte persondataforordningen[2] i kraft i EU, den afløste det tidligere gældende databeskyttelsesdirektiv.[3] Meget af det gamle skelet er videreført, men to nyskabelser har gjort at retsområdet har fået en fornyet relevans, navnlig databehandlerens rolle og de nye retsmidler. Blandt andet grundet frygten for bøder havde mange virksomheder forberedt sig på den nye forordning. Reglernes formål er at beskytte borgernes rettigheder mod uhæmmet indsamling og brug af deres persondata,[4] dette kan læses direkte ud af charterets art. 8.[5] Det er uden tvivl at sådanne data kan bruges til mange formål, og derfor er meget værdifulde. Virksomheder som Facebook, Google m.fl. er blevet beskyldt for at indsamle, og have delt indsamlede informationer med 3. parter uden noget lovligt grundlag. Et skrækeksempel er Cambridge Analytica, der er blevet undersøgt for ulovligt at have benyttet persondata fra Facebook, til at manipulere og personalisere indhold til de enkelte brugere. Det var derfor muligt at påvirke valget i USA og Storbritannien i forbindelse med hhv. det amerikanske valg og Brexit-valget.[6] Hensynet til at beskytte persondata bør ikke unødigt hæmme virksomheders mulighed for at indgå i værdiskabende relationer. Den dataansvarlige er forpligtet til at kunne påvise overholdelse af reglerne. En måde at gøre dette på er ved at føre tilsyn med databehandlerne. Det er ikke sikkert om manglende tilsyn potentielt medfører ansvar for disses handlinger eller undladelser. Dette medfører usikkerhed samt store omkostninger for de enkelte virksomheder. Det er næppe utænkeligt, at disse omkostninger betyder, at databehandlerkonstruktioner beholdes så små som muligt, hvilket betyder, at virksomheder påtager sig opgaver, som de ellers ville have kunne fået udført billigere og bedre i markedet. Denne problemstilling er udgangspunktet for nærværende afhandling.

[2] 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).
[3] Europa-parlamentets og rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
[4] Persondata og personoplysninger bruges som synonymer. Der vil i det fortløbende bruges persondata.
[5] Chartret om grundlæggende rettigheder.
[6] The Guardian, 2020. 'Fresh Cambridge Analytica leak 'Shows global manipulation is out of control''.

1.2 Problemformulering

Denne afhandling søger at afklare, og undersøge det grundlæggende spørgsmål, i hvilken udstrækning Persondataforordningens ansvarsstruktur er efficient samt hvilken betydning tilsynspligten har i denne sammenhæng. Til at besvare dette overordnede spørgsmål vil der stilles et juridisk, økonomisk hhv. integreret spørgsmål, der alle vil søge at besvare det overordnede spørgsmål:

Juridisk spørgsmål: Hvilken ansvarsstruktur er der mellem hhv. dataansvarlig og databehandler under persondataforordningen, og hvilken betydning har tilsynsforpligtelsen i denne sammenhæng?

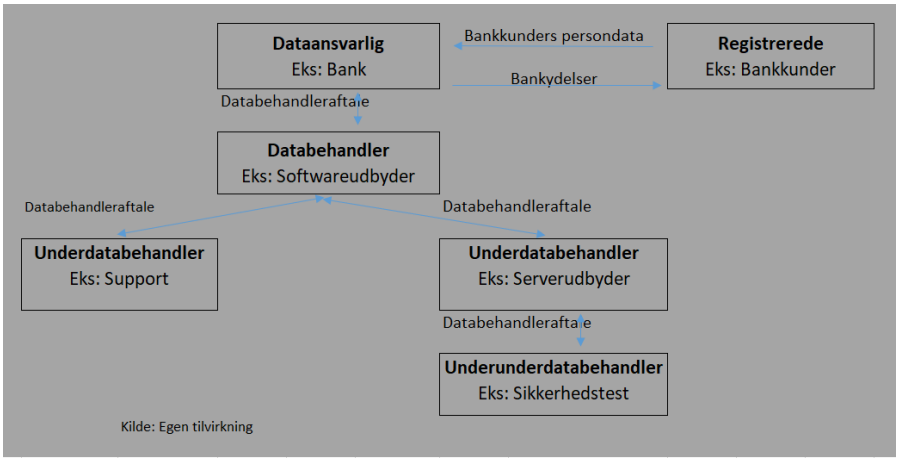
Økonomisk spørgsmål: Hvilken betydning har den overordnede ansvarsstruktur for den dataansvarliges og databehandlerens incitamenter, og hvilken kombination af tilsynsregel og tiltag skaber størst mulig efficiens, når man fastholder beskyttelsesniveauet?

Integreret spørgsmål: Hvilke øvrige virkninger vil der være ved den nuværende regulering samt foreslåede tilsynsregel, og hvilken betydning har samarbejdet mellem medlemsstaterne?

1.3 Synsvinkel

Specialets synsvinkel er på virksomhedsniveau. Det kan dog være vanskeligt i juridisk forstand at sige, at der er en særlig synsvinkel. Der vil dog undersøges de regler som gælder i relation til virksomheder, der enten er databehandler eller dataansvarlig, hvor der er særligt fokus på de pligter som parterne hver især har i forbindelse med databehandleraftaler, tilsynspligt og udskiftning af underdatabehandlere. I økonomisk forstand vil analyseniveauet være databehandleren/dataansvarlige og deres transaktion.

Formålet med den juridiske analyse er at adskille hhv. den dataansvarlige og databehandlerens pligter og ansvar. En databehandlerkonstruktion indenfor denne afhandlings problemfelt kunne se således ud:



I dette eksempel er en bankkundes persondata behandlet først og fremmest af banken. Ét af bankens IT-systemer som data behandles i, ejes og vedligeholdes af en 3. part, softwareudbyder. Softwareudbyderen har outsourcet support og server, der dermed får adgang til og behandler bankkundens persondata. Hele forudsætningen for, at det giver mening at behandle persondata er, at der kan skabes en merværdi ved at overlade en opgave til en tredjepart.

1.4 Afgrænsning

Der vil ikke tages højde for national sektorlovgivning, som visse virksomheder og særligt offentlige myndigheder er underlagt. Der vil i det hele taget ikke behandles de enkelte medlemsstaters nationale ret. Afhandlingens udgangspunkt er således at undersøge forordningens regler.

Der vil ikke tages højde for overførsel til 3. lande, da disse problemer falder uden for denne afhandlings problemfelt, hvorefter der er særlige forhold vedr. overholdelse, håndhævelse mv. De foreslåede tiltag og analyser tager som udgangspunkt kun anvendelse i de situationer, hvor data behandles inden for EU.

Der vil ikke blive behandlet regler vedr. kravet om oversigter over behandlingsaktiviteter, jf. art. 30. På lignende vis, vil der ikke behandles reglerne vedr. anmeldelse af brud, jf. art. 33.

Konsekvensanalysen vil kun behandles i begrænset omfang, jf. art. 35. En af årsagerne hertil, er at medlemsstaterne i et vist omfang har mulighed for at vedtage særlig regulering, jf. art. 35, stk. 5. Der

er tale om lex specialis, der ikke ofte finder anvendelse. Reglen fastsætter udvidede krav ift. det gennemgåede i den juridiske analyse.

Der vil kun overfladisk behandles de registreredes rettigheder, i det omfang en databehandler eller en dataansvarlig skal efterleve disse i forhold til risikovurderingen og tilsynet.

Den juridiske og økonomiske analyse tager ikke højde for private søgsmål som kan opstå ved brud. Der tages dette udgangspunkt, da private tab ofte er små i forbindelse med brud – Det er underforstået, at der skal være et beviseligt tab.[7]

1.5 Metode:

Juridisk metode:

Formålet med den retsdogmatiske tilgang er at udlede gældende ret, de lege lata. Den mest udbredte retsteori i Danmark er Alf Ross realistiske retsteori.[8] Teorien blev fremført af Alf Ross i 1953 i en tid før EU. Anvendelsen af teorien skal derfor tage særligt hensyn til EU-rettens struktur, navnlig i relation til principper, retskilder og fortolkningsstil. Af samme årsag er der eksempelvis heller ikke taget højde for de udfordringer, der kan være ved at have mange sproglige versioner af de samme retskilder. Alf Ross teori er grundlæggende en prognoseteori, hvorefter de juridiske slutninger er prognoser, der enten verificeres eller forkastes af domstolenes afgørelser.[9] Det afgørende for teorien er derfor, hvad den juridiske dommer mener er forpligtende. Selv påstande som efterfølgende forkastes af domstolene, bidrager til den retsvidenskabelige disciplin. På det filosofiske plan er grundtanken at bevæge sig væk fra, hvad retten bør være, og i stedet koncentrere sig om hvad retten er. Denne er fremherskende i de naturvidenskabelige discipliner.

[7] Der vil i øvrigt være krav til at de øvrige erstatningsbetingelser er opfyldt, se eksempelvis Eyben & Isager, 2015, s. 25-28.
[8] Tvarnø & Nielsen, 2017, s. 367.
[9] Tvarnø & Nielsen, 2017, s. 375.

I Ross teori er der ingen intern regulering mellem retskilderne,[10] der vil dog blandt andet tages højde for EU-rettens interne reguleringshierarki og på den måde tilpasse retsteoriens metodik til at kunne omfatte nærværende problemstilling. Af disse grunde vurderes det, at Alf Ross retsteori med de rette tilpasninger kan bruges til at analysere gældende ret på EU-plan for afhandlingens problemformulering.[11]

Anvendelse af retsteori:

Eftersom denne afhandlings fokus er de regler, der gælder på EU-plan og ikke nationale vil der ligeledes kort gives en gennemgang af sammenhængen i retssystemerne.

Persondataforordningen[12] gælder umiddelbart i hver medlemsstat. Derudover følger det af TEUF art. 16,[13] at enhver har ret til at få beskyttet sine persondata. Derved vil selv situationer, der falder uden for forordningens anvendelsesområde i et vidst omfang reguleres af EU-retten, i det omfang TEUF finder anvendelse – Herunder de generelle EU-retlige grundprincipper. Forordningen gælder sideløbende med medlemsstaternes øvrige retsregler, og skaber ingen ret til at foretage handlinger, der ville være ulovlig i medfør af andre regler.

Forordningen overlader et spillerum til medlemsstaterne til at udfylde og supplere forordnings lovtekst. Dette ses også i databeskyttelsesloven,[14] at der er særlige nationale regler, som kun finder anvendelse i Danmark, og som udvider anvendelsesområdet på rent nationalt plan.[15] Der vil i øvrigt ikke tages højde for disse nationale særregler/sektorlovgivning.

[10] Tvarnø & Nielsen, 2017, s. 378.
[11] Se ligeledes Neergaard & Nielsen, 2016, s. 135.
[12] Forordning 2016/679.
[13] Traktaten om Den Europæiske Unions Funktionsmåde.
[14] Lov nr. 502 af 23/05/2018.
[15] Eksempler på dette ses i Databeskyttelseslovens § 2, stk. 5-8. Derudover ses dette også på TV overvågningsområdet, hvor der gælder særregler – I andre EU-lande behandles tv-overvågning af persondataforordningen.

Primær regulering:

TEUF, TEU samt Chartret har stor betydning for retsområdet, men spiller ikke nogen særlig rolle indenfor specialets problemfelt. Disse udgør den øverste del i reguleringshierarkiet.

Bindende sekundær regulering:

Det næste type retskilde i reguleringshierarkiet er direktiver, forordninger og afgørelser, jf. art. 288 TEUF. Rådets forordning 2016/679 danner rammen omkring specialets område. Derfor er forordningen langt hen ad vejen den gennemgående og vigtigste retskilde. Forordningen er almengyldig og gælder umiddelbart i alle medlemsstaterne indenfor forordningens anvendelsesområde. Særligt er det for tilsynspligten med databehandlere, at disse regler ikke er et udtryk for nationale særregler.

Soft Law:

Der benyttes ligeledes vejledninger udstedt af det danske Datatilsyn i den juridiske analyse. Disse er dog ikke retsskabende, men indholdet af dem er så generelt, at indholdet af disse ikke kan forventes at være forkert. Der findes på nuværende tidspunkt ingen working papers eller vejledninger udstedt af EDPB eller de øvrige datatilsyn om den dataansvarliges tilsynspligt.[16] Der vil derudover benyttes udtalelser fra det europæiske databeskyttelsesråd, der har en særlig funktion som harmoniserende enhed i EU, se mere herom nedenfor. Den omtalte udtalelse er 'udtalelse 14/2019'.[17]

Retspraksis:

Der har særligt været tvivl om, hvilken retspraksis som eksisterede før d. 25/5 – 2018 som stadig er gældende, derfor vil denne kun bruges sparsomt, da det i en række tilfælde er tvivlsomt, hvorvidt

[16] Det danske datatilsyn har dog en vejledning om netop pligten til at føre tilsyn.
[17] Langt størstedelen af de udtalelser, der har været har afgjort spørgsmål vedr. konsekvensanalysen.

retstilstanden er uændret sammenlignet med det dagældende direktiv.[18] Der benyttes enkelte EU-domme fra før denne tid, hvor der alene er sket sproglige fornyelser uden nogen indholdsmæssige ændringer, og hvor fortolkningsbidraget også gælder for forordningen – eksempelvis, hvad der forstås ved persondata.

Der har på nuværende tidspunkt ikke været afsagt nogen afgørelser ved EU-domstolen vedr. forordningen. Den praksis, der har været har således været afsagt ved de nationale tilsyn, hvilket indebærer en risiko for, at de afsagte afgørelser er et udtryk for national praksis, og EU-domstolen ville fortolke spørgsmålet anderledes. Afgørelserne er dog, foruden forordningen på nuværende tidspunkt de bedste retskilder til at udfylde forordningens ord. Der bør tillægges særligt vægt på de nationale afgørelser som databeskyttelsesrådet, EDPB, fremhæver på deres hjemmeside https://edpb.europa.eu/edpb_en. Dette skyldes, at der i forordningens præambelbetragtning 139 tillægges EDPB en særlig rolle ved at bidrage til ens retshåndhævelse i EU og fremme samarbejdet samt afgøre uenigheder mellem de nationale tilsynsmyndigheder samt art. 70. Derudover rådgiver rådet kommissionen, jf. p. 136. Rådets medlemmer udgøres blandt andet af repræsentanter fra medlemsstaternes tilsyn og agerer uafhængigt af de nationale tilsyn. Af disse grunde vil særligt de afgørelser som EDPB fremhæver forventes at skabe fælles EU-praksis, da de nationale tilsyn vil følge udviklingen i de øvrige medlemsstater tæt – Dette må særligt forventes at være tilfældet på nuværende tidspunkt, hvor der er få domme fra EU-domstolen indenfor afhandlingens område.

Fortolkningsstil:

Eftersom EU-domstolen fortrinsvist benytter formålsfortolkning, når den skal afgøre et spørgsmål, vil denne fremgangsmåde ligeledes benyttes i denne afhandling. Årsagen til dette skal findes i de forskellige sproglige versioneringer af lovteksten, og er tidligere fremhævet i EU domstolens praksis.[19]

[18] Direktiv 95/46/EF.
[19] Sri CILFIT og Lanificio di Gavardo SpA mod sundhedsministeriet, Sag 283/81, EU:C:1982:335, p. 18-20.

Formålet med forordningen fremgår i øvrigt af art. 1, stk. 1-2, og søger at beskytte persondata ved behandling. Denne må dog ikke gå udover den frie udveksling af persondata.

Økonomisk metode:

Afhandlingens økonomiske analyse har til formål at belyse de incitamenter som hhv. dataansvarlig og databehandler har.[20] Den grundlæggende økonomiske tilgang til problemstillingen er ved brug af spilteori. Der vil i denne afhandling udelukkende være tale om non-kooperative spil, hvor hver part søger at optimere givet dennes antagelser om den anden spillers handlinger. Det er en grundlæggende antagelse om spillerne, der i udgangspunktet følger den strategiske nash-ligevægt.[21] Det antages, at spillerne er risikoneutrale, og har fuldstændig viden bortset fra spilleren naturs valg. Spilteorien vurderes at være velegnet, som grundlag for at analysere spillernes transaktion, da dette kan opstilles som et spil med forskellige strategivalg, hvor spillernes type, reglen, opdagelsesrisiko, omkostninger mv. påvirker spillets ligevægt.[22] Der indgår forskellige ingredienser i et givent spil, Knudsen udtrykker det på denne måde:[23] (1) Identificer de forskellige spillere, (2) Identificer spillernes strategivalg, (3) Specificer spillernes viden og (4) Specificer de payoffs som hver spiller modtager. På baggrund heraf skal det fastslås om der findes Nash-ligevægte og i det tilfælde, der er flere, hvilke som er realistiske. Spilteorien fastlægger stærke antagelser omkring spillernes rationalitet og viden. Disse antagelser holder dog ikke altid, der vil derfor søges at tage højde for dette ved at indføre omkostningsasymmetri og forskellige spillertyper, for bedre at kunne modellere virkeligheden.[24]

[20] Herefter benævnt spillerne.
[21] Knudsen, 1994, s. 273
[22] Knudsen, 1994, s. 278-279.
[23] Knudsen, 1997, s. 102.
[24] Knudsen, 1994, s. 274-276.

Omkostninger:

Der eksisterer transaktions- og overholdelsesomkostninger i denne model, eftersom parterne skal indgå en databehandleraftale. Overholdelsesomkostningerne er de omkostninger, der skal til for at tilpasse sikkerheden til risikoen – Der er lagt til grund, at des større risiko, der er, jo dyrere bliver overholdelsesomkostningen. Derudover er den en sammenhæng mellem antallet af led, der er i behandlerkonstruktionen og den samlede transaktionsomkostning, der eksisterer der ved tidspunkt T = 0. Der er derudover overvågningsomkostninger ved udførelse af tilsyn.

Overordnede ansvarsstruktur:

Der vil i denne afhandling først redegøres for de overordnede ansvarsovervejelser som reglerne udstikker, og hvilke incitamenter spillerne har. Som nævnt i afgrænsningen vil der ikke tages højde for private søgsmål. Den økonomiske sanktion som virksomhederne risikerer, er alt lige fra kritik, påbud til egentlige bødeforlæg, alt efter hvor alvorlig overtrædelsen er. Ved valg af sanktion lægges der særlig vægt på, hvorvidt overtrædelsen sker forsætligt eller uagtsomt. Der vil dog her antages ikke at være udfordringer ved bevisvurderingen. Der er som udgangspunkt ansvar for hver af parterne selvstændigt, ved brud på deres forpligtelser. Det indgår som et led i vurderingen, hvor sandsynligt det er, at de nationale tilsyn vil efterse en given spiller, og dermed hvilken risiko der er ved at blive opdaget.

Det spilteoretiske setup, som beskrevet vedr. den overordnede ansvarsstruktur[25] er sammenligneligt med det man finder i klassisk økonomisk litteratur vedr. forbrydelser.[26] Det er ukendt for spillerne, hvorvidt de vil blive ført tilsyn med, og dermed risikere straf fra de nationale tilsyn. Der vil derfor være tale om et sekventielt spil, hvor den sidste spiller er de nationale myndigheder. Det mulige tilsyn fra de nationale myndigheder vil i analysen blive anset som spilleren natur.[27] Risikoen vil dog være kendelig for spillerne inden de træffer deres strategivalg. Det antages generelt, at spillerne kender de regler, og

[25] Se den økonomiske analyse.
[26] Se eksempelvis Mark C Stafford's artikel 'Deterrence Theory: Crime', 2015.
[27] Spilleren natur vælger ved en for spillerne tilfældig strategi som de ikke kender på forhånd. De kender dog godt konsekvensen ved strategien samt med hvilken sandsynlighed denne forekommer.

forpligtelser de er underlagt. Strategivalget bliver truffet på baggrund af det forventede økonomiske payoff ved de givne strategivalg, hvorfor det ikke har nogen betydning for strategivalget på tidspunkt 0, om spilleren ender ved det 'gode' eller 'dårlige' state.

Det antages, at spillerne har to valg enten at efterleve reglerne eller ikke at efterleve reglerne. Spillerne vil kun indgå i transaktioner, der er bedre end deres reservationsnytte. Hvis spillerne ikke vælger det samme, ender de med et udfald på (0,0) – Det antages generelt, at spillernes reservationsnytte er 0. De vil derfor altid indgå i spillet, men det er ikke sikkert, at spillet medfører en transaktion. På den måde minder interaktionen om spillet 'Battle of the Sexes'.[28]

Ligevægtsbegreb og optimering:

Det grundlæggende ligevægtsbegreb følger Kaldor-Hicks mellem parterne,[29] hvorefter den ene spiller kan stilles dårligere såfremt det samlede payoff er større end under status quo. Efficiensen opgøres i den monetære værdi – Der antages derfor ikke at være forskel på om det er den første eller sidste krone, der er tjent.

Det er en grundlæggende betingelse, at den registrerede skal have samme payoff. Formålet med de persondataretlige regler er at forsøge at beskytte fysiske personers informationer. I økonomisk forstand er dette svært at omsætte værdien af denne beskyttelse for private personer. Derfor er den grundlæggende tilgang, at reglerne skal skabe det samme beskyttelsesniveau, men reducere de samlede omkostninger til håndhævelse af reglerne – Det mest efficiente udfald er derfor i denne afhandling, at det samme beskyttelsesniveau opnås , samtidig med at omkostningerne er mindst mulige. Dette kan ske ved f.eks. at ændre i ansvarsstrukturen, eller iværksætte andre tiltag.

[28] Dutta, 1999, s. 55

[29] Opkaldt efter Nicholas Kaldor og John Hicks. Hvorefter forbedringer bør ske, hvis det samlede payoff er højere end den nuværende tilstand.

Tilsynsforpligtelsen:

Der er på nuværende tidspunkt ikke klarhed over, hvorvidt den dataansvarliges manglende tilsyn kan påføre ansvar for den dataansvarlige, hvis databehandleren overtræder forordningen ved ikke at leve op til det aftalte.[30] Der er på nuværende tidspunkt to sandsynlige fortolkninger af forpligtelsen som danner udgangspunktet for den økonomiske analyse. Den ene udmærker sig ved at den dataansvarlige kan blive gjort ansvarlig, og kan bedst beskrives som et principal-agent-problem,[31] da forhold efter kontraktens indgåelse har indflydelse på den dataansvarliges payoff. Derudover er der en udtalt grad af asymmetrisk viden, og databehandleren har modsatrettede interesser.[32]

Integreret metode:

Der vil i det integrerede analyseafsnit tages udgangspunkt i den juridiske analyse og den økonomiske analyse.[33] På baggrund heraf fastlægges de konsekvenser som reglerne medfører. Det må bemærkes, at der ikke findes én anerkendt metodisk integreret tilgang. Det integrerede spørgsmål vil som udgangspunkt behandles under ét, forstået på den måde, at problemstillingen både vil underkastes juridisk og økonomisk metode og teori for på den måde at fastslå virkning og konsekvenser ved foreslåede retstillinger.

Den juridiske metode vil dels blive benyttet til at fastlægge gældende ret, men i høj grad også til at fastslå hvad retten bør være, de lege ferenda.[34] Retspolitikken beskæftiger sig med, hvad retten bør være, og er i teoretisk forstand anderledes end den retsdogmatiske analyse, der foretages i det juridiske analyse-afsnit. Økonomisk teori vil danne udgangspunktet for de forslag, der måtte være til at øge

[30] For yderligere se herunder afsnittet om tilsynspligten i den juridiske analyse.
[31] Hendrikse, 2003, s. 90-91.
[32] Dennes handlinger har indflydelse på, hvilket payoff principalen får. Principalen har muligheden for at føre tilsyn (kontrollere) og på den måde allokere ansvaret væk fra sig selv. Det vil særligt her gennemgås hvilke incitamenter parterne har samt, hvornår disse er konfliktende.
[33] Tvarnø & Denta, 2015, s. 191

[34] Tvarnø & Nielsen, 2017, s. 30.

efficiensen. Der vil i analysen tages særlig højde for, at det tidligere persondatadirektiv,[35] var gældende fra 1998-2018 og forordningen, ligeledes må forventes at have en lang levetid. Der vil derfor tages særligt forbehold for, hvilke realistiske tiltag og virkninger som kan indføres under det nuværende regelsæt.[36]

Den benyttede økonomiske teori vil søge at problematisere nogle af de stærke antagelser omkring spillerne, som behandlet i det økonomiske afsnit. Spilteorien er stadig teorigrundlaget, der vil som en tilføjelse tages højde for reciprocitet og usikkerhed ved håndhævelsen af reglen.[37] Analysen viser, at selv når man tager højde for disse forhold, at de foreslåede regler vil løse inefficiente ligevægte, som kan opstå som følge af reciprocitet og usikkerhed.

I den integrerede analyse vil der ligeledes undersøges på hvilken måde efficiensen kan øges, hvis det er muligt blot at sænke beskyttelsesniveauet marginalt. Der vil i denne del af analysen lægges særligt vægt på det forhold, at reglerne gerne skal beskytte noget, der forhindrer et tab og hvor brud medfører et tab.

1.6 Struktur:

Denne afhandlings struktur er således, at der først vil analyseres det juridiske spørgsmål. På baggrund af de resultater vil der ved hjælp af økonomisk analyse udlede de konsekvenser som reglerne medfører. Der er derfor valgt en fremgangsmåde, hvor der først udledes gældende ret og derefter de konsekvenser som dette medfører og hvorvidt det er muligt at optimere denne regel.

Der vil slutteligt på baggrund af den juridiske og økonomiske analyse, udledes de økonomiske konsekvenser som reglen medfører, og forslag til tiltag, der øger efficiensen. Den integrerede analyse baserer sig på resultaterne fra den juridiske og økonomiske analyse.

[35] Direktiv 95/46/EF.
[36] Det antages, at den grundlæggende ansvarsstruktur kun i meget begrænset omfang kan ændres.
[37] Disse to elementer har tidligere været antaget som ikkeeksisterende i den økonomiske analyse.

Kapitel 2 - Juridisk analyse

I de følgende afsnit vil de persondataretlige regler analyseres ved brug af den juridiske metode med det formål at fastlægge fordelingen af pligter og regler, der gælder for hhv. databehandler og dataansvarlige. Der vil i den forbindelse lægges særlig vægt på aftaler mellem parterne, databehandleraftaler, tilsynsforpligtelser og udskiftning af underdatabehandlere.

Til sidst vil der opsamles de vigtige analyseresultater, der tilsammen besvarer det stillede juridiske spørgsmål.

2.1 Personoplysninger:

I forordningens[38] art. 4, nr. 1, følger det, at personoplysninger er "…*enhver form for information om en identificeret eller identificerbar fysisk person …*", af den første del er det værd at bemærke, at informationen kan være i ethvert tænkeligt format. Af den anden del skal det være muligt at kunne identificere en fysisk person. Det er uden betydning, at ikke alle og enhver kan identificere den fysiske person. En sammenligning af forordningens tekst sammenholdt med det tidligere gældende direktiv har man beholdt det samme indhold, hvorfor praksis fra før forordningens ikrafttræden vurderes stadig at være relevant. Afgrænsningen mellem hvad der er persondata,[39] og hvad der ikke er, kan i grænsetilfælde være svær. Fra retspraksis er C-582/14,[40] hvor domstolen tog stilling til IP-adresser i forbindelse med en tysk statsborgers brug at tyske onlinemedietjenester. Borgerens IP-adressen blev udstillet offentligt, og der blev i sagen lagt til grund, at dynamiske IP-adresser[41] ikke udgjorde persondata, da det ikke var lovligt eller praktisk muligt at koble en midlertidig IP-adresse op på en enhed, jf. P. 46. Statiske IP-adresser[42] er væsentligt lettere at sammenkoble med øvrige oplysninger om

[38] Forordning 2016/679, herefter benævnt persondataforordningen eller forordningen.
[39] Persondata og personlysninger bruges som synonymer. Der vil herefter bruges persondata.
[40] Patrick Breyer mod Bundesrepublik Deutschland, sag C-582/14, EU:C:2016:779
[41] Dynamiske IP-adresser er IP-adresser, hvor der tildeles en ny ved hvert besøg på en ny hjemmeside, hvilket ikke giver internetudbyderen muligheden for at identificere den enkelte maskine og dermed den fysiske person.
[42] Statiske IP-adresser betyder, at internetudbyderen har mulighed for at kortlægge internettrafikken og dermed identificere den enkelte maskine.

enheden, hvorfor disse som udgangspunkt udgør persondata. Det er særligt interessant, at man ikke nødvendigvis behøver at kunne identificere den fysiske person med sikkerhed. Det er tilstrækkeligt så længe den sandsynlige bruger kan fastslås med en vis sikkerhed. En enkelt PC kan for eksempel, benyttes af flere fysiske personer, der således benytter samme IP-adresse. Af samme grund kan det i nogle tilfælde være svært at være sikker på, om en information reelt er persondata og dermed omfattet af forordningen eller ej.

2.2 Anvendelsesområde

Det materielle anvendelsesområde følger af persondataforordningens art. 2. Af bestemmelsens stk. 1 følger, at forordningen gælder for automatisk behandling af persondata samt manuel behandling omfattet af et register. Det er her særligt relevant at bemærke at automatisk behandling er omfattet – Den engelsksprogede version af forordningen bruger ordet 'automated', hvilket heller ikke synes at skabe større klarhed over, hvad der menes hermed. Man må antage at retstillingen er uændret i sammenlignet med databeskyttelsesdirektivets[43] art. 1, stk. 1, hvor behandling foretaget "*ved hjælp af edb*" var omfattet. I en mere moderne kontekst ville 'Edb' forstås som egentlig digital behandling – hvilket alt andet lige er meget udbredt. Der synes ikke at være tiltænkt en reel indholdsændring ved den nye formulering udover en sproglig opdatering. På samme måde som digitale informationer er lette at bruge, ved at søge i eller strukturere, er de tilsvarende lettere at misbruge, hvorfor visse manuelle behandlinger er undtaget.[44]

I tillæg hertil bør det nævnes, at TEUF[45] art. 16, stk. 1 fastslår:

> "*1. Enhver har ret til beskyttelse af personoplysninger om vedkommende selv.*"

[43] Direktiv 95/46/EF.
[44] Dette følger af forordningens præambel 15, hvorefter ustrukturerede sagsmapper eksempelvis ikke er omfattet af forordnings anvendelsesområde.
[45] Traktaten om Den Europæiske Unions Funktionsmåde

Bestemmelsens synes dog at udvide forordningens anvendelsesområde udover, hvad der følger af forordningens art. 2, stk. 1. Der er ikke et krav om at persondata vedrør en EU-borger. Der er ikke krav om grænseoverskridende interesse, som det eksempelvis er tilfældet med reglerne om fri bevægelighed. Reglernes anvendelsesområde er derfor enormt bredt.

I forordningens art. 2, stk. 2 oplistes en række behandlingsaktiviteter, der falder uden for forordningens anvendelsesområde. Det følger af litra a, at forordningen ikke finder anvendelse under udøvelse af aktiviteter, der falder uden for EU-retten – af præambel 16 følger det, at et eksempel på dette er udøvelse af medlemsstaternes sikkerhed, hvilket ikke umiddelbart finder anvendelse overfor virksomheder.

Det territorielle anvendelsesområde bestemmes af forordningens art. 3. Det følger af stk. 1, at forordningen finder anvendelse, når vedkommende databehandler eller dataansvarlig er etableret i unionen, uanset om behandlingen faktisk sker i EU. Som en nyskabelse er databehandleren tilføjet og direkte omfattet, sammenlignet med direktivets ordlyd.[46] Hvad der præcist ligger i etablering, bliver præciseret i præambel 22:

> "*Etablering indebærer effektiv og faktisk udøvelse af aktivitet gennem en mere permanent struktur*."

Der er intet krav om særlige selskabsformer, eller etableringsform, hvilket alt andet lige gør omgåelse sværere.

Af stk. 2 følger det, at forordningen tillige finder anvendelse for registrerede inden for EU, selv når databehandler og dataansvarlige, ikke er etablerede efter stk. 1, når der udbydes varer eller tjenesteydelser til de registrerede i Unionen. Det tillægges ingen vægt om den registrerede skal betale for ydelserne. Af præambelbetragtning nr. 23 følger det, at det ikke er tilstrækkeligt, at der eksempelvis er adgang til en udbyders internetside. Der vil dog i det omfang, at der på hjemmesiden benyttes sprog/valuta som kun benyttes i et eller flere EU-områder, formentlig være tilstrækkeligt til at kunne fastslå, at der udbydes ydelser inden for unionen. Denne retstilstand er meget vidtgående og

[46] Sammenlign med ordlyden i art. 3.

omhandler primært lovvalget. Man kan derfor med rette være i tvivl om, hvorvidt et 3. lands domstol vil lægge forordningen til grund forud for egne nationale regler, hvor behandling er lovlig i 3. land. Denne problemstilling er i øvrigt ikke noget som forordningen tager videre stilling til.

2.3 Persondatatyper, Lovlig behandling og behandlingsgrundlag

Det er en forudsætning for, at forordningen finder anvendelse, at persondata behandles. Begrebet behandling defineres i art. 4, stk. 1, nr. 2. Definitionen er enormt bred, jf. ordene: "enhver aktivitet" og der er oplistet en hel række tilfælde, hvor der er tale om behandling:

> "*… f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse*"

De oplistede tilfælde er en ikke-udtømmende liste, og begrebet omfatter derfor mere end dette. De fleste handlinger er derfor omfattet af behandler-begrebet.

Lovlig behandling forudsætter hjemmel, jf. art. 6. Dette udvides med de generelle principper i art. 5. Det er særligt vigtigt at lægge mærke til art. 5, stk. 1, nr. 1, hvorefter behandling skal være lovlig, rimelig og gennemsigtig – indholdsmæssigt svarer dette til direktivbestemmelsen i art. 6, stk. 1, nr. 1, hvorfor man må antage at praksis er uændret. I den dagældende persondatalov [47] var dette princip implementeret i dansk ret som "*god databehandlingsskik*", jf. § 5, stk. 1. Selvom denne formulering ikke går igen i databeskyttelsesloven,[48] må man alligevel kunne betragte bestemmelsen i art. 5 som en generalklausul, en generel rettesnor for hvordan behandling af persondata bør ske.

Det er ligeledes værd at bemærke, at forordningen ikke skaber ret til at foretage behandlinger, der ville være i ulovlig i medfør af andre retsregler. I tillæg hertil oplister art. 5 stk. 1, litra b-f en række pligter:

[47] Lov om behandling af personoplysninger, Lov nr. 429 af 31/05/2000 (historisk)
[48] Da forordningen gælder direkte i medlemsstaterne, ville det være forkert at videreføre strengt nationale betegnelser, da dette ville modvirke harmoniseringen i EU.

Formålsbegrænsning, dataminimering, berigtigelse af persondata, opbevaringsbegrænsning samt sikre behandlingens integritet og fortrolighed. Det er den dataansvarliges ansvar at sikre og kunne påvise at disse principper er opfyldt, jf. stk. 2.

Typer af persondata

Alle persondata er som udgangspunkt almindelige, medmindre de er oplistet i art 9 og 10, benævnt som særlige kategorier af persondata, i undertiden benævnt "følsomme oplysninger", jf. præambelbetragtning 10. Modsætningsvist er alle andre persondata for så vidt almindelige, og derfor gælder de almindelige regler i art. 6-7 for så vidt angår behandlingens lovlighed.

Der er i vidt omfang adgang for medlemsstaterne at fastlægge særlige nationale særregler for så vidt angår behandling efter art. 9 og 10.

Af art. 9 er blandt andet racemæssige, politisk, religiøse, seksuelle forhold omfattet af særlige regler. Efter art. 10 kræver behandling af straffedomme samt lovovertrædelser særskilt offentligt tilsyn. Oplistningerne i art. 9 og 10 er udtømmende.

Behandlingsgrundlag

For virksomheder er de vigtigste behandlingsgrundlag samtykke eller aftale mellem den registrerede og den dataansvarlige. Samtykke følger af art. 7, stk. 1., nr. 1 – Det er et krav, at samtykket er givet til et eller flere konkrete formål. Det er den dataansvarliges ansvar at kunne dokumentere, at der er givet samtykke, det vil sige, at risikoen for at en behandling ikke måtte foretages, da samtykket var ugyldigt, påhviler den dataansvarlige, jf. art. 7, stk. 1. Samtykke kan som hovedregel trækkes tilbage, hvorefter behandling skal ophøre. Samtykket skal være frivilligt, specifikt, informeret og utvetydigt, hvorefter den dataansvarlig kan behandle dennes persondata, jf. art. 4, stk. 1, nr. 11. Det er særligt værd at bemærke at behandling af følsomme persondata, jf. art. 9, stk. 2, litra a ligeledes kræver at samtykket er afgivet "udtrykkeligt", det kan ikke antages, at der i den forbindelse gælder et særligt krav sammenlignet med

samtykke-kravet for almindelige persondata. Ordet har derfor alene en signalværdi overfor den dataansvarlige, der bør udvise ekstra forsigtighed.

Kravet om at den registreredes samtykke kan tilbagetrækkes, kan skabe visse udfordringer, da data skal kunne fjernes fra eksempelvis de IT-miljøer som de indgår i. Dette gælder tilsvarende for backup-filer mv. fra det tidspunkt, hvor samtykket trækkes tilbage.[49] Persondata skal som udgangspunkt slettes efter tilbagetrækning, medmindre der foreligger andre behandlingsgrundlag, jf. art. 17, stk. 1, litra b. Det kræver, at den dataansvarlige systematisk og påviseligt kan håndtere sådanne henvendelser, modsætningsvist ville det kræve enorme tidsmæssige ressourcer, for at leve op til forordningens krav.[50]

Et andet vigtigt behandlingsgrundlag er behandling, der er påkrævet for opfyldelse af en kontrakt, hvor den registrerede[51] er aftalepart, jf. art. 6, stk. 1, litra b. Aftalegrundlaget må vurderes ud fra aftalens lovvalg. Det har som udgangspunkt den fordel for den dataansvarlige, at behandlingsgrundlaget først bortfalder når persondata ingen relevans har længere ift. opfyldelse af aftalen. Dette behandlingsgrundlag kan kun bruges i forbindelse med de almindelige persondata – Ved behandling af følsomme persondata findes der ikke en tilsvarende mulighed, der skal derfor i aftalen tages højde for at samtykke skal afgives selvstændigt, og kan tilbagetrækkes af den registrerede. Se de særlige krav i art. 7, stk. 2, hvorefter det ikke må være et krav at samtykke afgives førend aftalen er gyldig.[52]

2.4 Dataansvarlig og databehandler - ansvarsovervejelser:

I forbindelse med behandlingen af persondata, vil en given virksomhed, der behandler persondata være enten dataansvarlig eller databehandler, alt efter den konkrete konstruktion. Der vil altid være mindst en dataansvarlig, der er ansvarlig for behandlingsaktiviteten. Det er ikke sikkert, at der i konstruktionen

[49] Man har i forordningen netop forsøgt at imødekomme disse forhold i art. 25.
[50] I lighed hermed fastlægger forordningens art. 15-22, herunder ret til indsigt, berigtigelse, sletning, begrænsning, dataportabilitet, hvilket ligeledes taler for, at persondata relativt let bør kunne søges i samt fjernes når behandlingen ikke længere er relevant/lovlig.
[51] Den registrerede er den fysiske person, hvis persondata, der behandles, jf. art. 4, nr. 1.
[52] Et eksempel herpå kunne være optikerforretninger. Disse scanner kunders iris, der udgør biometrisk data, til brug for at levere optikerydelser. Forretningen bærer risikoen for, at de har sikret sig fornødent samtykke, modsætningsvist ville behandlingen i form af brugen og opbevaring være i strid med forordningen uanset, at formålet med behandlingen var at leve op til en gyldig aftale med den registrerede.

er databehandlere. Den dataansvarlige defineres i art. 4, stk. 1, nr. 7, som den part der kan tilrettelægge formålet og hjælpemidlerne i forbindelse med behandlingen. Det følger, at databehandleren i art. 4, stk. 1, nr. 8 behandler data på vegne af den dataansvarlige. Det er ikke altid ganske klart, hvori afgrænsningen mellem dataansvarlig og databehandler går. Datatilsynets vejledning[53] lægger vægt på, at databehandleren er underlagt instruks, dette synspunkt understøttes i forordningens tekst, da "*En databehandlers behandlingen skal være reguleret af en kontrakt*", [54] i praksis benævnt databehandleraftale. [55] Det er af afgørende betydning, at selve formålet med den ydelse databehandleren leverer, skal indebære behandling af persondata. I vurderingen af om en part er dataansvarlig/databehandler, vil der indgå som en del af vurderingen, hvad parterne har aftalt vedr. deres roller – Der vil dog ikke være direkte mulighed for omgåelse ved at overdrage ansvaret.[56]

Der er ikke nødvendigvis tale om, at man agerer som databehandler blot fordi man skal får adgang til persondata. Et eksempel som fremgår i vejledningen[57] om en reparatør af en kopimaskine ikke bliver til databehandler blot, fordi denne får adgang til persondata, da formålet med aftalen ikke på nogen måde er, at der skal behandles persondata. Derimod vil fejlretning af data i et kundesystem udgøre persondata, da selve formålet netop er at behandle persondata, jf. art. 4, stk. 1, nr. 2. I grænsetilfælde kan det være svært at skelne mellem de to, og forordningen efterlader medlemsstaterne et rum til at præcisere, hvornår en given part handler som dataansvarlig, jf. art. 23.

Overordnede ansvarsfordeling i forhold til persondata og behandlingsgrundlag:

Hverken dataansvarlig eller -behandler kan blive gjort ansvarlige for hinandens bøder. Parterne vil som udgangspunkt hæfte selvstændigt ved deres overtrædelse af persondatareglerne. Den dataansvarlige er som udgangspunkt ansvarlig for hele behandlingsaktiviteten og dermed alle databehandlere, jf. art.

[53] 'Vejledning om dataansvarlige og databehandlere', publiceret i November 2017 af Datatilsynet, afsnit 3.1.2
[54] Art. 28, stk. 3.
[55] I det følgende blot benævnt DBA.
[56] Særligt instruksen vil udgøre en vigtig del af vurderingen, da databehandleren således vil være underlagt at handle på vegne af den dataansvarlige.
[57] 'Vejledning om dataansvarlige og databehandlere' Publiceret November 2017 af Datilsynet. Afsnit 3.1.1 Benævnt eksempel 1.

5, stk. 2. Der gælder ikke en tilsvarende pligt for databehandleren, der som udgangspunkt kun er ansvarlig overfor sine egne aktiviteter, jf. art. 32. Netop ansvarlighedsprincippet er en nyskabelse sammenlignet med det tidligere direktiv, hvor denne forpligtelse ikke var kodificeret. Databehandleren er dog uagtet om den dataansvarlige anser en oplysning som persondata, og dermed omfattet, stadig underlagt forordningens regler, hvis oplysningen er omfattet af reglerne. Databehandleren må ligeledes ikke handle efter ulovlig instruks.

Den dataansvarlige skal kunne påvise, at en given oplysning ikke er persondata. Konsekvenserne ved en fejlagtig fortolkning af persondata-begrebet kan i sidste ende medføre bødestraf grundet manglende overholdelse af forordningens øvrige regler.[58]

Ved vurderingen af, hvorvidt en overtrædelse skal medføre bødestraf vil der tages særlig højde for, hvilken viden parterne havde eller burde have, jf. art. 83, stk. 3, litra b og d. Den dataansvarlige er dog underlagt at sikre, at der er tale om persondata, og der er et lovligt behandlingsgrundlag, jf. art 5, stk. 2. Databehandleren er ikke underlagt samme pligter, og der skal ved vurderingen om databehandleren har overtrådt forordningen, tages højde for hvilken viden disse havde eller burde have. Databehandleren må ikke behandle data på en måde der ville være ulovlig i medfør af national ret eller forordningen.

I det omfang databehandleren selv udformer formålene hvormed persondata behandles, indtræder de selv som dataansvarlige for den del af behandlingen – Eksempelvis, hvis data behandles uden for instruks/databehandleraftale. På tilsvarende vis, vil den oprindelige dataansvarlige kunne blive gjort ansvarlig for brud, ved at have overdraget persondata uden hjemmel. Parterne er forpligtet til at indgå en databehandleraftale, jf. art. 28. Databehandleraftalen er det praktiske værktøj, der langt hen ad vejen fordeler ansvar og pligter. Derfor er denne aftale vigtig i vurdering af parternes forpligtelser inter partes, og i et vidst omfang også overfor tilsynsmyndighederne.

[58] Der er ikke I forordningen en regel, der formelt fastlægger sådan en pligt, men den dataansvarlige har i sidste ende ansvaret for at sikre at en given behandlingsaktivitet lever op til forordningens regler.

Databehandlerens pligter følger bl.a. af art. 28, databehandleren er alene ansvarlig for de pligter som forordningens regler retter direkte mod databehandleren, eller hvis databehandleren ikke handler i overensstemmelse med databehandleraftalen, jf. art. 82, stk. 3.

2.5 Den risikobaserede tilgang

Den grundlæggende tilgang til behandling af persondata, sker ud fra en risikobaseret tilgang. Dette kan læses ud af forordningens art. 24 for den dataansvarlige og 32 for både databehandleren og den dataansvarlige. Behandlingen skal ske under hensyntagen til: "…*risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder…*" [59] – Den dataansvarlige skal påvise lovligheden af behandlingen efter art. 24. Bestemmelsen bør læses som en toleddet-test, hvorefter behandlingen skal vurderes ud fra to parametre: (1) sandsynligheden for brud på reglerne og (2) konsekvensen for den registrerede. De to første led udgør behandlingsaktivitetens risiko. Dette er den grundlæggende tilgang for den dataansvarlige for at kunne (3) udføre tiltag, der sikrer, at behandlingen overholder forordningens regler. I forordningens art. 35 fastslås det, at der skal laves en konsekvensanalyse forud for behandlingsaktiviteten, når der er tale om ny teknologi, og der er høj risiko for brud på fysiske personers rettigheder og frihedsrettigheder. Det er den dataansvarliges pligt at efterleve disse regler, der gælder for hele behandlingsaktiviteten.

Artikel 32 gælder både for databehandler og dataansvarlig og regulerer behandlingssikkerheden. For databehandleren gælder den dog kun i det omfang denne er en del af behandlingen. For den dataansvarlige gælder det for alle led i behandlerkonstruktionen på samme måde som art. 24.

Bestemmelserne har et vist overlappende anvendelsesområde, og har den konsekvens, at den dataansvarlige er nødsaget til at formalisere sine processer og overvejelser til brug for dokumentation – databehandleren er ikke pålagt at skulle kunne påvise lovligheden, men skal alligevel overholde og

[59] European Data Protection Board har ligeledes revideret tidligere guidelines, vedrørende konsekvensanalyse 'Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)', hvoraf det fremhæves, at den risikobaserede tilgang udgør hele grundlaget for forordningen.

sikre behandlingssikkerheden, jf. art. 32. Art. 5, stk. 2 fastslår, at den dataansvarlige skal kunne påvise lovligheden, hvilket også medvirker til at processer skal formaliseres.

For den dataansvarlige bør det overvejes i det omfang, at der antages databehandlere og underdatabehandlere, at deres forhold, behandling og afhjælpning udgør en stor del af den samlede behandling. Det er vigtigt at kunne dokumentere, hvilke foranstaltninger som der iværksættes hos databehandlerne. Den dataansvarlige bør risikovurdere forud for behandling påbegynder uagtet om pligten udspringer af art. 24 eller 35, jf. art. 5, stk. 2. Da den dataansvarlige i sidste ende er ansvarlig ved overtrædelse efter art. 32 hos en databehandler, hvis den dataansvarlige ikke har risikovurderet. En vigtig distinktion er, at databehandleren skal efterleve sine forpligtelser på samme måde som den dataansvarlige, men er ikke forpligtet til at risikovurdere.

De mest nærliggende måder at øge sikkerhedsniveauet er ved at indrette sine systemer og arbejdsgange så de i det hele taget modvirker misbrug og fejl.[60] Det er klart, at nogle af de største trusler udgøres af 3. mands uberettigede adgang til data i form af hacking/dårlig it-sikkerhed.

Ad (1) Sandsynlighedsvurderingen er langt hen ad vejen en teknisk vurdering, det handler om den konkrete sandsynlighed for at en given konsekvens sker. Det kan være svært at sige noget om, hvor sikre ens systemer er ifm. Hacking og om data er tilstrækkeligt beskyttet mod destruktion/ændringer. Det følger af præambelbetragtning nr. 76, at vurdering skal være objektiv, hvilket kan synes som en omsonst betragtning. Dette sender dog et klart signal til den dataansvarlige om at være påpasselig med at undervurdere risici i forbindelse med behandlingsaktiviteter – Det kan kræve, at den dataansvarlige indhenter eksterne ressourcer til denne vurdering, f.eks. i form af juridiske-/IT-eksperter eller revisorer, da den dataansvarlige i sidste ende er ansvarlig for en fejlagtig risikovurdering, og derved muligvis ikke have stoppet risikofyldte behandlingsaktiviteter. Denne pligt følger ligeledes af art. 32,[61] hvor

[60] Eksempelvis som nævnt i art. 25: ”Privacy by design and default”. Design: hvor det fremgår at software bør udvikles så risici minimeres, f.eks. ved pseudonomisering af data. Default: systemer og organisationer bør handle efter faste principper, f.eks. separation of duties, hvorefter den samme person ikke kan have flere predefinerede roller på samme tid, da der ville være risiko for misbrug.

[61] Artikel 32 regulerer behandlingssikkerheden og udgør en hjørnesten i risikovurderingen. Denne bestemmelse gælder ligeledes for databehandleren. For databehandleren gælder den dog kun i det omfang denne er en del af behandlingen. For den dataansvarlige gælder det for alle led i behandlerkonstruktionen.

behandlingssikkerheden skal afspejle den konkrete risiko. Der er oplistet en række eksempler på, hvorledes sikkerheden kan øges, eksempelvis pseudonymisering/kryptering, genoprettelse af data mv., men den konkrete fremgangsmåde til at opnå dette er ikke yderligere specificeret.

IT-området er dynamisk og præget af en vis usikkerhed. Kravstillerne til hvad der generelt betragtes som god sikkerhed varierer meget på tværs af landegrænser og brancher. Offentlige myndigheder, private aktører m.fl. vil uden tvivl have en holdning til, hvilke risikomomenter en given behandlingsaktivitet er underlagt. Disse aktører må forventes at have stor indflydelse på den fortsatte udvikling af retsområdet, dette kan ligeledes læses ud af art. 32, stk. 3, hvorefter certificeringer efter art. 42 kan indgå som et led, i vurderingen af om behandlingssikkerheden er tilstrækkelig.[62] Det er derfor svært på et givent tidspunkt at sige, hvad sandsynligheden for at der sker et brud, da den teknologiske udvikling sker sideløbende. Det bør nævnes, at menneskelige fejl/forglemmelser indgår som en del af denne vurdering.

Ad (2) Der er i præambelbetragtning nr. 75 oplistet en række situationer der er omfattet af den anden del. Det er navnlig den påvirkning et brud på reglerne medfører for den registrerede. Eksempelvis vil de følsomme persondata typer, betydelige økonomiske eller sociale konsekvenser være momenter, der lægges vægt på. Konsekvensvurderingen går konkret på, hvilken konsekvens brud måtte medføre. Det samme persondata vil i forskellige kontekster, kunne udgøre forskellige konsekvenser for den registrerede. Et tilfældigt CPR-nummer er for så vidt persondata, men er uden yderligere informationer svære at misbruge. På samme måde gælder det, at såfremt alle tænkelige informationer er tilgængelige, så må det forventes at have store konsekvenser for den registrerede. Det er klart, at des mere indgribende en konkret situation er for en registreret, des mere årvågne bør den dataansvarlige agere. I denne vurdering kan og bør der lægges vægt på, om data er egnede til misbrug. Dette er for så vidt den mest simple del af vurderingen.

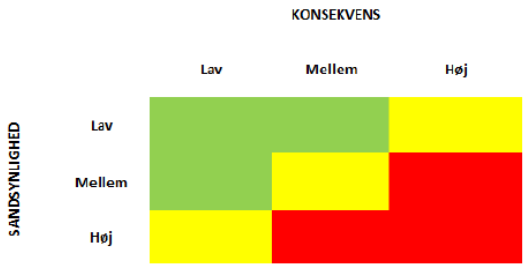
Konsekvens- og sandsynlighedsvurderingen dækker også over om den dataansvarlige/databehandlerne kan efterkomme den registreredes rettigheder, jf. art. 12-22.

[62] Et eksempel herpå er ISAE3000-erklæringerne, der er kommet til i et samarbejde mellem Datatilsynet og FSR. De kan indgå som en del af vurdering af om behandlingsaktiviteten er lovlig, men man skal konkret forholde sig til indholdet.

Ad (3) Det følger af bestemmelsen, at der såfremt det er muligt at nedbringe hhv. sandsynlighed/konsekvens skal den dataansvarlige gøre det, denne pligt følger ligeledes af art. 32. Omvendt er det klart, at der skal tages højde for den konkrete risiko ved behandlingen, da det er denne der styrende for hvor mange foranstaltninger, der skal iværksættes, og hvilket risikoniveau der er acceptabelt. Det er generelt accepteret, at der vil være risiko ved alle behandlingsaktiviteter. Det medfører dog en udfordring i juridisk kontekst at beskrive det lovlige risikoniveau. Det vil kræve et stort overblik over ny teknologi for at leve op til pligten i art. 24 og 32, der ikke er begrænset i tid, men gælder sideløbende med behandlingen.[63] Afhjælpningsmetoden skal være egnet til at minimere de konkrete risici. Et af de tiltag man i praksis kan håndtere sådanne udfordringer, er ved at begrænse mængden af persondata. Man kan indrette sine systemer til ikke at søge i/benytte persondata, da dette alt andet lige nedsætter det samlede risikobillede.[64] Det kan ligeledes være ved at ændre sine arbejdsgange således, at risikoen for menneskelige fejl nedbringes, det kan for eksempel være ved at have stram adgangsstyring, indføre ændringslogs og i det hele taget uddanne sine medarbejdere til at minimere risici. I forlængelse heraf kan der tages højde for det aktuelle tekniske niveau og implementeringsomkostninger, når det skal vurderes, hvilke foranstaltninger, der skal iværksættes. Det konkrete indhold af denne undtagelse er dog i retspraksis stadig uafklaret.

Ifølge datatilsynets vejledning om risikovurdering[65] bør rangeringen ske internt efter et princip om at inddele i forskellige kategorier, eksempelvis efter Lav, Mellem og Høj. Tilsvarende for risikoen for brud. Risikobilledet ved en given behandling kan opsummeres som "$(konsekvensen\ x\ sandsynligheden) - eksisterende\ foranstaltninger = risikoen$". Datatilsynets vejledning inddeler vurderingerne i nedenstående risiko-matrix:[66]

[63] Se mere herom i afsnittet om tilsynsforpligtelsen.
[64] Dette er også fremhævet i forordningens tekst, jf. art. 25 samt art. 5, stk. 1, litra. c.
[65] 'Vejledende tekst om risikovurdering' Publiceret Juni 2019 af Datatilsynet og Rådet for Digital Sikkerhed. Pkt. 4.
[66] 'Vejledende tekst om risikovurdering' Publiceret Juni 2019 af Datatilsynet og Rådet for Digital Sikkerhed. Pkt. 4.4, risikobilledet.



En af de udfordringer, der kan være ved at udarbejde risikovurderingen er, at der på nuværende tidspunkt ikke er fuldstændig klarhed over, hvad der forventes. Der kan være store forskelle i de konkrete konstruktioner, der gør at risikomomenterne er vidt forskellige fra hinanden. Datatilsynet har i samarbejde med FSR[67] udarbejdet en revisionserklæring, ISAE3000, der under pkt. 4 "Kontrolmål, kontrolaktivitet, test og resultat heraf", er en hel række af punkter der kan testes efter for at vurdere de samlede behandlingsrisici – Der er alene tale om en dansk revisionserklæringstandard. Den gennemgår de tematikker man som dataansvarlig må forventes at skulle gennemgå – Den stiller dog også store krav til den part der skal udfylde den. For at den dataansvarlige er fuldstændig sikker på at have afdækket alle risici og bevisovervejelser, skal denne have risikovurderet den samlede behandlerkonstruktion. Den danske standard er ikke en certificering i medfør af art. 42, stk. 8 – der findes ikke nogen på EU-plan på nuværende tidspunkt.[68]

2.6 Databehandleraftalen

Databehandleraftalen[69] er det praktiske redskab, der skal sikre at hhv. dataansvarlig såvel som databehandler, overholder forordningens regler. Det følger af art. 28, stk. 3, at forholdet skal være reguleret af en kontrakt, der som minimum tager stilling til behandlingens genstand, varighed, karakter, formål, typen af data samt den dataansvarliges forpligtelser og rettigheder. Både databehandler og dataansvarlig er pålagt at indgå DBA.

[67] Revisorerklæring udarbejdet mellem Datatilsynet og FSR – Danske Revisorer publiceret d. 8/2 – 2019 til brug for tilsyn med ens databehandlere.
[68] EDPB. 2020. 'Register of certificitaion mechanism, seals and marks'.
[69] I det følgende blot forkortet DBA.

Det vil derfor ikke være muligt at indgå en mundtlig aftale af rent bevismæssige årsager. På samme måde vil rent generiske aftaledokumenter mellem to parter ikke leve op til forordningens krav. Der vil være risiko for, at der ikke konkret er taget stilling til behandlingen. Der er ikke noget tidsmæssigt krav i bestemmelsen, men DBA'en skal indgås senest samtidig med, at behandlingen igangsættes, og efter der er udarbejdet en risikovurdering på behandlingsaktiviteten.

DBA'en reguleres efter det regelsæt, der finder anvendelse for aftalen. Det har ligeledes stor relevans hvilke andre aftaler, der indgås mellem parterne. Det er begge parters pligt at sikre at aftalekomplekset lever op til forordningens regler uanset dens konstruktion, lovvalg og øvrige vilkår.

Det følger af art. 28, stk. 3, litra a, at data kun må behandles efter instruks. Det er den del af aftalen, der langt hen ad vejen implementerer, hvordan databehandler konkret må og skal behandle persondata på vegne af den dataansvarlige. Der er ingen formtvang i forhold til hvordan instruksen indarbejdes i aftalen eller dennes omfang, i Datatilsynets standarddatabehandleraftaler har instruksen indtil videre været placeret som et bilag til DBA'en.[70]

Det er ligeledes i DBA'en, at forhold omkring tilsyn samt udskiftning af underdatabehandlere reguleres inter partes, jf. nærmere herom senere. Det er særligt vigtigt for den dataansvarlige at sikre sig, at DBA'en lever op til forordningens regler. En nærliggende måde at gøre dette på er simpelthen bare at benytte Datatilsynets standard databehandleraftale.[71] Det svenske og norske datatilsyn har vedtaget den danske standard, og der må alligevel være en formodning om, at aftalen ikke vil underkastes nogen egentlig retlig vurdering i de øvrige medlemsstater.[72] Det følger af publiceringen, at datatilsynet ikke vil efterprøve DBA'ens bestemmelser:

> *"I det omfang organisationer vælger at benytte sig af disse standardbestemmelser, vil Datatilsynet, fx i forbindelse med et tilsynsbesøg, ikke efterprøve disse bestemmelser nærmere."*

[70] Denne løsning synes praktisk, da der kan være behov for at give en ny instruks. På den måde kan man blot udskifte et enkelt bilag uden at konsekvensændre hele aftalen.
[71] DBA'en har været sat til gennemgang hos European Data Protection Board. Aftaleudkastet blev givet en række kommentarer og forhold, der var nødvendige at ændre for at aftalen levede fuldstændigt op til forordningen, Se nærmere om EDPB's rolle i EU i det juridiske metodeafsnit samt 'Udtalelse 14/2019'.
[72] Datatilsynet, 2020. 'Datatilsynets standarddatabehandleraftale kan også anvendes i Norge og Sverige'.

På nuværende tidspunkt må det forventes, at brugen af denne standard heller ikke vil føre til retlig efterprøvelse af aftalens gyldighed i andre EU-medlemsstater. Aftalen har været kommenteret og vurderet af det Europæiske databeskyttelsesråd, jf. art. 64, stk. 1, litra d. Se udtalelse 14/2019 på edpb.europa.eu, hvorefter formålet er at tilsikre ens retsanvendelse og harmonisering på forordningens område, jf. art. 70 samt betragtning 1 i den omtalte udtalelse.

Udkastet til den nuværende standard DBA var i første omgang til vurdering hos Det Europæiske Databeskyttelsesråd for at sikre ens retsanvendelse i EU, den afløste den dagældende standard DBA, der blev publiceret i februar 2018.[73] På den måde sikrer det, at der ikke er behov for den dataansvarlige, at have eget kontraktparadigme med den risiko der lægger i, at et tilsyn fra et medlemsstats nationale myndigheder ville føre til, at den indgåede DBA ikke lever op til forordningens regler.

Man kan med rette overveje, hvorvidt den oprindelige standard DBA i det hele taget lever fuldstændigt op til forordningen. Der er en hel del ændringer i den nye som er en direkte konsekvens af at Databeskyttelsesrådets bemærkninger om, at de oprindelige bestemmelser ikke var i overensstemmelse med forordningen. Det oplyses dog, at Datatilsynet vil tage hensyn til tidligere indgåede databehandleraftaler før d. 10/12 – 19. Det har også den betydning, at der for DBA'er indgået efter den dato, at de som udgangspunkt kan måles mod den nyeste version af standard DBA'en. Det danske Datatilsyn kan derfor forventes at arbejde med to forskellige standarder at vurdere databehandleraftalernes bestemmelser før/efter d. 10/12 – 19. Det er ligeledes et åbent spørgsmål, hvilken betydning dette måtte have i relation til de øvrige medlemsstaters praksis, da man ikke uden videre kan antage, at denne danske praksis vil tillægges nogen betydning.

[73] Datatilsynet, 2018, 'Ny skabelon skal hjælpe virksomheder og myndigheder med at blive klar til databeskyttelsesforordningen'.

Overordnede ansvarsfordeling i forhold til risikovurdering og databehandleraftalen:

Den dataansvarlige er pålagt at risikovurdere hele behandlerkonstruktionen og alle de aktiviteter, som databehandlere laver for denne, jf. art. 24 samt art. 5, stk. 2. En tilsvarende pligt gælder ikke for databehandleren. Efter art. 32 er begge parter underlagt at sikre et acceptabelt risikoniveau, for de enkelte databehandlere gælder dette dog kun for egne aktiviteter.

Hvis databehandleren benytter underdatabehandler, skal der være godkendelse fra dataansvarlige, jf. art. 28, stk. 2. Underdatabehandleren skal være omfattet af en aftale, der som minimum sikrer samme pligter som denne selv er underlagt. Der er ikke ansvar hos databehandleren, hvis underdatabehandleren er underlagt samme forpligtelser som sig selv og den dataansvarlige har godkendt dette, jf. art. 28, stk. 4.

Det er den dataansvarliges pligt at sikre sig denne viden inden denne godkender. Modsat risikerer denne at blive ansvarlig for disses fejl, jf. princippet i art. 24 samt art. 5, stk. 2. Hvis den dataansvarliges risikovurdering er korrekt, og der sker en overtrædelse hos en databehandler, så ligger ansvaret som udgangspunkt hos databehandleren. Det bliver i praksis sværere for den dataansvarlige des flere led, der tilføjes da denne er ansvarlig for hele konstruktionen. Der har på nuværende tidspunkt ikke været noget særligt fokus hos de nationale tilsynsmyndigheder at efterse, hvorvidt de dataansvarlige har forholdt sig lige så seriøst til underdatabehandlere og underunderdatabehandlere.[74]

Det er blevet afgjort af datatilsynet, at såfremt en databehandler ikke oplyser, at der benyttes underdatabehandlere, at det er databehandleren der bærer ansvaret, se eksempelvis tilsynsafgørelsen 'Databehandlers behandling af persondata uden for instruks', Publiceret 19-12-2019.[75] Dette flugter i øvrigt med udgangspunktet, hvorefter en databehandler bliver selvstændig dataansvarlig, når denne behandler uden for instruks.

[74] Det må forventes at blive mere udtalt i fremtiden såfremt risikovurdering ligeledes dækker databehandlere i 2. og 3. led, hvilket man må forvente.
[75] Afgørelse vedr. 'Databehandlers behandling af personoplysninger uden for instruks' Publiceret 19-12-2019 af Datatilsynet.

2.7 Den dataansvarliges tilsynspligt

Den dataansvarlige er underlagt en tilsynspligt, hvorefter hele behandlingsaktivitetens lovlighed skal revurderes. Pligten udspringer af art. 5, stk. 2. Den dataansvarliges egne aktiviteter, navnlig i forhold til sikkerhed, vil man kunne løfte ved en virksomheds interne processer. Det kan være svært at vide, hvordan de aktiviteter, der er placeret hos en databehandler, og som den dataansvarlige i et vidst omfang er ansvarlig for, bliver håndteret. I længerevarende forhold er spørgsmålet derfor, i hvilket omfang tilsynspligten, og manglende overholdelse heraf, påvirker ansvarsvurderingen. Det er heller ikke klart, hvor længe risikovurderingen opfylder kravet om ansvarlighed og påviselighed. Der findes ikke praksis vedr. manglende tilsyn fra før indførelsen af forordningen.[76] Overvejelsen omkring tilsynets nødvendighed udspringer netop af påviselighedskravet som ansvarlighedsprincippet udstikker, jf. art. 5 stk. 2. Dette må forventes at kunne afhjælpes på flere forskellige måder: revisorerklæringer, inspektioner, selv-auditering mv.

Overordnede forpligtelse:

Ansvarlighed i art. 5, stk. 2 forudsætter påviselighed. Dette indebærer, at der skal føres en form for tilsyn når det skal vurderes om en databehandlers aktiviteter fortsat er lovlig. Databehandleren har ingen tilsvarende pligt overfor sine underdatabehandlere.

Pligten er enormt bred, forstået på den måde, at der i bestemmelserne ikke er noget krav om hvor ofte dette skal ske, i hvilke situationer, på hvilken måde og i hvilken form. I art. 24, stk. 1, er pligten beskrevet som: *"Disse foranstaltninger skal om nødvendigt revideres og ajourføres."*. Databehandleren skal i DBA'en forpligtes til at hjælpe i forbindelse med tilsyn, jf. art. 28, stk. 3, litra h. Det skal aftales i DBA'en, hvordan og på hvilken måde dette skal ske.[77] Måden den dataansvarlige kan løfte pligten er i DBA'en, ved at sikre sig de relevante rettigheder samt forpligte databehandleren til en række ting, der gør det

[76] Sammenlign evt. formuleringen i databeskyttelsesdirektivet art. 17, stk. 3.
[77] Nogle af de tematikker som ofte er genstand for forhandling vil være formen, omkostninger i forbindelse hermed og hyppigheden. Forordningen skaber ikke nogen pligt for databehandleren til at lade sig tilsynsføre, det gør kun aftalen. Virkninger af manglende efterlevelse af tilsyn vil følge af den samlede fortolkning af aftalen og aftalens lovvalg.

muligt at efterse, at behandlingen er lovlig. Det er et krav, at der i DBA'en skal forpligte databehandleren til at stille alle oplysninger tilgængelige således at kravene i art. 28 kan påvises opfyldt. Der kan ikke være nogen tvivl om, at omfanget af informationer, der potentielt skal kunne leveres, er enormt bred, jf. ordene "*Alle oplysninger*". Oplysninger som ikke direkte er beskyttet af forordningen, eksempelvis forretningshemmeligheder, kildekoder mv., må antages at kunne beskyttes af en NDA.[78] Det er derfor svært uden videre at fastslå, hvad der kræves for at overholde ansvarlighedsprincippet. På den ene side skal ansvarlighedskravet sikre beskyttelse af persondata, jf. art. 1, stk. 1, mens det på den anden side heller ikke må indskrænke den fri udveksling af persondata i EU, jf. art. 1, stk. 3.

Det er langt fra ualmindeligt, at en databehandler enten helt eller delvist benytter sig af underleverandører, der får adgang til persondata. Dermed fungerer disse som underdatabehandlere. Det er ingen grænser for, hvor mange databehandlere eller hvor mange underdatabehandlere disse må benytte sig af. Pligten til at føre tilsyn omfatter for den dataansvarlige alle led i kæden. De få afgørelser der har været afsagt herom, er danske. Se eks. afgørelse om tilsyn i Viborg Kommune,[79] hvor kommunen slet ikke havde ført tilsyn med en række databehandlere og ingen af deres underdatabehandlere, hvilket gav grundlag for at udtale kritik.

Det vil derfor ikke være tilstrækkeligt for dataansvarlige blot at skrive i aftalen, at databehandleren har ansvaret at føre tilsyn med sine underdatabehandlere – den dataansvarlige ville i så fald efterspørge dokumentation for dette. Der er ikke nogen mulighed rent aftaleretligt at aftale ansvaret. Den ene part kan godt hæfte for den anden part, men det vil være som et regreskrav for eksempelvis en bøde. Der kan ligeledes være visse praktiske problemer, eftersom den dataansvarlige ofte i meget ringe grad har samme kontraktuelle rettigheder til at tvinge en underdatabehandler til at lade sig underkaste tilsyn. Tilsynet bør derfor ske igennem databehandleren som så skal stille det til rådighed for den dataansvarlige.

[78] Non Disclosure Agreement (Fortrolighedsaftale): formålet med en sådan aftale er at sikre at oplysninger der deles mellem to parter ikke må bruges til andre formål end de angivne.
[79] 'Tilsynsafgørelsen vedr. Viborg Kommune', publiceret d. 5/8-2019 af Datatilsynet – For yderligere om sagen se litteraturlisten.

Pligtens indhold og form:

Der er i forordningen ingen krav til form eller måden hvorpå tilsyn skal ske. Det er intet i vejen for at tilsyn kan ske telefonisk, fysisk eller skriftligt. Det bør dog generelt overvejes de bevismæssige konsekvenser, da princippet om ansvarlighed ligeledes kræver, at den dataansvarlige kan påvise at tilsynet bekræfter, at reglerne er overholdt. Det er netop kravet om at kunne påvise, der skaber tvivl om, hvorvidt et mundtligt tilsyn helt generelt opfylder ansvarlighedsprincippet. Det må antages, at skriftlighed på samme måde som en lydfil indeholdende en samtale vil kunne opfylde kravet om påviselighed. I datatilsynets vejledning om tilsyn,[80] nævnes de fysiske hhv. skriftlige tilsyn. Der lægges vægt på at tilsynet skal tilrettes risikomomenterne, det vil sige, hvis egentlig tilsyn kræver et fysisk besøg så bør denne fremgangsmåde vælges. På det mere generelle plan kan det dermed sammenfattes, at de to hovedkrav som tilsynet skal kunne opfylde er, at det skal være egnet og kunne påvise, at reglerne overholdes. Dette flugter med den risikobaserede tilgang.

En anden vigtig overvejelse er, hvor ofte der skal føres tilsyn samt, hvorvidt der findes situationer, hvor det ikke er nødvendigt. Der kan ikke ud af forordningen læses nogle krav om tid/hyppighed. I datatilsynets vejledning, er det deres holdning, at hyppigheden styres af risikoen, forstået på den måde, at des højere risiko des oftere skal der føres tilsyn. Det taler ligeledes for, at oftere at føre tilsyn, hvis risikobilledet er ændret i forhold til den oprindelige risikovurdering. Som et eksempel på de situationer, hvor det skal gøres ofte er 6 måneder. På de behandlingsaktiviteter, hvor risikoen er mere beherskede kan det ske årligt, og ved lav risiko kan det ske sjældnere. Det er værd at bemærke, at der ikke findes nogen fælleseuropæiske afgørelser, vejledninger/tilsynsafgørelser fra andre medlemsstater, der omhandler netop dette, hvorfor disse spørgsmål langt hen ad vejen stadig er uafklarede.

Det synes dog logisk, at tilsyn ikke er meningsfyldt, når der er lavet en risikovurdering og behandlingsaktivitetens varighed er under i hvert fald et halvt år. Hverken Datatilsynet eller den

[80] 'Vejledende tekst om tilsyn med databehandlere og underdatabehandlere' Publiceret Maj 2018 af Datatilsynet.

praksis,[81] der har været har på nuværende tidspunkt taget stilling til de intervaller som den dataansvarlige skal iværksætte tilsyn af sine databehandlere.

Indholdet af tilsynet afhænger i høj grad af de identificerede risikomomenter. Baggrunden for tilsynet bør være den risikovurderingen, altså en prøvning af om der er sket nogen ændringer i risikobilledet sammenlignet med det oprindelige ved aftaleindgåelsen.

Den dataansvarlige skal reagere, hvis tilsynet viser, at risikoen findes at være højere end det passende niveau. Det fremgår ligeledes, at adfærdskodekser/certificeringsmekanismer som omhandlet i art. 42 kan indgå som en del af overholdelsen af art. 32. Det har dels den betydning, at det forhåbentligt vil blive lettere at påvise for den dataansvarlige, at ens databehandlere overholder visse sikkerhedsmæssige minimumsstandarder – Der findes dog ingen på nuværende tidspunkt.[82] Selvom, der eksisterer eksempelvis ISAE3000-erklæringer, er det i praksis en udfordring, at erklæringerne kan være dyre at få udarbejdet. Særligt, hvis kontraktværdien er af beskeden størrelse. Efter art. 32 kan der lægges vægt på det nuværende tekniske niveau samt implementeringsomkostninger ved vurderingen af hvad der er et passende sikkerhedsniveau, dette har en betydning for, hvad den dataansvarlige skal iværksætte efterfølgende, men har ikke nogen betydning i forhold til pligten at føre tilsyn.

Det ville stride imod forordningens formål at føre tilsyn efter sine leverandørers forhold. Forstået på den måde at stille lavere krav, fordi databehandlerens generelle modenhedsniveau er lavt. Da retten til at føre tilsyn alene følger af DBA'en bør den dataansvarlige være opmærksom på, at kontraktens fortolkning og lovvalg har indflydelse på, hvorledes kontrakten må forstås. Omkostninger ved et tilsyn er, hvis det ikke fremgår af aftalen efter dansk ret som udgangspunkt, at hver part bærer egne omkostninger.

[81] Der har været to tilsynsafgørelser fra det danske Datatilsynet vedr. Randers og Viborg kommune, der har efterprøvet forpligtelsen – For yderligere om sagerne, se litteraturlisten.
[82] EDPB. 2020. 'Register of certificitaion mechanism, seals and marks' og EPDB. 2020. 'Register for Codes of Conduct, amendments and extensions'.

Praksis og fremtidig udvikling:

Der er på nuværende tidspunkt afsagt to afgørelser vedrørende pligten til at føre tilsyn. Der er heller ikke nogen verserende sager ved EU-domstolen, der kan forventes at bidrage væsentligt til forståelsen af denne forpligtelse. Der er afsagt to tilsynsafgørelser mod hhv. Randers og Viborg kommune, hvor der alene blev fastslået at der var kritisabelt, at der ikke var ført tilsyn.[83] Som tidligere nævnt blev der i løbet af 2019 givet respons fra EDPB[84] på datatilsynets standarddatabehandleraftale fra 2018, der var en række kommentarer, bl.a. om tilsynsbestemmelserne i aftalen. EDPB havde ingen kommentarer til, at aftalen foreslår, at der skal føres tilsyn med databehandleren ved et fast interval.[85] I udtalelse 14/2019 blev der i pkt. 43-46 kommenteret på forhold vedr. tilsynet, men disse relaterede sig alene til, hvilke rettigheder den dataansvarlige skulle have, og hvilke forpligtelser databehandleren skulle kunne efterleve. Det vigtige var at sikre, at den dataansvarlige reelt har mulighed at efterse sine databehandlere, og eventuelle underdatabehandlere. Denne ret må ikke indskrænkes, jf. pkt. 44-46. Databeskyttelsesrådet har således alene efterprøvet omfanget af den kontraktlige forpligtelse, der skal sikres i medfør af art. 28, stk. 2, litra h. På det led bidrager udtalelsen ved, at omfanget af tilsynet bliver belyst. På baggrund heraf skal den kontraktlige bestemmelse give ret til et nærmest uhindret tilsyn, hvor den dataansvarlige skal have alle informationer for, at denne del af DBA'en er fuldstændigt i overensstemmelse med forordningen. Hvorvidt en mere indskrænket tilsynsret i eksisterende DBA'er vil medføre krav om at disse tilsynsbestemmelser skal tilrettes synes tvivlsomt. I det omfang, at tilsynsbestemmelsen er bredt formuleret, kan der være udfordringer i rent aftaleretligt perspektiv om hvad databehandleren er forpligtet til at levere. Denne uklarhed vil I dansk perspektiv muligvis betyde, at standardvilkår fortolkes mod koncipisten,[86] og i det omfang, at den kontraktlige forpligtelse er byrdefuld,[87] vil denne formentlig fortolkes på en sådan måde, at kun de nødvendige oplysninger skal stilles til rådighed for den dataansvarlige.

[83] Se mere herom under tilsynsafgørelser i litteraturlisten.
[84] European Data Protection Board, 'Udtalelse 14/2019'.
[85] Parterne kan sagtens aftale andet, men omvendt sender det et klart signal til den dataansvarlige, at disse bør gøre det ved faste intervaller. Se 'Udtalelse 14/2019' på edpb.europa.eu.
[86] Andersen & Madsen, 2012, s. 27.
[87] F.eks. hvis omkostninger til tilsyn må bæres af databehandleren.

Det interessante er, at Databeskyttelsesrådet ikke har kommenteret på forhold vedr. tilsynets hyppighed, indhold eller dets form. Det danske datatilsyn foreslår klart at tilsyn sker med faste intervaller. Om udtalelsen er et udtryk for accept af det danske Datatilsyns opfattelse, er mere tvivlsomt – I persondataretligt regi er der intet i vejen for, at tilsyn sker med en fastsat hyppighed. Omvendt har man heller ikke taget stilling til det ovennævnte, på trods af det havde været gavnligt. Det synes derfor ikke videre klart om tilsynspligten reelt er en pligt, eller en rettighed som den dataansvarlige kan gøre brug af når eksempelvis behandlingsrisikoen vurderes til at være høj, eller der er ændrede omstændigheder.

Om den vedtagne DBA sender et signal til den dataansvarlige om, at der skal føres tilsyn, synes der ikke at være tvivl om. Om de øvrige landes datatilsyn deler denne opfattelse, virker ikke klart. Sammenligner man de informationer, andre tilsynsmyndigheder stiller til rådighed, synes det ikke åbenlyst, at der indtages samme holdning. ICO[88] oplyser på deres hjemmeside, at rettigheden i art. 28, stk. 3 litra h, alene fastsætter, at databehandleren skal forpligtes til at kunne stille en række oplysninger til rådighed for den dataansvarlige. ICO lægger sig dermed tæt op ad databeskyttelsesrådets 'Udtalelse 14/2019'.[89] De nævner dog, at tilsyn ("*Audits*") kan være en måde at udvise overholdelse af ansvarlighedsprincippet.[90]

Den fremtidige udvikling må ventes med spænding, da der på nuværende tidspunkt ikke er grundlag for at sige meget med sikkerhed, før man reelt ser praksis forme sig i EU. Det vil dog næppe være efter forordningens formål, at den dataansvarlige slippe for at føre tilsyn når behandlingsaktiviteten strækker sig over en længere periode og behandlingsaktiviteterne er risikofyldte, uagtet om der var noget ved den oprindelige behandlerkonstruktion, der gav anledning til at efterprøve dennes lovlighed, jf. art. 28, stk. 3, litra h.[91]

Hvis en behandlingsaktivitet strækker sig eksempelvis over 5 år, er det ikke klart om dette medfører en pligt til at føre tilsyn for den dataansvarlige. Det er heller ikke klart, hvilken form for sanktion dette

[88] De britiske datatilsynsmyndigheder.
[89] ICO. 2020. 'What needs to be included in the contract?'.
[90] ICO. 2020. 'Accountability and governance'.
[91] Netop påviselighedskravet påhviler den dataansvarlige, der derfor skal kunne bevise overholdelsen af reglerne.

potentielt kan medføre, samt hvilken betydning risikovurderingen har i denne sammenhæng. Særligt, hvis forholdene i risikovurderingen stadig er relevante og korrekte. Det er interessant at se, hvorvidt den dataansvarlige vil kunne blive gjort ansvarlig for, ikke at kunne påvise at behandlingen til stadighed er lovlig – her er det navnlig afgørende, hvad der forstås ved "*påvise*" i og med, at der ikke er nogen begrænsning i tid efter art. 5, stk. 2. Sagt på en anden måde: Hvor lang tid risikovurdering kan forventes at være tilstrækkelig dokumentation.

Hvis databehandleren ikke efterlever sine forpligtelser, kan det muligvis stadig medføre bødestraf eller sanktioner i medfør af art. 58 for den dataansvarlige, for manglende efterlevelse af art. 5, stk. 2, jf. art. 83, stk. 5. Der er simpelthen ikke nok praksis til på nuværende tidspunkt at kunne sige, hvad der forventes af den dataansvarlige vedr. denne forpligtelse, og hvorvidt manglende efterlevelse kan medføre en potentiel bødestraf/ansvar for databehandlerens manglende overholdelse af forordningens regler og efterlevelse af DBA'en.

En mere lempelig fortolkning af tilsynsforpligtelsen er, at den dataansvarlige skal efterse egne behandlingsaktiviteter og revurdere sine databehandlere samt risikovurderinger. Hvis der på baggrund af en sådan gennemgang viser, at det eksisterende setup muligvis ikke er tilstrækkeligt, vil der skulle handles på denne viden og tages skridt mod at kunne udvise ansvarlighed. Dette vil give anledning til at føre tilsyn/iværksætte yderligere foranstaltninger, for på den måde at vurdere om det er nødvendigt at nedbringe risikoen. Databehandleren er underlagt en lignende pligt i art. 28, stk. 3, litra f og art. 32, hvorefter denne dog kun skal efterprøve egne behandlingsaktiviteter.

Det danske datatilsyn er af den holdning, at pligten først og fremmest er en forpligtelse der skal ske uanset om intern revurdering af den samlede behandlerkonstruktion giver anledning hertil. Dette synes støttet til en vis grad af EDPB's accept af den danske standarddatabehandleraftale, der er bygget op omkring periodevise tilsyn, fremfor tilsyn ved behov for justering af de aftalte foranstaltninger/mistanke om manglende efterlevelse hos databehandleren. Risikoen ligger først og fremmest i, at der i EU udvikles en forskelligartet praksis, hvor forskellige nationale tilsyn vil ligge forskellige fortolkninger til grund.

Der er for nuværende kun udtalt kritik i tilsynsafgørelserne mod Viborg Kommune og Randers Kommune,[92] der viste, at kommunernes tilsyn var mangelfuldt eller helt fraværende. I den samlede praksis fra hele EU har der ikke været afsagt andre afgørelser. Om det er et udtryk for, at det ikke er en forpligtelse, er tvivlsomt, når tilsynspligten omfatter en efterprøvelse af om behandlingssikkerheden i art. 32 er overholdt. I de to sager mod hhv. British Airways og Marriot International Inc.,[93] der pr. 13/05-2020 endnu ikke er afgjort, men bødeniveauet forventes at ligge i omegn af hhv. 1,5 mia. DKK og 825 mio. DKK og omhandler netop brud på art. 32.

Brud på tilsynspligten kan på nuværende tidspunkt ikke forventes at medføre bødestraf, men indgår som et moment, hvis der er sket brud på behandlingssikkerheden hos ens databehandler. Det er dog ikke klart på nuværende tidspunkt, hvor stort et tilsyn skal være for udgøre fuldstændig fritagelse for bøde ved brud på eks. art. 32 for den dataansvarlige. Tilsynet må forventes at indgå som et lempende moment efter art. 83, stk. 2.

Der er på nuværende tidspunkt ingen tvivl om, at den dataansvarlige risikerer at blive gjort ansvarlig, hvis denne har viden om, at behandlingen ikke er lovlig hos dennes underdatabehandlere. Det er navnlig det forhold, om tilsynet udvider den dataansvarliges ansvar udover forordningens øvrige regler, og som alene kommer til udtryk i de længerevarende databehandlerforhold, hvor der muligvis skal tilsynsføres. I overensstemmelse med formålet, er det i højere grad den enkelte behandlingsaktivitets særegne kendetegn, der bør være styrende for hvilke tiltag, der benyttes.

Udskiftning af og kontrol med underdatabehandler i relation til tilsynsforpligtelsen

Efter art. 28, stk. 2 må databehandleren ikke udskifte sine underdatabehandlere, medmindre den dataansvarlige har givet et specifikt samtykke efter henvendelse eller en mulighed for indsigelse ved et generelt samtykke fra den dataansvarlige. Det bør antages, at indsigelse alene kan ske, hvis dette er sagligt begrundet, der er dog ikke nogen krav i bestemmelsen om hvilke kriterier der skal være opfyldt.

[92] For mere om tilsynsafgørelserne se litteraturlisten.
[93] ICO. 2019: '*ICO announces intention to fine British Airways £183,39m under GDPR for data breach*' og ICO. 2019: 'Statement: *Intention to fine Marriot International, Inc more than £99 million under GDPR data breach'*.

Der må dog ikke være tale om en ren proforma bestemmelse, hvor den dataansvarlige reelt ikke har nogen mulighed for at reagere. Der er på nuværende tidspunkt intet i vejen for, at den dataansvarlige kan blokere for en udskiftning af rene forretningsmæssige årsager. Denne pligt gælder for alle databehandlere, hvorfor det bliver sværere for den dataansvarlige at kontrollere des flere led, der er i behandlerkonstruktionen - på samme måde som det er tilfældet med risikovurderingen og tilsynet i øvrigt. I forbindelse med tilsynet og ansvarlighedsprincippet bør den dataansvarlige sikre sig, at der ikke er sket ændringer i behandlerkonstruktionen. Den dataansvarlige skal reagere, hvis der er sket ændringer i risikobilledet. Hvis dokumentationen fra databehandleren ikke er tilfredsstillende, bør det overvejes, hvorvidt behandlingsaktiviteten bør indstilles.[94]

[94] Der kan dog være visse aftaleretlige overvejelser omkring, hvad virkning af dette måtte være.

2.8 Juridisk Delkonklusion:

Den grundlæggende ansvarsstruktur er sådan, at den dataansvarlige er ansvarlig for hele behandlingsaktiviteten, jf. art. 5, stk. 2. Det er ligeledes den dataansvarliges ansvar at sikre sig om der er tale om persondata. De enkelte databehandlere er ansvarlige for egne behandlingsaktiviteter. Det er vigtigt for denne, at der behandles inden for instruks. Hvis databehandleren iværksætter sine egne behandlingsaktiviteter med egne formål, vil denne agere som dataansvarlig med de forpligtelser dette medfører. Den grundlæggende tilgang til lovlig behandling af persondata er den risikobaserede tilgang, jf. art. 24, stk. 1 og art. 32, stk. 1. Der skal herefter iværksættes passende foranstaltninger, der modsvarer den konkrete risiko for, at behandlingssikkerheden og forordningens øvrige regler ikke overtrædes. Det er fastslået at sandsynligheden for brud som ovenfor nævnt og den konsekvens dette medfører for de(n) registrerede er behandlingens risiko. Dette udgør udgangspunktet for den dataansvarliges pligt til dels at risikovurdere, men udgør også udgangspunktet for opfyldelse af ansvarlighedsprincippet.

Tilsynet udspringer af påviselighedskravet og af art. 5, stk. 2. Man har fra databeskyttelsesrådet taget stilling til, hvilke rettigheder man bør have som dataansvarlig i DBA'en. Det virker dog mere tvivlsomt om databeskyttelsesrådet reelt anser tilsynet som en pligt, der medfører en regelmæssig revision hos ens databehandlere. Dette er i hvert fald det danske datatilsyns holdning og praksis. Spørgsmålet er dog, om manglende tilsyn i længerevarende behandlingsaktiviteter potentielt kan medføre bøde for den dataansvarlige i situationer, hvor databehandleren ikke efterlever sine forpligtelser, og der ikke var noget der gav anledning til at iværksætte en revision af databehandleren. Det er dermed ikke sikkert om vi har en tilsynsregel som det danske datatilsyn foreslår, eller om reglen i højere grad skal fortolkes i overensstemmelse med den risikobaserede tilgang, hvorefter ansvarlighedsprincippet i højere grad opfyldes alt efter den konkrete risiko og behandlings karakteristika. Det er heller ikke klart om manglende tilsyn potentielt kan medføre ansvar for brud hos databehandleren. Det er på nuværende tidspunkt ikke ganske klart om, der kan tages mindre tiltag i brug for at opfylde ansvarlighedsprincippet, en vigtigt grund hertil er, at forordningen alene har været i effekt i godt og vel 2 år, hvorfor problemstillinger vedr. forsat overholdelse endnu ikke er kommet til udtryk i retspraksis.

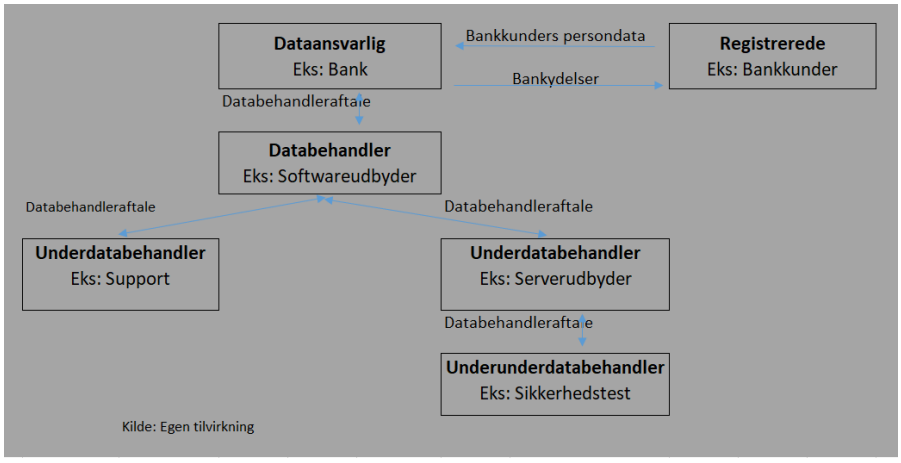
Kapitel 3 - Økonomisk analyse

Det grundlæggende ved den økonomiske analyse er, at der søges at fastholde det samme beskyttelsesniveau samt reducere transaktions- og overholdelsesomkostninger for spillerne. Der vil i den økonomiske analyse lægges vægt på, de pligter og rettigheder som udspringer af persondataforordningen som gennemgået i den juridiske analyse. Først vil den generelle ansvarsstruktur analyseres, samt de incitamenter som parterne har. De enkelte ligevægte vil analyseres under de angivne omstændigheder. Der vil i den sidste del af den økonomiske analyse være særligt fokus på tilsynsforpligtelsen, og ansvarsallokering for de to forskellige fortolkninger af retstilstanden vil medføre. Disse ligevægte vil sammenlignes, og den optimale tilstand udledes.

3.1 Overordnede ansvarsstruktur:

Den grundlæggende ansvarsstruktur kan beskrives på den måde, at parterne kun bliver gjort ansvarlige for egne brud på reglerne.[95] Det har den betydning, at bødeudstedelser er rettet mod den, der har overtrådt reglerne. Parterne har mulighed for at aftale efterfølgende skadeløshed, dette vil dog forudsætte likvide midler.

Et eksempel på en databehandlerkonstruktion kunne være som her:



[95] Se et eksempel på en databehandlerstruktur nedenfor.

De omkostninger der afholdes ved tidspunkt 0 antages at gå til den risikovurdering, den dataansvarlige skal foretage for at kunne dokumentere, og bevise at hele konstruktionen behandler persondata lovligt, og i øvrigt lever op til visse sikkerhedskrav. Generelt er det sådan at generiske behandlingsaktiviteter,[96] alt andet lige er billigere for spillerne eftersom, der potentielt blot kunne laves én risikovurdering, hvis aktiviteterne er forskelligartede, skal disse tilpasses det enkelte forhold.[97] Der vil derudover også være omkostninger forbundet ved at efterleve et givent sikkerhedsniveau, det antages, at des højere niveau des flere omkostninger.

Parterne er bl.a. underlagt at indgå en databehandleraftale i det omfang en databehandleren behandler persondata på vegne af en dataansvarlig. Den dataansvarlige skal sikre, at den foreslåede behandling er lovlig, og der i øvrigt er et tilpas sikkerhedsniveau hos alle databehandlere. Den grundlæggende tilgang er den, at parterne skal være enige om den fælles handling, dvs. indholdet af aftalen og sikkerhedsniveauet. Parterne kan ligeledes være enige om ikke at efterleve reglerne. Der er lagt til grund, at det ikke kan betale sig 'næsten' at efterleve reglerne. På den måde kan spillet sættes op som en simpel spilmatrix som her:

	Efterlev	Efterlev ikke
Efterlev	(X1, Y1)	(0, 0)
Efterlev ikke	(0, 0)	(X2, Y2)

Kilde: Egen tilvirkning

Det antages generelt at spillernes nyttefunktion kan beskrives som: $0 \leq U(C,P) = C + P$.

Spillerne har altid valget om at udtræde (ikke indgå i spillet), hvorfor spillernes reservationsnytte er lig med 0. Leddet C er de omkostninger, der er ved at overholde reglerne. I det omfang reglerne ikke overholdes udgøres C af den forventede negative værdi, der er for at ifalde bødeansvar ved ikke at overholde reglerne. P er den pengemæssige nytte spillerne får ved samarbejdet og er uændret, uanset

[96] Hvor en leverandør kun leverer en type behandlingsaktivitet.
[97] Det kan f.eks. nævnes at mange revisionserklæringer, der lever op til de krav, der måtte være til dokumentation og overvejelser, starter fra 100.000 DKK for at komme omkring de forskellige kontrolspørgsmål.

om spillerne overholder reglerne eller ej. Eftersom spillerne er risikoneutrale, vil de vælge ikke at efterleve reglerne, hvis der er tilpas lav sandsynlighed og konsekvens ved at blive opdaget.

Omkostninger til at udforme kontrakten, iværksætte sikkerhedstiltag, dokumentere mv. kan være betragtelige, og er derfor ikke ønskelige for spillerne. Modsat modvirker reglerne, at der potentielt sker brud/datalæk til skade for de personer, hvis persondata, der behandles. I økonomisk forstand er det derfor lagt til grund, at den omkostning der er for de personer, hvis persondata behandles, er så stor, at fordelene ved, at de potentielt kunne få bedre/billigere produkter, ikke opvejer denne risiko.[98]

Der er tale om et simultant spil, hvor spillets ligevægt afhænger af en række faktorer som i de næste afsnit vil analyseres. Hvis parterne ikke spiller samme strategivalg, så vil det føre til nedbrud uden nogen omkostninger for parterne. Der vil være særskilte omkostninger forbundet ved at efterleve reglerne, men der vil ikke være nogen særskilte omkostninger ved strategivalget 'Efterlev ikke' på tidspunkt $T = 0$.

Spillet er en tilpasset version af Battle of the Sexes,[99] selvom der er i spillet 'Battle of the Sexes' er to ligevægte ved hhv. X1, Y1 og X2, Y2. I nærværende version af spillet er det muligt at spillet er ens med 'Battle of the Sexes'. Der kan dog være en entydig ligevægt, hvis eksempelvis sandsynligheden for at blive opdaget ikke eksisterer så vil spillerne ikke vælge at påtage sig flere omkostninger.[100] Strategivalget 'Efterlev ikke' vil derfor dominere 'Efterlev' for begge spillere.

Spillerne risikerer at blive opdaget, hvis de ikke efterlever reglerne, der er forskellige sanktioner spillerne risikerer. Der vil tages udgangspunkt i at parterne risikere at modtage en bøde samt, at der foruden bøden vil være en negativ effekt i det marked som spilleren agerer i.[101]

Nedenfor vil den overordnede ansvarsstruktur analysere under de angivne omstændigheder.

[98] Det er derfor lagt til grund at beskyttelsesniveauet skal være uændret.
[99] Dutta, 1999, s. 55.
[100] I 'Battle of the Sexes' er der lagt til grund, at spillerne hver i sær har en præference for hhv. (X1,Y1) og den anden spiller for (X2,Y2), se bl.a. Dutta, 1999, s. 55.
[101] Tab af omdømme, kunder, omsætning mv.

Ansvarsstrukturen:

Den dataansvarlige er ansvarlig for hele konstruktionen og alle de led som efterfølgende tilføjes.[102] De enkelte databehandlere er som udgangspunkt kun ansvarlige for deres egne aktiviteter.

Det må først bemærkes, at den sandsynlighed, der er for at modtage en bøde er 1:1 sammenhæng med antallet af nationale tilsyn.[103] Disse nationale myndigheder har dog begrænsede ressourcer, hvorfor ikke alle ulovlige handlinger vil blive opdaget. De nationale tilsynsmyndigheder vil ligeledes maksimere virkningen af deres indsats. Dette vil de gøre ved fortrinsvist at efterse den dataansvarlige. Eftersom den dataansvarlige skal kunne dokumentere for hele behandlerkonstruktionen, vil man her opfange de databehandlere, der ikke efterlever reglerne. Ved at føre vilkårlige tilsyn kan myndighederne skabe en deterrence-effekt,[104] som kommer til udtryk ved at sandsynlighed for at blive opdaget ved manglende efterlevelse stiger, leddet C bliver dermed større – Dette resultat er i overensstemmelse med tidlige økonomiske teoriers resultat omkring kriminalitet.

De ressourcer som de nationale myndigheder har til rådighed, bliver brugt der, hvor de giver størst effekt. Det vil ved være ved de spillere som har en stor økonomisk volumen, eller som behandler mange persondata. Der vil være en formodning om, at netop disse typer af spillere potentielt kan have en stor skadevirkende effekt. Disse spillere har mange aktiviteter, og må formodes at have store behandlerkonstruktioner – Man kan derfor med nationale tilsyn, opnå at få spillerne til at overholde reglerne.

Dette har flere afledte effekter. Dels har det den effekt, at små spillere ikke har samme risiko for at blive opdaget, hvis de ikke lever op til reglerne. Helt grundlæggende vil der for små spillere, i økonomisk forstand, være et mindre incitament til at leve op til reglerne som følge af en potentiel bødestraf. Grunden til dette skal findes i, at risikoen for at blive opdaget, alt andet lige er mindre end for større spillere. Det er derfor lagt til grund, at der findes to typer spillere: de spillere, der har incitament til at

[102] Den dataansvarlige skal sikre sig at have et overblik over, og kunne redegøre for, dels hvilke behandlinger, der sker, og hvilken sikkerhed disse er underlagt.
[103] De nationale tilsynsmyndigheder efterser om spillerne handler i overensstemmelse med de regler og pligter disse er underlagt.
[104] Se eksempelvis Mark C Stafford's artikel 'Deterrence Theory: Crime', 2015.

overholde reglerne, og de spillere som ikke har. Disse benævnes store hhv. små spillere. Dette betyder, at man kan opdele de grundlæggende spiltyper som herunder:

Grundlæggende spiltyper:

(1) De afledte effekter ved dette er dels, at der findes et spil med to små spillere, hvor der vil være en ligevægt ved (X2, Y2), hvor der er tilpas lille risiko for at blive opdaget.
(2) Derudover findes der et spil med to store spillere, hvor ligevægten findes ved (X1, Y1), da spillerne er udsat for en risiko for at blive opdaget, der gør at det forventede payoff ved manglende efterlevelse er lavere end efterlevelse.
(3) Derudover findes der et spil med en mindre og større spiller, der er identisk med spillet 'Battle of the Sexes', hvor de to ligevægte er hhv. (X1, Y1) og (X2, Y2) – Der vil dog i de fleste spil være en ligevægt, der er mere troværdig end den anden.

I tillæg hertil vil der være flere forhold der har betydning for ligevægten som herunder vil gennemgås.

Databehandler og dataansvarlig:

Helt grundlæggende er ansvarssfæren grundlæggende forskellig for databehandler hhv. dataansvarlig. Det må bemærkes, at databehandlere generelt har et væsentligt mere begrænset ansvar end den dataansvarlige. Sammenholdt med, at de nationale tilsyn fortrinsvis efterser de dataansvarlige, gør det, at databehandlerne alt andet lige er underlagt væsentligt mindre kontrol, hvilket nedbringer risikoen for at blive opdaget for databehandlerne. I relation til ovenstående spil vil det betyde, at mange databehandlere alt andet lige vil være små spillere, og dataansvarlige vil være store spillere.

Små spillere vil ikke have incitament til at overholde reglerne. Det vil være en positiv sammenhæng mellem des flere led der tilføjes i behandlerkonstruktionen, og risiko for at blive opdaget for den dataansvarlige. Det vil sige, at den dataansvarlige helt generelt vil opleve en større risiko des flere led der tilføjes som denne skal kunne redegøre for, og sikre overholder reglerne.

I relation til ovenstående spiltyper vil der altså være en tendens til, at det reelt set er den sidste type (3), der er udgangspunktet, når der er en transaktions mellem en dataansvarlig og en databehandler – Det er også den spiltype, der hedder 'Battle of the Sexes'.

Transaktionsomkostninger:

Ovenstående analyser har dels den betydning, at der ved eksistensen af omkostninger ved at overholde reglerne både er mindre og større funktioner og ydelser som kunne udføres mere efficient i markedet i stedet internaliseres, forstået på den måde at forhandling fører til nedbrud (0, 0).

Dette kan dels ske, da risikoen for at blive opdaget er stor samt, at omkostningerne ved overholdelse er store. I teoretisk forstand vil en given spiller eksternalisere sine aktiviteter indtil det punkt hvor den marginale nytte ved at eksternalisere endnu en ydelse er lig med den marginale nytte ved at internalisere ydelsen.[105] Ved at sænke transaktionsomkostningerne, selv om det bare er marginalt, vil der ske flere eksternaliseringer, der på den måde vil være en Kaldor-Hicks forbedring.[106]

Det er værd at bemærke at efterlevelse af reglerne forudsætter at det kan bevises, at reglerne efterleves. Det betyder, at der skal udarbejdes procesbeskrivelse, notat eller lign., der beskriver visse handlinger. Dermed forudsætter efterlevelse en vis grad af bureaukrati, hvilket medfører omkostninger, der ellers ikke ville foreligge, hvis spilleren ikke var underlagt beviskrav. Spillerne vil formalisere handlinger, der ikke på andre måder kan bevises, når de efterlever reglerne.

Det er ligeledes ikke en urealistisk at antage, at der eksisterer Economy of Scales-effekter[107] i relation til overholdelse af reglerne. Forstået på den måde, at små spillere skal afsætte relativt flere ressourcer i forhold til dennes størrelse og samlede forpligtelser for at efterleve reglerne.[108] Små spillere, der har

[105] Dette flugter med resultaterne fra Coase-teoremet, hvorefter parterne opnår et paretooptimalt resultat, se Hendrikse, 2003, s.66-68.
[106] I Coase-teoremet vil man forstå dette som at payoff øges ved at eksternalisere, hvilket vil medføre flere aktiviteter eksternaliseres.
[107] Christensen & Rasmussen, 2013, S. 170-173.
[108] Viden hos større spillere er muligvis inhouse, processerne er faste og kendte. Det vil formentligt ikke være tilfældet hos en mindre spiller, der langt hen ad vejen skal hente viden og opkvalificeres udefra for at sikre efterlevelse af reglerne.

bedre ydelser end sammenlignelige store spillere, vil selvom, at leddet P er større, have sværere ved at kontrahere med store spillere, da store spillere vil forvente, at reglerne skal overholdes. Det er her lagt til grund, at de spillere, der har tilpas store Economy of Scales-effekter vil komme til udtryk ved, at leddet C er mindre.

De forholdsmæssige større transaktionsomkostninger for små spillere, vil give sig udslag i, at store spillere fortrinsvist indgår aftaler med andre store spillere, da begge spilleres incitament som ovenfor analyseret er det samme og de ender i ligevægten (X1, Y1). For små spillere vil der ligeledes være særskilte omkostninger til efterlevelse af givne sikkerhedsniveau, som store spillere sandsynligvis allerede har afholdt.

Et eksempel på disse effekter kan ses herunder, hvor en given spiller har 4 mulige samarbejdsspillere:

Ved overholdelse af reglerne:

	Spiller 1	*Spiller 2*	*Spiller 3*	*Spiller 4*
Nytte ved aftale	5	5	5	5
Overholdelsesomkostning	2	1,5	1	0,5
Produktionsomkostning	1,75	2	2,25	2,5
Samlet overskud	1,25	1,5	1,75	2

Ved ingen overholdelse af reglerne:

	Spiller 1	*Spiller 2*	*Spiller 3*	*Spiller 4*
Nytte ved aftale	5	5	5	5
Overholdelsesomkostning	2	1,5	1	0,5
Produktionsomkostning	1,75	2	2,25	2,5
Samlet overskud	3,25	3	2,75	2,5

Kilde: Egen tilvirkning

Spiller 1, der ellers kan producere til en lavere omkostning har så store omkostninger til overholdelse, at spillets ligevægt ved overholdelse af reglerne er et samarbejde med spiller 4, der har de højeste produktionsomkostninger. På samme måde vil en lille spiller foretrække spiller 1, da overskuddet er størst her.[109]

Dels kan ovenstående eksempel ligeledes belyse nogle forhold vedr. nye teknologier/løsninger. Ved nye teknologier forstås, at der er lavere produktionsomkostninger, men samtidig også højere overholdelsesomkostninger end tidligere teknologier. Årsagen til dette er, at teknologien skal dokumenteres, beskrives og tilpasses de sikkerhedskrav, der måtte være. Hvis ovenstående eksempel i stedet for spiller 1, 2, 3 og 4 repræsenterer forskellige teknologier, vil dette betyde, at der vil benyttes

[109] Der er i eksemplet ikke taget højde for den forventede omkostning forbundet ved sandsynligheden for bøde ved manglende efterlevelse. Den forventede omkostning skal dermed være mindre end $3{,}25 - 2 = 1{,}25$ for at det er tilfældet, da payoff ved spiller 1 uden overholdelse er ≤ 2.

inefficiente teknologier, hvis reglerne overholdes. Spørgsmålet er, hvilken indflydelse dette har på spillernes incitament til at videreudvikle på teknologier.

Spillerne vil muligvis i højere grad afholdes fra at benytte bedre teknologier, en grund hertil kunne være, at der alt andet lige er behov for, at mange spillere vælger den samme teknologi for på den måde at nedbringe overholdelsesomkostningerne. Dette vil formentlig særligt gøre sig gældende når denne teknologi har en stor grad af aktivspecificitet hos en enkelt spiller, og ikke ville give samme nytte hos andre spillere.[110]

Et relevant spørgsmål er ligeledes, hvilken indflydelse de omtalte Economy of Scales-effekter har på teknologier. Forstået på den måde, at des flere der benytter en given teknologi, des lavere bliver overholdelsesomkostningen. I det omfang teknologien som standard kan tilpasses de sikkerhedskrav, der måtte være så vil der være aftagende overholdelsesomkostninger. På tilsvarende vis, vil spillere, der leverer tilpassede løsninger, ikke opleve disse effekter. Man vil derfor på sådanne markeder se, at der er en tendens til, at der leveres standard-produkter. Disse forhold gør sig gældende for de spillere som har incitament til at overholde reglerne. De spillere som ikke har incitament til at overholde reglerne vil derfor være mere tilbøjelige til at benytte nye teknologier og derfor ikke skele til overholdelsesomkostningerne.

Navnlig det forhold, at spillerne skal vælge den samme strategi, for at kunne eksternalisere en ydelse vil betyde, at store spillere, på en måde skal få en lille spiller til at vælge at overholde reglerne. Alt efter afhængigheder, forhandlingsposition og de øvrige omstændigheder vil parterne fordele omkostningerne imellem sig.

Generelt lever spillet ikke op til forudsætningerne i Coase-teoremet eftersom der eksisterer transaktionsomkostninger. Navnlig det forhold, at en større spiller potentielt kunne overtage flere opgaver fra mindre spillere i en transaktion og på den måde opnå en Kaldor-Hicks forbedring[111] i form af lavere transaktionsomkostninger er en interessant tese, men hvorvidt dette faktisk sker, afhænger af flere forhold. Dels er der visse udfordringer ift. Ansvarsfordelingen, og om denne er mulig, da der i

[110] Hendrikse, 2003, s. 214-215.
[111] Det er generelt antaget at spillerne kan opgøre for tab modspilleren måtte have ved et givent strategivalg.

et vidst omfang kan være ansvar for den andens handlinger – Se mere herom senere. Så foruden den kendte risiko vil en del af den risiko de kan påtage sig være direkte afhængigt af den anden spillers efterfølgende handlinger – Disse handlinger er ukendte for modspilleren.[112]

Derudover har spillernes viden om reglerne også betydning i forhold til, hvordan ansvaret deles. I det tilfælde en lille spiller har dårlig viden om hvilke forpligtelser de skal efterleve, vil disse næppe tage råd/overlade det til den store spiller at udforme kontrakten og ansvarsfordelingen, da den store spiller vil egennyttemaksimerende på bekostning af modspilleren.[113] Det er ikke lagt til grund i analysen, at dette er tilfældet, men kommer i stedet til udtryk ved Economy of Scales-effekter vedr. overholdelse. En af måderne en lille spiller kan undgå dette er ved at opnå viden, f.eks. ved 3. parter eller ansætte eksperter. Løsningen for de små spillere vil være, at de ofte vil vælge 3. parter, da de opgaver de har behov for at få løst, er relativt få. Disse opgaver løses dog til en højere pris end store spillere. Det efficiente udfald ville være, at spillerne fordeler ansvaret derhen, hvor det billigst kan placeres, men dette forudsætter parterne har perfekt viden, og der ikke er forskellige opfattelser af reglen.

Reglen siger, at spillerne skal indgå en databehandleraftale. For at efterleve dette medfører dels nogle omkostninger ved, at denne skal forhandles og udformes.[114] Disse omkostninger ville man i vidt omfang kunne nedbringe ved, at man i stedet lod reglerne gælde direkte i stedet for at reglerne stiller krav om, at de skal fremgå af aftalen, når man nu på EU-plan har formuleret sine krav til aftalen. Kravene er dog ikke entydige, og åbner for at spillerne har mulighed for at fraskrive sig en del ansvar og omkostninger, ved efterlevelse af reglerne og allokere disse til den anden spiller. De vil selvsagt have en interesse i at påtage sig mindst muligt omkostninger og risiko. Spillernes viden er enorm interessant set ift. Coase-teoremet og dens forudsætninger. Coase teoremet forudsætter, at parterne har perfekt viden. I det omfang, at eksempelvis, små spillere ikke har viden om hvad de skal efterleve, vil der være et vidensproblem, hvor den informerede spiller vil udnytte denne bedre viden i spillet. Man vil her risikere

[112] Forhandling medfører dermed ikke altid et efficient resultat efter Coase-teoremet, da der vil være asymmetrisk information.
[113] Det er en antagelse, at spillerne har modsatrettede interesser, navnlig at minimere eget ansvar og transaktionsomkostninger.
[114] Der blev d. 11/12-2019 publiceret en standard DBA af datatilsynet, der har været igennem de Europæiske myndigheder og må forventes at være det klart bedste bud på en fælles Europæisk DBA. På samme måde vil mange af de retlige vilkår være prædefinerede, selvom parterne i øvrigt har mulighed for at aftale andet.

at opnå et resultat, der ikke er Haldor-Hick efficient, hvis den informerede part kunne have overtaget mere risiko ved en lavere omkostning end den uinformerede part. Selv i de spil, hvor reglerne ikke efterleves ville deklaratoriske[115] regler, såsom reglerne vedr. databehandleraftalen, alt andet lige, øge den samlede sikkerhed.[116] På samme måde ville mange parter formentligt langt hen af vejen acceptere disse fælles regler uden videre, og set fra et samfundsperspektiv kunne man formentlig nedbringe de samfundsomkostninger, der måtte være ved forhandling ved et udgangspunkt, der mere minder om 'Battle of the Forms', hvor hver part søger at maksimere egne rettigheder og fraskrive sig ansvar.[117] Selv i de tilfælde, hvor parterne vil efterleve reglerne vil en deklaratorisk regel fastsætte et minimumsniveau som parterne kan fravige i det omfang de har en interesse heri. Man vil på den måde nedbringe transaktionsomkostningerne, og beskyttelsesniveauet ville være det samme. Dette vil ligeledes efterlade rum for, at spillere som ønsker en anden ansvarsfordeling, kan indgå i en værdimaksimerende kontrakt, og lade andre forhold gælde mellem parterne.

Der kan ligeledes være rene forretningsmæssige overvejelser, der kan betyde, at spillerne vil have incitament til at beskytte sine oplysninger på lignende måde, uagtet om de er underlagt reglen eller ej. F.eks. ved at beskytte forretningshemmeligheder mod, at 3. parter uretmæssigt kommer i besiddelse af disse. Her vil nogle spillere muligvis overopfylde sammenlignet med den regel de er underlagt. Dette ville spillerne dog gøre uagtet om de var underlagt reglen eller ej, da dette sikkerhedsniveau i så fald vil være et dominerende strategivalg. På den måde vil bødestraffen ikke øge incitamentet for at overholde reglerne for disse spillere.

[115] Deklaratoriske regler gælder i det omfang parterne ikke har fraveget reglerne.
[116] Dette står i modsætning til det der gælder nu, hvor vilkårene skal fremgå af aftalen og individuelt forhandles.
[117] Ved Battle of the Forms forstås den situation, hvor hver parts standardvilkår er vedhæftet en given aftale og hvorved, der givetvis vil være diskrepans mellem de to sæt vilkår. Se i øvrigt Andersen og Madsen, 2012, s. 73-74.

Informationer ml. spillerne og de nationale myndigheder:

Det er ovenfor antaget, at spillerne ikke vil lyve vedr. en given aktivitet, eller forstået på den måde, at de nationale tilsyn ikke vil have nogen problemer ved at bevise og efterse, hvorvidt reglerne er overholdt.

I virkeligheden baserer myndighedernes tilsyn langt hen ad vejen sig af de informationer som de får under tilsynsbesøg. En spiller kunne potentielt undlade at fortælle, at der sker givne aktiviteter. På samme måde kunne brud på sikkerheden og den påkrævede information blive undertrykt inden den kommer til de nationale myndigheder. Dette er i strid med de regler som spillerne er underlagt.

Sammenhængen mellem behandlerkonstruktionens størrelse og incitament:

Den dataansvarlige skal sikre, og kunne dokumentere samtlige aktiviteter, som ligger hos de enkelte databehandlere. Den dataansvarlige har ikke nogen kontraktrelation, til andre end databehandlerne i 1. led. I det omfang, der er databehandlere i 3. led, så skal sikkerhedskravene føres igennem databehandleren i 1. led som viderefører disse til 2. led, som viderefører til 3. led.

Alene den situation, at der skal ske kommunikation i flere led førend en given handling kan ske, medfører to typer tab, dels transaktionsomkostninger og tidstab. Lige præcis disse forhold berør alle spillere, der er en del af konstruktionen. Des større konstruktion, des større bliver den samlede omkostning. Dels kan det have den betydning at store spillere fortrinsvist vil forsøge at minimere antallet af led, da flere led alt øger den samlede risiko og omkostninger. Små spillere vil formentlig, som analyseret ovenfor, have et begrænset incitament til at overholde reglerne, hvorfor tilføjelse af flere led vil betyde at disses incitament til at overholde reglerne øges.[118]

Disse regler medfører dermed, at flere funktioner internaliseres i stedet for at videreoutsource/købe fra andre spillere i markedet. I tillæg hertil vil spillerne, selvom det er den bedste beslutning på tidspunkt 0, internalisere. I et samfundsperspektiv opnår man dermed ikke de fordele, der kan være

[118] Årsagen hertil skal findes i at opdagelsesrisikoen stiger når der tilføjes flere led.

ved, at specialistvirksomheder har mulighed for at forbedre, og udvikle eksisterende løsninger og teknologi.[119] Dette kan potentielt have en effekt på naturlige monopoler, der ellers i vidt omfang ville have mulighed for at dominere en branche/geografisk område, hvor der er lange forsyningskæder.[120] Dette vil ikke ske i samme omfang, når mange spillere ikke har incitament til at udvikle på eksisterende løsninger.

Der vil i tillæg hertil være et klart incitament for eksempelvis databehandlere i 1. led, at udvælge den billigste løsning hos en databehandler i 2. led, da databehandleren i 1. led ikke hæfter for brud hos sikkerheden i 2. led. Selv en databehandler, der har incitament til at overholde reglerne vil derfor ikke skele til om 2. led overholder reglerne. Dette svarer til, at de fortrinsvist skeler til produktionsomkostningerne, uden at tage højde for overholdelsesomkostninger som tidligere beskrevet. I relation til det tidligere fremhævede spil vil databehandleren vælge spiller 1, selvom det for den dataansvarliges synspunkt burde vælge spiller 4, da dette medfører de samlet set laveste omkostninger ved overholdelse. Det helt afgørende for om, der benyttes den ene eller den anden spiller på tidspunkt $T = 0$ påvirkes af flere forhold. En af de primære årsager til at dette kan være tilfældet er, at databehandleren i 1. led allerede har indgået aftale med 2. led før aftalen, indgås med den dataansvarlige. Dette medfører et samfundstab, da man ville kunne øge efficiensen ved at valget i 2. led skete efter den dataansvarlige skulle vælge spiller i 1. led.

For de databehandlere som ikke har incitament til at overholde i 1. led, vil vælge databehandlere i 2. led, der heller ikke vil overholde reglerne. Dette stiller krav til den dataansvarlige om at sikre sig at behandlingen, der foregår i 2. led, er lovlig.[121] Databehandleren i 2. led, vil have samme incitament som i 1. led, hvorfor den billigste databehandler i 3. led vælges. Det er det forventelige udfald af mange spil – både fordi mange er afhængige af andres ydelser, for selv at kunne levere, og den del af behandlerkonstruktionen er fastlagte før tidspunkt $T = 0$.

[119] Disse forhold er analyseret længere oppe.
[120] I den situation hvor stordriftsfordelene ikke opvejer de overholdelsesomkostninger, der måtte være.
[121] På den måde vil den dataansvarlige kunne opleve, at samtlige led i disse konstruktioner ikke overholder reglerne, og det kan være omkostningstungt at sikre overholdelse i alle led.

Den dataansvarlige vil i sidste ende, af praktiske årsager, have svært ved at efterleve sine forpligtelser, da databehandlere i 2. og 3. led kun kan honorere de dokumentations- og sikkerhedskrav som påkræves til en stor omkostning. Dette vil formentlig også være medvirkende til, at de dataansvarlige, der ikke overholder reglerne alligevel, beholder konstruktionerne så små som muligt, eftersom risikoen for bøder er stigende med antallet af led.

3.2 Tilsynsforpligtelsen og modifikationer til ansvarsstruktur:

Det store spørgsmål som går igen i denne afhandling, er indholdet af tilsynsforpligtelsen. Den dataansvarlige er pålagt at skulle efterse, om databehandlerne til stadighed efterlever reglerne. Det vil sige, at der løbende vil være overvågningsomkostninger, såfremt spillerne ønsker at overholde reglerne. Det er alene den dataansvarlige, der underlagt denne regel, manglende efterlevelse påvirker for så vidt ikke databehandleren negativt. Spillerne risikerer stadig en potentiel bødestraf, hvis de hver især ikke efterlever sine forpligtelser efter tidspunkt 0. De løbende tilsynsomkostninger antages at ske årligt.

Det er navnlig to forhold der er særligt interessante. Først og fremmest er det ikke ganske klart, hvorvidt manglende efterlevelse medfører en potentiel bødestraf, eller om spillerne i alle tilfælde "blot" vil modtage kritik for ikke at efterleve denne forpligtelse. Derudover er det selve indholdet af forpligtelsen, der har en stor indflydelse på hvor store omkostninger er, og hvordan disse kan fordeles. Den forståelse, der er i den juridiske konklusion er, at der er en streng tilsynsregel som beskrevet herefter, hvor den dataansvarlige risikerer at modtage en bøde, på trods af at denne ikke havde den fornødne viden til at kunne reagere herpå.[122] Der vil herunder analyseres de to forskelligartede opfattelser af reglens indhold samt hvordan de forskellige ansvarsovervejelser påvirker udfaldet af spillet. Der vil under hver af de nævnte scenarier for spillerne ikke være tvivl om hvilken regel eller ansvar de er underlagt. Til sidst vil resultaterne sammenstilles og analyseres for på den måde at foreslå en retsstilling, der medfører færrest samlede omkostninger, samtidig med, at reglernes beskyttelsesniveau fastholdes.

[122] Tilsynet er i virkeligheden den proces, hvor den dataansvarlige skal sikre sig den fornødne viden.

Modifikationer til ansvarsstrukturen:

Den grundlæggende ændring er her, at den dataansvarlige her i et vidst omfang risikerer at blive gjort ansvarlig for andres fejl og mangler. Dette harmonerer ikke med udgangspunktet. Denne situation opstår, når spillernes forhold er længerevarende, f.eks. længere end et år. Modifikationen finder derfor ikke anvendelse i det omfang, der er tale om kortere relationer.

Årsagen til, at den dataansvarlige risikerer ansvar på et senere tidspunkt, er navnlig to forhold, dels at reglerne ikke er statiske[123] og dels, at den dataansvarlige på et senere tidspunkt skal kunne bevise og redegøre for, at de aftalte behandlingsaktiviteter rent faktisk udføres som aftalt.

Tilsynet er en forpligtelse, hvorefter den dataansvarlige er underlagt at efterse hele behandlerkonstruktionen. De aktiviteter, som varetages hos den dataansvarlige kan langt hen af vejen klares ved virksomhedens interne processer. Denne problemstilling vedrør for så vidt ikke denne del af analysen, da problemet er behandlet i afsnittet om den overordnede ansvarsstruktur.

Det må først bemærkes, at de samme overordnede overvejelser om spilleren er stor eller lille, for så vidt går i igen i denne del af analysen.

Der må forventes at være forskel i spillernes viden efter tidspunkt 0 – Graden af asymmetrisk information er stigende mellem parterne efter dette tidspunkt. Af denne grund er Principal-Agent-teorien relevant for at analysere tilsynsforpligtelsen.[124] Der er navnlig 3 forhold, der gør sig gældende ved Principal-Agent forhold:

(1) Der skal være en grad af asymmetrisk information,
(2) Der skal kunne genereres et overskud ved at indgå i spillet,
(3) Derudover skal der til sidst være konfliktende interesser for spillerne.

[123] Et eksempel herpå, er at den teknologiske udvikling gør at risikobilledet ændrer sig, det samme gør kravene til beskyttelse af persondata. Derfor er holdningen, at det ikke er nok, at den dataansvarlige sikrer overholdelse på tidspunkt 0, men skal sikre overholdelse i hele behandlingens varighed.
[124] Hendrikse, 2003, s. 91.

Disse betingelser vil være opfyldt i spillet 'Battle of the Sexes'. Visse store spillere, der agerer som databehandlere, vil formentlig stille generiske dokumenter/revisionserklæringer til rådighed.[125] På den måde kan man minimere egne omkostninger til at dokumentere tilsyn. For disse virksomheder vil omkostningerne ganske vidst være store, men forholdsmæssigt vil disse være større for små virksomheder.[126] Disse dokumenter skal dog udarbejdes årligt og opdateres, i disse situationer vil der for så vidt ikke være tale om et problem i Principal-Agent-teoretisk forstand, eftersom spillerne ikke nødvendigvis har afvigende interesser. Her vil principalen kunne forudsige agentens adfærd, og denne adfærd er ønskelig for Principalen. I PA-teorien er der grundlæggende to problemstillinger man behandler, Adverse Selection og Moral Hazard.[127] Adverse Selection omhandler agentens type, som analyseret under den overordnede ansvarsstruktur sondres der mellem små hhv. store spillere. Moral Hazard-udfordringerne relaterer sig til de handlinger som agenten træffer efter kontraktens indgåelse, og som principalen kun kan få viden om ved at monitorere, føre tilsyn. I nærværende analyse er det først og fremmest Moral Hazard-overvejelser som er relevante eftersom spillernes type er kendt.

I nærværende spil vil der være tale om et sekventielt spil, hvor parterne først vælger under den overordnede ansvarsstruktur enten at efterleve, eller ikke at efterleve reglerne. Efterfølgende sker handlinger hos agenten, som principalen så kan vælge at monitorere, hvis principalen vælger ikke at monitorere, er der risiko dette opdages af de nationale myndigheder. Hvis reglerne ikke efterleves på tidspunkt 0, så vil der ikke føres tilsyn. Reglen siger, at principalen skal sikre, at agenten overholder reglen. Principalen skal få agenten til at sikre sig at underdatabehandlere, [128] handler i overensstemmelse med reglen. I det tilfælde der er en underunderdatabehandler, skal tilsynet føres gennem underdatabehandleren. På den måde minder denne konstruktion om den man finder i mange virksomheder, hvor virksomhedens ledelse er agent for bestyrelsen som er principal. Der er ligeledes et lag under, hvor de ansatte er agenter, hvor ledelsen er principal.[129]

[125] Disse spillere vil formentlig ikke være små spillere og der vil derfor ikke være konfliktende interesser for spillere.
[126] Som tidligere beskrevet er der Economy of Scales-effekter til stede i relation til dokumentation og sikkerhed, disse gør sig gældende på samme måde i nærværende situation.
[127] Hendrikse, 2003, s. 95-96.
[128] Herefter benævnt agentens agent.
[129] Hendrikse, 2003, S. 99.

3.3 Tilsyn under en streng eller lempelig tilsynsregel?:

Den strenge tilsynsregel:

Under den strenge tilsynsregel gælder det, at tilsynet først og fremmest kræver, at den dataansvarlige involverer sine databehandlere. Fokus er rettet væk fra en selv. På den måde kan manglende tilsyn betyde, at den dataansvarlige kan blive gjort ansvarlig, for ikke at have efterlevet sine forpligtelser.[130]

Spillernes viden har under denne regel en reel betydning for, hvorvidt den dataansvarlige potentielt pådrager sig ansvar. I det omfang databehandlerne overholder sine forpligtelser, vil den dataansvarlige alene risikere at modtage kritik for ikke at udføre tilsyn. På trods af at kritikken har økonomiske konsekvenser, må disse dog antages at være begrænsede sammenlignet med bødeforlæg. Af disse grunde minder dette setup om de klassiske Principal-Agent-problemstillinger som beskrevet ovenfor.[131] Denne version af reglen er en udvidelse af principalens ansvar sammenlignet med den generelle ansvarsstruktur.

Derfor kan principalen ved at føre tilsyn, slippe for enhver usikkerhed vedr. sanktioner. Omvendt vil principalen vælge at gøre det på alle eller ingen agenter, eftersom de vil modtage en sanktion i det omfang, at blot en af omtalte agenter ikke er blevet udført tilsyn med. Uanset valget af tilsynsregel risikerer principalen at blive gjort ansvarlig, hvis denne ikke iværksætter tilsyn, eller såfremt der er mistanke om manglende efterlevelse hos agenten.

Den lempelige tilsynsregel:

Den lempelige tilsynsregel medfører, at der vil være ansvar for principalen i det omfang, denne ikke reagerer på viden denne spiller har. Det skal forstås sådan, at tilsynet alene skal ske, hvis der er noget af det tidligere oplyste af agenten, der giver anledning hertil. Dette lægger derfor tæt op ad den generelle ansvarsstruktur som tidligere beskrevet. Dels forudsætter dette, at principalen først og

[130] Der vil herunder tages højde for de forskellige sanktioner som en spiller risikerer at modtage.
[131] Hendrikse, 2003, s. 91.

fremmest foretager en intern gennemgang, hvilket alt andet lige er mindre omkostningstungt sammenlignet med den strenge regel. Hvis der er noget i den eksisterende konstellation, der ikke længere er lovligt, eller i øvrigt giver anledning til, at der muligvis kan være noget der skal afklares, så bør der føres tilsyn. Det skyldes, at agenten er ansvarlig for sine egne aktiviteter samt, at reglen som de er underlagt, ikke er statisk, men derimod ændrer sig med tiden. Agenten er underlagt selv at skulle kommunikere tilbage til principalen ved ændringer, der kan påvirke lovligheden – Dette er en generel regel.

Dels har det den betydning, at de tidligere beskrevne PA-overvejelser ikke kommer til udtryk i samme omfang. Principalen kan under denne regel til en langt lavere omkostning efterleve sine forpligtelser. De enkelte agenter har ligesom det er tilfældet under den strenge regel, et selvstændigt ansvar til at tilrette sine aktiviteter, og meddele til principalen ved ændringer. Denne ansvarsstruktur minder om den generelle ansvarsstruktur som tidligere beskrevet. Der er tale om et PA-problem, men de lavere omkostninger for principalen gør, at problemets omfang bliver mindre, da det må antages at flere principaler vil afholde disse omkostninger sammenlignet med reglen under strengt tilsyn. Omvendt har dette muligvis en betydning for agenternes incitament, og hvorvidt de vil overholde deres forpligtelser, altså om den samlede beskyttelse er lavere sammenlignet med den strenge tilsynsregel.

Denne tilsynsregel gør, alt andet lige, at Principalen alene vil føre tilsyn når der er anledning hertil og PA-problemet bliver derfor mindre udtalt. Uanset valget af tilsynsregel, risikerer principalen at blive gjort ansvarlig, hvis denne ikke iværksætter tilsyn, hvis der er mistanke om manglende efterlevelse hos agenten.

3.4 Konsekvens ved manglende efterlevelse - kritik:

Det er grundlæggende, at de eneste sanktioner, der på nuværende tidspunkt har været ved manglende efterlevelse af tilsynsforpligtelsen været udtalt kritik.[132] Der vil her lægges til grund, at kritik er den eneste sanktion de dataansvarlige-spillere risikerer at modtage. Der må bemærkes, at kritikken alt efter

[132] Se evt. litteraturlisten under tilsynsafgørelser for yderligere.

spillerens størrelse vil blive gengivet i medier samt på det nationale tilsyns hjemmeside. Det vil formentlig have en afskrækkende effekt på de spillere, der jævnligt, f.eks. årligt, er underkastet tilsyn fra de nationale myndigheder, og hvor sådan omtale har en væsentlig indflydelse på deres forretning/omdømme. Det må dog bemærkes, at der ikke er en direkte monetær konsekvens ved manglende efterlevelse, selv hvis reglerne ikke er overholdt hos de enkelte agenter. Principalen vil alt andet lige have svagere incitament til at overholde denne forpligtelse sammenlignet med den overordnede ansvarsstruktur.

Agenten, der som udgangspunkt ikke vil blive underkastet noget tilsyn fra myndighederne, vil have et nærmest ikkeeksisterende incitament til at overholde reglerne, eftersom der som udgangspunkt ikke er nogen, der vil efterse, at reglerne overholdes. På samme måde vil de ikke føre tilsyn længere tilbage i kæden uden principalen på en eller anden måde beder om det.

Under den lempelige tilsynsregel:

Et brud under den lempelige tilsynsforpligtelse medfører kritik, uanset om agenten har efterlevet sine forpligtelser. Der vil som tidligere beskrevet ikke være nogen stor konsekvens ved manglende efterlevelse. Henset til de lavere omkostninger ved overholdelse vil flere principaler overholde denne regel og aktivt forholde sig til de eksisterende aktiviteter.

Det kan ikke forventes, at små spillere vil efterleve reglerne på tidspunkt 0 blot, fordi der er en lempelig regel. Der er generelt en sammenhæng, hvorefter des længere en aktivitet strækker sig, at der er større risiko for opdagelse. Derfor vil det snarere være den generelle ansvarsstruktur, der vil få agenterne til at overholde sine forpligtelser end sanktionen ved manglende tilsyn.

For de store principaler er der to effekter i spil. Agenterne vil umiddelbart på den ene side endnu sjældnere blive mødt med tilsyn, hvorfor man må antage at deres incitament til at overholde, vil være svækket sammenlignet med den strenge regel. På den anden side vil de principaler, der fører tilsyn ske ud fra viden om agentens mulige manglende efterlevelse. De situationer, hvor der således er begrænset risiko, eller man har en klar overbevisning om, at agenten opfylder sine forpligtelser, vil der således ikke

blive gennemført omkostningstunge tilsyn. Der vil kun blive ført tilsyn på de få, hvor der er noget, der giver anledning hertil. Sammenlignet med under den strenge regel vil man se, at der for principalen, vælges konsekvent enten tilsyn eller intet tilsyn. På samfundsniveau er det ønskeligt, at der ikke føres tilsyn med de agenter, der efterlever reglerne. På det led skaber denne regel en incitamentsstruktur for principalen, der er i samfundets interesse i stedet for at påføre principalen en sanktion for et strategivalg, der er i samfundets interesse under den strenge tilsynsregel. Der vil dog være visse omkostninger forbundet ved at foretage en intern vurdering, og konsekvensen er ikke voldsom for principalerne, hvor alene store principaler vil efterleve denne regel.

Under den strenge tilsynsregel:

Eftersom omkostningerne til tilsyn er større end under den lempelige regel, vil der være færre principaler, der sikrer efterfølgende efterlevelse. De principaler, som vælger at gøre, vil dog efterse alle deres agenter. Der vil være et samfundstab eftersom der vil blive ført tilsyn selv med agenter, hvor der reelt ingen risiko er.[133]

Under denne regel vil meget få agenter overholde reglerne foruden den dataansvarlige – Denne incitamentsstruktur er meget lig med den man finder under den lempelige regel.[134] Det bør bemærkes, at den pågældende sanktion vil betyde, at den efterfølgende beskyttelse af persondata, langt hen ad vejen alene vil være mangelfuld mange steder. Dette skyldes, at agenterne ikke realistisk risikerer at blive undersøgt, hvorvidt de har efterlevet reglerne. Hvis agenterne ikke efterlever reglerne, risikerer de bøde, men risikoen er minimal. Principalen vil ligeledes ikke have et stærkt incitament til at efterse, at agenten handler i overensstemmelse med reglen, da konsekvensen er minimal ved manglende efterlevelse for principalen.

Et af de eksempler, hvor der incitament til at efterleve reglen er de helt store principaler, der ikke vil risikere at modtage kritik. Dels vil behandlerkonstruktionerne være mindre, da

[133] Principalen vil modtage kritik, hvis blot, der er en agent, hvor der ikke er tilsynsført.
[134] Det skyldes den svage incitament til efterlevelse, grundet kritik som sanktion.

overvågningsomkostningerne sker årligt. På den anden side vil reglerne efterleves hos principalens agenter, da principalen modsat kan risikere et bødeansvar i det omfang principalen ikke reagerer på de informationer denne modtager.

Sammenfatning vedr. kritik:

På baggrund heraf må det konkluderes, at kritik ikke egner sig som sanktionsvalg. Dels vil sanktionen ved brud være lempeligere end under den generelle ansvarsstruktur, som vil medføre at meget få vil efterleve reglerne. Behandlingssikkerheden kommer dermed under det ønskede niveau, hvorfor denne sanktion medfører inefficiens, uanset hvilken tilsynsregel man har.

3.5 Konsekvens ved manglende efterlevelse - bøde:

Under denne regel vil den nationale myndighed bede principalen om at føre tilsyn, hvis spilleren ikke allerede selv har gjort det. I det tilfælde, at tilsynet viser, at reglerne er brudt hos agenten vil, der være bødestraf. Hvis tilsyn viser, at reglerne er overholdt vil der alene udtales kritik. Det er generelt sådan, at der ved bødestraf tages højde for overtrædelsens varighed. Des længere overtrædelsen har stået på des større bøde, dette er allerede tilfældet under den generelle ansvarsstruktur. Tilføjelsen her er, at der er potentielt, kan være ansvar for agentens handlinger, som er ukendte for principalen, og dermed er konsekvensen væsentligt hårdere end tilfældet er under sanktionen 'kritik'.

Konsekvensen ved manglende efterlevelse hos de efterfølgende led vil dels betyde, at PA-problemet bliver mere udtalt, da konsekvensen ved manglende overholdelse potentielt medfører en bødestraf. Det bør have særlig betydning, hvilken tro principalen har omkring agentens type, og hvorvidt en agents type er statisk over tid: I det tilfælde, at agenten f.eks. skulle blive nødlidende på et senere tidspunkt, og derfor bliver villig til at påtage sig større risiko, ved ikke at overholde reglerne, vil der for principalen alligevel være et behov for at monitorere agentens efterfølgende adfærd. Så selvom principalen har viden om agentens type vil, der være risiko for, under denne regel, at agenten handler anderledes end principalen tror.

Navnlig store agenter vil ikke risikere at modtage en bøde, og dermed overholde sine egne forpligtelser. Tilsyn vil derfor ikke være meningsfyldte at udføre – Principalen vil dermed risikere at få en sanktion (kritik) for ikke at efterleve sine forpligtelser. Under denne regel vil der, alt andet lige, være færre agenter, der ikke efterlever reglerne på et senere tidspunkt sammenlignet med sanktionen kritik. Årsagen til dette skal findes i, at principalens incitamentsstruktur er anderledes.

Det kan være meningsfyldt for Principalen at monitorere agenten, med henblik på om agentens type er uændret. Hvis agenten bliver villig til at påtage sig stor risiko, påvirker dette principalen, også selvom denne ikke er det på tidspunkt 0. Der vil derfor føres tilsyn bredt, også mod agenter som principalen ved overholder sine forpligtelser. I økonomisk såvel som beskyttelsesperspektiv er sådanne tilsyn uønskede, da disse omkostninger, under en optimal tilstand, ikke bør afholdes. Det må bemærkes, at flere principaler vil efterleve reglerne sammenlignet med under sanktionsformen kritik.

Spørgsmålet er derfor om spillerne selv kan afhjælpe dette problem, ved f.eks. at aftale erstatning ved brud hos agenten, for de bøder som principalen heraf måtte pådrage sig, som følge af agentens adfærd. Der kan være flere udfordringer ved dette. Dels kan agenten være illikvid, da denne selv vil blive ramt af en bøde ved brud. Der kan ligeledes være forhold i ejerstrukturen, som gør at selskabet, agenten, ikke vil have øget incitament til at overholde ved at indføre sådan en ansvarsklausul.[135] Små spillere, som ikke bliver konkursramte af en selvstændig bøde, kan et erstatningskrav for så vidt godt ændre deres adfærd i principalens interesse – Man må fortolke det sådan, at leddet C stiger for agenten. Der bør være større sandsynlighed for overholdelse, hvis det kan aftales, at ejerne af agenten bliver ansvarliggjort på samme vilkår som agenten. Dels kan man herved have øget incitamentet for, at agenten overholder reglerne, da den der i sidste ende drager nytte af manglende efterlevelse, selv risikerer at blive ansvarliggjort.[136]

[135] Der er her lagt til grund, at der er tale om et kapitalselskab og ejeren vil have en holdning om, at der i den situation, hvor overtrædelser opdages vil blive illikvid og alligevel ikke kunne betale principalen. Agenten må forventes at agere efter ejerens ønske.

[136] Det er klart, at der findes en række selskabsstrukturer, hvorefter ansvarliggørelse af ejere ikke vil have nogen betydning, da disse selv kan være 'tomme' kapitalselskaber. Derfor kan sådan en løsning ikke løse alle Hidden Action-problemer, men derimod øge incitamentet for overholdelse i nogle tilfælde.

Streng eller lempelig tilsynsregel – Bøde:

Under den strenge regel vil man se, at det forhold, at principalen risikerer at blive gjort ansvarlig selv når denne ikke er vidende herom, udgør et stærkt incitament til at føre tilsyn. Omkostningerne vil blive afholdt af flere principaler end under kritik.

Som tidligere beskrevet vil de principaler, der vælger at føre tilsyn under den strenge regel gøre det på alle deres agenter, hvilket vil medføre betragtelige løbende omkostninger. Dette vil medføre et samfundstab, da mange agenter må forventes at efterleve reglerne. Dette vil ske i et vidst omfang. Særligt for de agenter der udfører typeopgaver for mange forskellige principaler,[137] vil der være et samfundstab, da man reelt set som samfund burde kunne nøjes med ét tilsyn, da principalernes behov for tilsyn er ens.

Der er under den lempelige regel et stærkt incitament for principalen til at efterleve tilsynsreglen. Dels fordi omkostningerne er mindre, og fordi de kun fører tilsyn når omstændighederne tilsiger det. I virkeligheden er tilsynet, under den lempelige regel, kun i spil, når noget giver anledning hertil. Flere principaler vil derfor efterleve sine forpligtelser sammenlignet med den strenge regel, hvilket er ønskeligt. På den anden side vil en række agenter ikke blive ført tilsyn med, eftersom principalen ikke er vidende om manglende efterlevelse. De agenter som oplever ikke at blive tilsynsført, vil ikke efterleve reglerne, fordi sandsynligheden for, at de bliver opdaget således, er minimal. Der må derfor, for at opretholde det samme beskyttelsesniveau, som under den strenge regel, i tillæg til den lempelige regel iværksættes yderligere tiltag, for at sikre det samme beskyttelsesniveau.

En af måderne hvorpå man kan gøre dette, ved at se på, hvad den reelle forskel på de to regler er. I virkeligheden er en af de vigtige forskelle på den strenge og den lempelige regel, at de nationale myndigheder overlader kontrolopgaver til principalen. En af årsagerne til, at det efficiente resultat i økonomisk teori omhandlende kriminalitet[138] netop ikke foreslår at tilsynsføre alle, er det kan have en afskrækkende virkning blot at gøre det nogle gange. Med den strenge regel risikerer man, at de samlede

[137] Et eksempel herpå ville være Microsoft Azure, der er en platform, hvor der kan udvikles og leveres services og hvor der er enorme mængder persondata, der er beskyttet på den samme grundlæggende måde.
[138] Se eksempelvis Mark C Stafford's artikel 'Deterrence Theory: Crime', 2015.

omkostninger til overholdelse bliver højere end det efficiente niveau.[139] I virkeligheden vil man, ved i højere grad at overlade vilkårlige tilsyn til de nationale myndigheder kunne opnå et mere efficient resultat. Principalen vil ikke kunne opnå samme afskrækkende virkning, men skal derimod tilsynsføre altid, ellers ved agenten at denne ikke vil gøre dette. At en given principals tilsynsførende handling skaber nogen effekt i andre spil, end netop denne interaktion synes ikke realistisk. De nationale myndigheders tilsyn er som tidligere forklaret ved spilleren natur, de er altså ubekendte for alle spillere og rammer vilkårligt. Af den grund må man forvente, at der ved at tilsynsføres blot en gang mere øger sandsynligheden for, at en tilfældig spiller udvælges – disse tilsyn vil derfor påvirke både den tilstand på tidspunkt 0, hvor spillerne vælger strategivalg, men også ift. den efterfølgende overholdelse. På den måde undgår man, at alle dataansvarlige skal kontrollere sine aktiviteter, men at man i stedet opnår samme virkning ud fra et deterrence-synspunkt. Det må forventes at øgede tilsynsaktiviteter, kan have samme betydning for overholdelsen, som tilsynet under den strenge regel. Dette forudsætter dog, at de nationale tilsynsmyndigheder iværksætter vilkårlige tilsyn mod både principaler og agenter, hvor der ikke er noget, der giver anledning hertil.[140]

Man bør overveje, hvorvidt omkostningerne for principalen er lavere ved tilsyn, end for de nationale myndigheder, eftersom de kender kontrakten og behandlingskonstruktionen. Hvorvidt dette skulle medføre, at det er mere efficient at have en streng tilsynsregel, synes dog alligevel tvivlsomt. Virkningen vil være den samme, og medføre det samme beskyttelsesniveau. Selvom de enkelte nationale tilsyn er mere omkostningstunge end principalens tilsyn, kan dette dog ikke forventes at være i en sådan forskel, at det mest efficiente er den strenge tilsynsregel. Betragt følgende eksempel.

[139] Det efficiente niveau må forventes at være der, hvor sandsynligheden for at blive opdaget og bødeniveauet er tilpas store, at overtrædelse ikke er et dominerende strategivalg for nogen spillere.
[140] Det bør bemærkes, at der ligeledes kan være visse fordele ved at en 3. part håndhæver disse regler, hvis reciprocitet spiller en rolle i spillet 'Battle of the Sexes'. Se mere herom under den integrerede analyse.

I dette setup er der 100 uniforme spillere. De modtager hver værdien 5 ved at indgå i spillet. Det koster under den strenge tilsynsregel 1 at overholde reglerne. Der er lagt til grund, at det koster 2 for de nationale myndigheder at føre tilsyn. Hver spiller modtager $5 - 1 = 4$, hvis de overholder reglerne. Hvis de ikke overholder reglen, modtager de 5, men risikerer en afskrækkende bøde på $4 + \varepsilon$.[141] Procentsatsen til venstre er det procentvise antal af spillere, der underkastes tilsyn fra de nationale myndigheder. I dette eksempel skal der således tilsynsføres over 25% af alle spillere før alle spillere har incitament til at overholde reglerne. Hvis der tilsynsføres under 25% vil spillerne alle bryde reglerne – Samfundsgevinsten, når man tager højde for alle tilsynsomkostninger, bliver således 350.[142]

	Under den strenge tilsynsregel		
	Spillernes forventede gevinst		Samfundsgevinst
	Ved overholdelse	*Ved brud*	*Ved overholdelse*
0%	400	500	400
10%	400	460	380
20%	400	420	360
25%	400	400	**350**
30%	400	380	340
40%	400	340	320
50%	400	300	300
60%	400	260	280
70%	400	220	260
80%	400	180	240
90%	400	140	220
100%	400	100	200

Kilde: Egen tilvirkning

Vi implementerer en lempelig regel, der for spilleren betyder en lavere overholdelsesomkostning i eksemplet 0,5. Alt andet er det samme. Man vil se, at payoff ved overholdelse stiger, på samme måde vil antallet af nationale tilsyn falde sammenlignet med den strenge regel i ligevægten. Er dette et overraskende resultat? På sin vis ikke. Ved at nedbringe den gevinst, der er ved at bryde reglerne, vil der være behov for færre nationale tilsyn og dermed en større samlet payoff.

	Under den lempelige tilsynsregel		
	Spillernes forventede gevinst		Samfundsgevinst
	Ved overholdelse	Ved brud	Ved overholdelse
0%	450	500	450
10%	450	460	430
12,5%	450	450	**425**
20%	450	420	410
30%	450	380	390
40%	450	340	370
50%	450	300	350
60%	450	260	330
70%	450	220	310
80%	450	180	290
90%	450	140	270
100%	450	100	250

Kilde: Egen tilvirkning

[141] Der er lagt til grund i forordningen, at bøder skal have afskrækkende virkning.
[142] Der er lagt til grund, at alle ligevægte, hvor spillerne ikke efterlever sine forpligtelser er ineffektive tilstande, hvorfor ligevægten 350 er optimum.

Spørgsmålet er således om dette holder generelt. Der har hidtil været lagt til grund, at spillerne ikke er uniforme. Det er derfor af stor vigtighed, at der ligeledes føres tilsyn med agenterne.[143] Det samme overordnede resultat vil dog holde for agenten. Eftersom de forventede overholdelsesomkostninger falder for principalen, vil de gøre det tilsvarende for agenten.[144] Det vil dermed være mere profitabelt at overholde sine forpligtelser for agenten, sammenlignet med den strenge tilsynsregel. Selv i den situation, hvor enten principalen eller agenten skulle have stor gevinst ved at afvige fra reglen, vil der således kunne tilsynsføres op mod 50% af samtlige spillere, før den lempelige regel ville være inefficient at implementere. I optimum bør de nationale myndigheder indrette sine tilsyn på en sådan måde, at der hvor incitamentet for manglende overholdelse er stort skal der tilsynsføres ofte. Der hvor incitamentet er mindre bør det ske sjældnere.

Det vurderes derfor, at virkningen af højere tilsynsfrekvens samt et tilpas bødeniveau opnår den samme virkning som den strenge regel. Dette medfører lavere samlede omkostninger hvoraf den vigtigste årsag er, at ikke alle agenter skal tilsynsføres. Under den strenge tilsynsregel opnår en given principal netop kun at påvirke, de spil denne selv er en del af.

Af disse grunde foreslås det, at der bør implementeres en lempelig tilsynsregel, hvor ansvarsfordelingen er ens med den man finder under den generelle ansvarsstruktur, da der her kun er ansvar i det omfang, der er viden eller bør-viden som principalen ikke reagerer på. Der bør være bødestraf på samme måde som under den generelle ansvarsstruktur.

I stedet for påtvungne tilsyn fra principalen, bør disse ske ved de nationale tilsynsmyndigheder, da man på denne måde får skabt en deterrence-effekt. Dette må antages at kunne ske til en lavere omkostning sammenlignet med, hvis spillerne skulle skabe samme virkning, hvor det ville kræve fuldstændig efterlevelse. Dette medfører store omkostninger, se eksemplet ovenfor. Af disse grunde vil man derfor kunne opnå det samme beskyttelsesniveau som under den strenge regel, samtidig med at de samlede omkostninger reduceres til gavn for alle, hvilket udgør en Kaldor-Hicks-forbedring.

[143] På den måde får man skabt deterrence-effekten i alle led.
[144] Agenten skal endnu sjældnere besvare anmodninger om tilsyn mv.

3.6 Økonomisk Delkonklusion:

Det kan på baggrund af analysen konkluderes, at det spil som kommer tættest på den interaktion, der sker mellem databehandleren og den dataansvarlige bedst kan beskrives som et koordinationsspil. Koordinationsspillets udfald er bl.a. bestemt af opdagelsesrisikoen som spillerne mødes med, spillernes type, hvilken værdi der kan skabes, størrelsen af overholdelses- og transaktionsomkostninger. Der findes grundlæggende tre spiltyper: (1) Et hvor begge spillere har et dominerende strategivalg ved overholdelse, (2) Et hvor begge spillere har et dominerende strategivalg ved ingen overholdelse, (3) og den sidste type, hvor spillerne har afvigende interesser. Den er navnlig den sidste spiltype, der har flere forskellige ligevægte. Reglernes ansvarsstruktur skaber generelt et svagt incitament for store behandlingskonstruktioner. Man vil se, at der, henset til opdagelsesrisikoen, først og fremmest er den dataansvarlige, som har et stærkt incitament til at overholde reglerne. Databehandleren har i svagere grad incitament til at overholde reglerne. Der er en positiv sammenhæng mellem størrelsen på behandlingskonstruktionen, samt varigheden set i forhold til opdagelsesrisikoen – Des større konstruktion og længere varighed, des større risiko for at blive opdaget.

Tilsynsforpligtelsen kan på nuværende tidspunkt beskrives som en streng tilsynsregel. Der undersøges ligeledes, hvad konsekvenserne af en lempelig regel er, og hvorvidt man kan iværksætte tiltag, der i økonomisk forstand er lige så effektive. Det konkluderes på baggrund af analysen, at man kan opnå en deterrence-effekt ved i stedet at overlade vilkårlige tilsyn til de nationale tilsynsmyndigheder. Den strenge regel forudsætter, at principalen fører tilsyn, hvorfor effekten af tilsyn kun har virkning i det enkelte spil og man således ikke opnår de gevinster, der er ved deterrence-effekten. Det analyseres ligeledes, at kritik som sanktionsvalg er en uegnet, da incitamentet til overholdelse bliver meget svagt. Netop ved at gøre overtrædelse mindre profitabelt, vil der være behov for færre nationale tilsyn sammenlignet med den strenge regel. På baggrund heraf kan det foreslås, at man kan øge efficiensen, ved at implementere en svag tilsynsregel, samt lade antallet af nationale tilsyn være styret af spillernes mulige gevinst ved et lavere payoff. Sanktionen for manglende efterlevelse bør være mulig bøde, da dette flugter med den overordnede ansvarsstruktur. På den måde vil man kunne minimere omkostningerne til overholdelse samtidig med, at man opnår samme beskyttelsesniveau.

Kapitel 4 - Integreret analyse

Der vil i den integrerede analyse undersøges den retsstilling, som den juridiske analyse fastlægger. Eftersom EU består af snart 27 lande, og Danmark ikke udgør en særligt stor del heraf, bliver det spændende at se, hvordan de enkelte medlemsstaters praksis og EU-praksis vil forme sig. Retsområdet er relativt ungt[145] og er i de senere år blevet en vigtigere del af mange virksomheders bevidsthed. Forordningen bidrog med to grundlæggende ændringer: (1) databehandlerens rolle blev beskrevet og ansvaret udvidet og (2) sanktionerne, herunder særligt bøderne, blev væsentligt forhøjet. Af disse grunde kan den generelle modenhed ikke antages at være fuldt opnået. Man vil formentlig se ny praksis udspringe i EU, efterhånden som de første EU-afgørelser bliver afsagt, og der vil ske flere afklaringer på andre områder. Det er ligeledes heller ikke til at sige, hvilken indflydelse eksempelvis udviklingen af lignende retsområder som eksempelvis outsourcing (EBA-guidelines), finansiel terrorlovgivning, hvor virksomheder bliver stillet lignende krav til risikovurderinger og tilsyn.[146]

Virkning ved nuværende regulering og den foreslåede tilsynsforpligtelse:

Der er lagt til grund, at der på europæisk plan skal lægges den samme fortolkning til grund ift. tilsynsforpligtelsen på forordningens anvendelsesområde.[147] Som tidligere fremhævet har det europæiske databeskyttelsesråd taget stilling til den danske databehandleraftale og vedtaget, at tilsynsvilkårene i pålagt den dataansvarlige at føre tilsyn, jf. ordene '*Skal*' i standarddatabehandleraftalens bilag C, C.7-C.8. Risikoen ligger i, at man udvikler en forskelligartet praksis i EU. I Danmark består risikoen i, at man indtager en position, der overimplementerer visse af persondataforordningens regler og krav.[148]

[145] Det dagældende direktiv blev vedtaget i 1995.
[146] Disse falder uden for afhandlingens område, men der vil i praksis være visse lighedstegn mellem de forpligtelser, som de enkelte virksomheder skal efterleve.
[147] Medlemsstaterne har i et vist omfang mulighed for at regulere udover forordningens bestemmelser. I Danmark har man eksempelvis ikke vedtaget bestemmelser, der udvider eller ændrer reglerne for databehandleraftaler eller kravene om påviselighed. Det danske datatilsyns praksis er et udtryk for reglen i forordningen, jf. forordning 2016/679
[148] Man benævner ofte denne situation gold plating, der beskriver en situation, hvor en medlemsstat overimplementerer et direktiv. Eftersom der er tale om forordning burde denne situation dog ikke kunne opstå.

Der er lagt til grund, at der potentielt kan pådrages bødeansvar for manglende tilsynsførelse for manglende påviselighed efter art. 5, stk. 2, jf. art. 83, stk. 5, litra a. Dette vil dog først komme på tale i længerevarende behandlerforhold, hvor den dataansvarlige ikke vil have taget skridt mod at sikre sig efterlevelse af art. 5, stk. 2 – Her er det forudsat, at behandlingen fra dens begyndelse har været lovlig, og den dataansvarlige har kunnet påvise dette.

Det er netop rækkevidden af tilsynsforpligtelsen og betydningen ift. ansvarsfordelingen, der vil have stor betydning for den fremtidige retspraksis og udvikling inden for denne afhandlings område. Det fremgår direkte af forordningens tekst, at bødeniveauet skal have afskrækkende virkning, jf. art. 83, stk. 9. Virksomheder og de enkelte registrerede vil have en klar interesse i en klarere retstilling, for bedre at kunne træffe informerede valg. På den anden side kan en uklar retsstilling betyde, at der ofte sker en af to ting: At selv risikoneutrale spillere vil overopfylde sine forpligtelser eller hvis der er tilpas stor usikkerhed, slet ikke efterleve reglen overhovedet.[149] Begge dele er ikke ønskeligt i et efficiens-perspektiv, da spillerne under den optimale regel netop kun efterlever det påkrævede niveau, forudsat sanktionen og risikoen for, at den indtræffer, er tilpas store. Så på måde vil en klarere retstilling, være en måde hvorpå man kan øge efficiensen. Der bør være overvejelser omkring, i hvilken udstrækning de nationale tilsynsmyndigheder overhovedet kan efterse de handlinger, som spillerne laver, i Craswell og Calfee's modeller indgår dette som standardafvigelse. I den økonomisk analyse har der været lagt til grund, at der ingen standard afvigelse er.

Som det fremgår i den økonomiske analyse, er det ønskeligt med en potentiel bødesanktion forudsat, der er en svag tilsynsregel, der tager afsæt i, at tilsynsaktiviteter fra de nationale tilsynsmyndigheder modsvarer gevinsten ved overtrædelse. Det bør bemærkes, at såfremt databehandleren nægter at lade sig tilsynsføre, så kan principalen reelt set kun opsige kontrakten og stoppe behandlingsaktiviteten. Der kan dog være afhængigheder, der vil gøre at principalen vil acceptere den risiko, der er for, at de ikke kan påvise overholdelse – Som et eksempel kan der fremhæves Hold-up-problemstillinger, hvor opsigelse ikke vil være en troværdig trussel for en part, der har investeret kraftigt.[150]

[149] Se bl.a. Craswell, Richard & Calfee, John E. 1986.
[150] Hendrikse, 2003, s. 210.

Der vil ikke være samme udfordring ved de nationale tilsyn. Man kan heller ikke udelukke, at tilsyn kan blive set som en fjendtlig handling, hvis reciprocitet har en betydning i spillet. Man kender denne situation med mange auditeringsbestemmelser.[151] I Rabins artikel,[152] der inkorporerer nogle psykologiske aspekter i spilteorien, vil man se, at spillet eksempelvis Battle of the Sexes potentielt kan få flere ligevægte, end hvad der følger af den strategiske Nash-ligevægt – Et af den centrale resultater er, at det netop er troen om modspillerens intentioner, som er styrende for spillerens strategivalg. Ved at tilsyn fortrinsvist sker gennem nationale myndigheder, fjerner man ligeledes de udfordringer, der potentielt kan være vedr. reciprocitet og brugen af tilsyn som en fjendtlig handling.

Der vil derfor være flere fordele ved at eksternalisere de vilkårlige tilsyn, og på den måde opnå en deterrence-effekt. Principalen bør alene være forpligtet til at føre tilsyn i de følgende situationer: Hvis principalen har, eller bør have viden om potentiel manglende efterlevelse, og de situationer, hvor der er stor risiko for de registrerede, og konsekvensen for de registrerede ved misbrug er store.[153] Den deterrence-effekt, der skabes ved de nationale tilsynsmyndigheder, vil sikre, at agenterne dels overholder reglerne samt, at de meddeler principalen ved ændringer i eksempelvis sikkerheden. På samme måde vil principalen handle overfor de nationale tilsynsmyndigheder.

Da man ikke nødvendigvis har indtaget den ovenfor beskrevne position, vil der være et potentielt værditab forbundet ved efterlevelse af reglen, som den på nuværende tidspunkt må fortolkes. Man må derfor håbe, at den fremtidige udvikling vil tage form i denne retning, og den risikobaserede tilgang i højere grad kommer til udtryk, ved vurdering af om et tilsyn overhovedet er påkrævet, og i givet fald iværksættes ved konkret viden/mistanke.

En af de effekter som persondatareglerne i al almindelighed medfører er, at der i højere grad leveres IT-produkter, som kan installeres direkte hos den enkelte kundes eget servermiljø for på den måde at

[151] Det ses ofte, at der i mange licensaftaler indføres auditeringsbestemmelser. Disse forpligter brugeren til at kunne stille en række oplysninger til rådighed, for at der således kan efterses om licensaftalen er overholdt. Det er grundlæggende en fjendtlig handling eftersom spilleren, som auditerer, ikke tror på modspilleren og søger at optimere på bekostning af modspilleren.

[152] Rabin, Matthew. 1993. 'Incorporating Fairness into Game Theory and Economies'.

[153] Den sidste del flugter med den risikobaserede tilgang, hvorefter der skal tages større skridt mod at beskytte data des større risiko, der er. Den bagvedliggende tanke er, at disse oplysninger, hvis misbrugt kan føre til store private tab.

undgå, at man har en databehandlerkonstruktion, hvis IT-løsningen leveres som SaaS.[154] På den måde opnår man ikke de stordriftsfordele, der kan være ved at levere Cloud-tjenester, hvor hver kunde ikke behøver et selvstændigt servermiljø, beskyttelse mv. På den anden side kan den dataansvarlige selv definere sikkerhedskravene, og har ingen risiko for, at der går noget galt hos en databehandler, så de samlede effekter er ikke entydige.

Man vil se, at de parter som alligevel behandler persondata, langt hen ad vejen vælger at rykke/etablere behandling inden for EU. Modsat er parterne forpligtet til at iværksætte en del flere foranstaltninger for at efterleve reglerne. Der kan være de helt lavpraktiske effekter såsom, at det kan være dyrere at drive et datacenter i EU end udenfor, f.eks. at strøm, leje af lokaler mv. er mere omkostningsfyldt. Reglerne medvirker til, at virksomheder fra 3. lande får sværere ved at entrere det indre marked. På den anden side er der ligeledes større sikkerhed for, at 3. landes regeringer ikke misbruger nationale virksomheders data til mere lyssky formål, som eksempelvis Huawei har været beskyldt for.[155]

Det håndhævelsessystem man har i eksempelvis Danmark, er i økonomisk forstand ikke optimalt. Datatilsynet kan kun udstede bøder i ukomplicerede sager, hvor den overtrædende virksomhed accepterer ansvaret og bøden, jf. Databeskyttelseslovens § 42, stk. 1. Det gør alt andet lige, at bødetruslen ikke er ligeså udtalt. Årsagen hertil skal findes i, at virksomheden først skal politianmeldes, og sagen derefter behandles ved domstolene, førend skyldspørgsmålet og bøden bliver effektueret. Sammenlignet med de fleste medlemsstater, hvor de nationale tilsynsmyndigheder har mulighed for at udstede bøder, vil effekten i Danmark være svagere. Det vil dels være tilfældet, da det ikke er sikkert, at en domstol vil komme frem til samme resultat som den nationale tilsynsmyndighed.[156] Derudover risikerer man, at der kan ske et tab af viden ved overdragelsen mellem datatilsyn og politi. Begge effekter gør alt andet lige, at risikoen i Danmark er mindre end lande, hvor der de nationale myndigheder kan udstede bøder. Årsagen til, at man i Danmark har valgt denne løsning er, at der ikke er mulighed for, at nationale myndigheder kan udstede bøder med den fortolkning, der er af magtdeling

[154] Software as a Service, dækker den situation, hvor den dataansvarlige eksempelvis får leveret et software-program denne tilgår via en internetforbindelse. Data processeres i skyen af leverandøren, der dermed bliver databehandler. Hvis det derimod leveres i den dataansvarliges egne servermiljøer, er der ikke tale om en databehandlerkonstruktion.
[155] Information. 2019: 'Kinesere i netværket: Skal vi være bange for Huawei?'.
[156] Der er her lagt til grund, at reglen som skal efterleves, indebærer usikkerhed for hvordan den vil fortolkes.

i Grundloven, jf. dennes § 3. Det er klart, at der i det omfang, der ikke er håndhævelsesproblemer og omkostninger, at den ene løsning er lige så god som den anden. Der vil dog ved at tilføje flere parter, som alle skal være enige om, at en given handling skal straffes være færre sager, der føres igennem. Man kender bl.a. denne problemstilling fra militæret, [157] hvorefter man har et hierarkisk beslutningssystem og beslutninger skal godkendes på alle hierarkiske niveauer førend man beslutter noget. I militære sammenhænge er det for at undgå de store konsekvenser, der kan være ved et forkert strategisk valg. Det er urealistisk, at grundloven ændres således, at det bliver muligt at indføre administrative bøder. Der bør derfor være flere nationale tilsyn i stater, der har et håndhævelsessystem som i Danmark.

Retlig standard eller regel?:

Det må først bemærkes, at den generelle tilgang er risikobaseret. Det vil sige, at des mere risikofyldt en given behandlingsaktivitet er, des mere må en part forventes at skulle iværksætte for at efterleve forordningens regler. Behandlingssikkerheden i art. 32 et udtryk for en standard, der er i evig forandring, fordi trusselsbilledet er i konstant forandring.

En del af forordningens regler bærer præg af at være standarder. Forskellen mellem en regel og en standard er, at standarden er mere fleksibel end reglen. Reglen fastlægger konkrete tiltag, der skal overholdes. I samfundsmæssigt perspektiv kan de to størrelser fungere lige fint, hvis indholdet blot er klart for den, denne retter sig imod. Hvorvidt store og små spillere som behandlet i den økonomiske analyse har fuldstændig viden, er næppe en realistisk antagelse. Navnlig små spillere, der ikke opnår Economy of Scales-effekter, vil drage nytte af, at forpligtelserne i højere grad fik form som egentlige regler. I værste fald risikerer man, at den retspraksis, der gerne skulle afhjælpe de tvivl, man konkret måtte have om IT-sikkerhed, kommer på et så sent tidspunkt, at de spørgsmål som afklares, ikke længere er relevante for nogen.

[157] Hendrikse, 2003, s. 365-366.

Spillerne vil forsøge at finde denne viden andre steder, f.eks. branchestandarder, best practice mv. Dette indebærer en risiko for, at domstolene ikke vil acceptere sådan dokumentation. Der er i forordningen lagt op til, at certificeringer kan fungere på lignende måder, hvilket netop skaber en formodning for, at man på europæisk plan får regulering, der minder om en regel, jf. art. 42. Det tilskyndes, at certificeringsmekanismen foregår på EU-plan. Det ville være enormt positivt sammenholdt med at reglen tager højde for: "*Mikrovirksomheders og små og mellemstore virksomheders særlige behov tages i betragtning.*", jf. art. 42, stk. 1, 2. pkt. Reglen er enormt vigtig i et transaktionsomkostningsperspektiv, fordi alle parter må forventes at kunne efterleve forordningens regler, men de omkostninger der er forbundet herved, kan være enormt store. En certificeringsmekanisme, hvor f.eks. IT-sikkerhedsstandarder fastslås, kan nedbringe transaktionsomkostninger og overholdelsesomkostningerne, men på nuværende tidspunkt findes der ikke nogen certificeringer, der lever op til dette på EU-plan.[158] I Danmark har man som tidligere nævnt ISAE3000-erklæringerne, men disse kan ikke uden videre tages som et udtryk for efterlevelse af forordningen, da erklæringens scope og revisorens undersøgelse har stor betydning for, hvad den reelt belyser. I det hele taget er den regulering, der ligger til grund meget løseligt formuleret, og bærer præg af at være mål og ønsker. Man har ikke forordningens tekst taget stilling til, hvordan man opnår fælleseuropæiske standarder. Det er derfor en meget reel risiko for, at der ikke vil være nok retskilder, til at fortolke reglens indhold på et givent tidspunkt. Det kan forventes, at private parter i høj grad kommer til at udfylde det tomrum, men der følger den risiko, at domstolene ikke vil anerkende et givent beskyttelsesniveau. Det er derfor af stor betydning, at der over tid udvikles og samarbejdes omkring retskilder på EU-plan, der opdateres og er tidssvarende. Risikoen ligger netop i, at selv risikoneutrale spillere overimplementerer reglerne som analyseret ovenfor, når der er usikkerhed i spillet.[159]

[158] EDPB. 2020. 'Register of certificitaion mechanism, seals and marks'.
[159] Richard & Calfee, John E. 1986.

Databehandleraftalen:

Et andet tiltag som kort er nævnt i den økonomiske analyse er, at transaktionsomkostninger direkte forbundet til databehandleraftalen kan nedbringes. I stedet for at lade parterne vedtage databehandleraftalen, kan man lade deklaratoriske regler gælde i det omfang parterne ikke har taget stilling til det. Fordelen herved er, at man fra lovgivers side kan fastsætte en rimelig baggrundsret, som mange uden videre vil acceptere.

Det er klart, at det ikke er muligt at gøre for hele aftalen. Parterne skal dermed tage stilling til færre forhold, og de risikerer ikke, at deres aftaletype vil blive underkendt ved en retslig vurdering. Transaktionsomkostninger må forventes at være mindre sammenlignet med den situation, hvor parterne skal forhandle sig frem til en aftale. På den måde er det positivt, at der nu er kommet en standard databehandleraftale, da den skaber grobund for videre diskussion og nogle af de samme effekter. En af de store udfordringerne er samtidigt også, at denne standard alene eksisterer på dansk og engelsk.[160] Man vil dermed ikke opnå den samme udbredelse som tilfældet ville have været, hvis det var udgivet på samtlige officielle EU-sprog af Databeskyttelsesrådet og i øvrigt havde bindende virkning overfor de nationale tilsynsmyndigheder. Et tiltag som dette vil ikke sænke beskyttelsesniveauet, men alene gælde deklaratorisk og dermed potentielt nedbringe de samlede omkostninger til overholdelse. Der kan være udfordringer imellem de enkelte medlemsstater, eftersom der grundlæggende er forskellige tilgange til aftaleretten. Man bør dog kunne tilpas standarden, til ligeledes at kunne bruges i disse medlemsstater, selv hvis egentlige fælles deklaratoriske regler er umulige at gennemføre.

Nationale tilsyn og bødeniveauet:

Det følger af forordningens art. 83, stk. 9, at der ved idømmelsen af bøder, at disse skal have afskrækkende virkning, og relaterer sig til bødeniveauets størrelse. Man må i økonomisk forstand forstå

[160] Der er pr. 7/5 – 2020, oplyst, at den danske standard anerkendes af de svenske og norske myndigheder. Dette binder dog ikke andre medlemsstater, se: Datatilsynet, 2020. 'Datatilsynets standarddatabehandleraftale kan også anvendes i Norge og Sverige'.

dette på en måde, hvormed sandsynligheden for at blive opdaget, og bødeniveauet begge er tilpas store således, at den fordel en part ville få ved at overtræde reglerne, ikke overstiger den forventede bødestraf ved overtrædelse. Man kan forvente, at bødeniveauet er ens uanset hvor overtrædelsen sker, og alle medlemsstaternes nationale myndigheder vil vurdere spørgsmålet ens.[161] Det er dog i økonomisk forstand ikke givet, at antallet at tilsyn er ens på tværs af medlemsstater. Det er muligt, at overtrædelser skaber større payoff for en spiller i et land sammenlignet med et andet. Eksempelvis, hvis omkostningerne ved at drive virksomhed i en medlemsstat er lavere end andre. I økonomisk forstand skal antallet af tilsyn de nationale myndigheder iværksætter, være relativt flere end de medlemsstater med større produktionsomkostninger. Det er vigtigt de enkelte medlemsstater sikrer, at der netop blot er et negativt payoff ved en given overtrædelse. Dette resultat medfører netop, at lavomkostnings-medlemsstater skal tilsynsføre oftere, end tilfældet er i højomkostningslande. Effektiv beskyttelse forudsætter dermed, at medlemsstaterne koordinerer og tilsikrer, at der ikke er mulighed for, enkelte virksomheder kan spekulere i, hvor de med fordel kan placere sine aktiviteter.

4.1 Hvilke tiltag kan indføres, hvis beskyttelsesniveauet kan nedsættes blot marginalt?

Der har generelt i denne afhandling været lagt vægt på, at beskyttelsesniveauet skulle være uforandret. En måde man kan øge efficiensen er, hvis det er muligt ændre på eksempelvis forordningens anvendelsesområde. Eftersom forordningen trådte i kraft i 2018, og det dagældende direktiv havde være gældende i 20 år, må man gå ud fra, at forordningen ligeledes får en lang levetid. Det vil derfor ikke være realistisk at ændre den grundlæggende model. I det omfang risikovurderingen viser, at der er meget begrænset risiko, så bør der være mulighed for, at forholdet ikke bør tilsynsføres. Med den forståelse der er nu, skal alt tilsynsføres uanset om risikoen er absolut minimal. Nogle af de åbenlyse eksempler kunne være, at oplysningerne er offentligt tilgængeligt, der kunne være tale om arbejdsmails/navne, eller endda oplysninger som er, i den registreredes interesse bliver behandlet. Man kan overveje, hvorvidt det er meningsfyldt overhovedet at lade forordningen omfatte sådanne oplysninger – I økonomisk perspektiv ville det være mest efficient kun at beskytte de oplysninger, der

[161] Der tages her ikke højde for national(e) sektorlovgivning/særregler.

potentielt kan være skadegørende. Dette er dog ikke et realistisk udfald. Det må derfor være i samfundets interesse, at der ikke skal tilsynsføres, hvis risikovurderingen viser, at risikoen er næsten ikkeeksisterende. Man undgår dermed, at der skal bruges ressourcer til at beskytte oplysninger, der ved brud er mere eller mindre 0. På samme måde vil det være fordelagtigt, at de nationale tilsynsmyndigheder heller ikke undersøgte sådanne behandlinger.

Datatilsynet nævner i deres vejledninger, at tilsynets hyppighed er direkte afhængigt af den konkrete risiko. En meget lav risiko udgør i sig selv ikke, at man kan undgå at skulle føre tilsyn. I økonomisk forstand bør dette dog være tilfældet. Det er hensigtsmæssigt i de situationer ikke at tilsynsføre, når risikoen er meget begrænset, netop fordi det private/samfundsmæssige tab ved brud er absolut minimalt. Det vil derfor være i samfundets interesse, at den fremtidige praksis vil udvikle sig i denne retning, selvom det indebærer et lavere beskyttelsesniveau.

4.2 Integreret delkonklusion

Det fastslås i den integrerede analyse, at den lempelige tilsynsregel bør implementeres. Det foreslås derudover, at medlemsstaterne i høj grad samarbejder på EU-plan, for at sikre at de retlige standarder bliver yderligere præciserede – På den måde modvirker man overcompliance fra spillerne. På tilsvarende vis kan tilsyn fra nationale myndigheder løse de inefficiente ligevægte, der kan følge af reciprocitet. Der bør ligeledes komme en fælles standard databehandleraftale, og man bør på EU-plan overveje, hvorvidt disse krav først og fremmest skal gøres deklaratoriske. På den måde vil man nedbringe transaktionsomkostningerne. De nationale tilsyn bør fastsætte deres tilsynsfrekvens, efter hvilket payoff spillerne får, for på den måde at skabe deterrence-effekt. Det er derfor vigtigt, at man i medlemsstaterne samarbejder og sikrer ens håndhævelse, således at arbitrage ikke er muligt. F.eks. via certificering, der tager højde for virksomhedens størrelse, jf. art. 42, stk. 1, 2. pkt.

Et af de tiltag man kan iværksætte og nedbringe behandlingssikkerheden, under det nuværende regelsæt, er at lade enorm lille risiko være et udtryk for, at der ikke er behov for tilsyn, hverken fra den dataansvarlige eller de nationale myndigheder.

Samlet konklusion:

Denne afhandlings overordnede spørgsmål er, i hvilken udstrækning Persondataforordningens ansvarsstruktur er efficient samt hvilken betydning tilsynspligten har i denne sammenhæng.

Den grundlæggende ansvarsstruktur er således, at den dataansvarlige er ansvarlig for hele behandlerkonstruktionen, jf. art. 5, stk. 2. Dette indebærer, at denne skal godkende, påvise og kunne dokumentere databehandlernes aktiviteter. Netop kravet om påviselighed indebærer, at den dataansvarlige på et senere tidspunkt stadig skal efterleve disse krav. En måde at gøre dette på, er ved at føre tilsyn med databehandlerne, jf. art. 28, stk. 3, litra h. Mængden af retskilder på nuværende tidspunkt omhandler langt hen ad vejen, hvilke informationer databehandleren skal kunne stille til rådighed. To danske tilsynsafgørelser har fastslået, at tilsynet er en pligt som den dataansvarlige skal efterleve. Det er derfor ikke taget stilling til, om manglende tilsyn potentielt kan medføre ansvar, for ikke at kunne påvise lovlig behandling. Forordningens formål er at beskytte persondata, hvorfor der ikke kan være nogen tvivl om, at den dataansvarlige skal kunne påvise overholdelse – Det er dog ikke ganske klart på nuværende tidspunkt, hvad der er tilstrækkeligt, og hvilken konsekvens manglende efterlevelse medfører.

Interaktionen mellem databehandleren og den dataansvarlige kan sættes op som spillet Battle of the Sexes. Spillernes incitamentsstruktur er dog ikke altid som i Battle of the Sexes. De spillere som har en lav risiko, for at blive opdaget, betegnes små spillere – Dette vil ofte være databehandleren. Den dataansvarlige vil være udsat for en større risiko for opdagelse, hvorfor disse betegnes store spillere. Generelt skaber reglerne incitament til at beholde små behandlerkonstruktioner, og reglerne har en negativ betydning for nye teknologier. Der er Economy of Scales-effekter i forbindelse med overholdelse af reglerne for spillerne. Tilsynsreglen er undersøgt hhv. som streng og lempelig. Den strenge regel medfører en tilsynspligt, hvorimod den lempelige regel forudsætter, at tilsyn skal ske ved konkret mistanke/viden. Sanktionen kritik er uegnet som sanktion i alle tilfælde sammenlignet med bøde. Den lempelige regel og tilpas mange vilkårlige tilsyn fra de nationale myndigheder kan have samme beskyttelsesniveau. Denne tilstand medfører færre omkostninger end den strenge regel, årsagen hertil skal findes i, at man ved at nedbringe tilsynsomkostningen, nedbringer incitamentet for

ikke at overholde reglen. Der skabes ligeledes en deterrence-effekt, hvilket kommer til udtryk på to måder. Der er behov for færre nationale tilsyn for at sikre overholdelse, og spillerne vil opnå et større payoff ved overholdelse sammenlignet med den strenge regel.

Foruden resultaterne i den økonomiske analyse, er det ligeledes i den integrerede analyse fastslået, at særligt samarbejde mellem medlemsstaterne er af stor vigtighed. Dels skal det koordineres så, der opnås deterrence-effekt i samtlige lande, dette kan medføre, at nogle lande skal tilsynsføre oftere end andre. De retlige standarder skal specificeres, således at overholdelse bliver lettere for mindre virksomheder. Derudover bør certificeringsmekanismer og databehandleraftaler udarbejdes på EU-niveau, således at reglerne bliver klarere, og transaktionsomkostningerne ved overholdelse minimeres. På den måde undgår man overcompliance, og dermed et inefficient beskyttelsesniveau, som følge af usikkerhed omkring, hvordan reglen må forstås. Vilkårlige nationale tilsyn kan ligeledes, hvis reciprocitet spiller en rolle, eliminere inefficiente ligevægte i spillet 'Battle of the Sexes' som følger heraf.

Det kan dermed foreslås, at der samarbejdes tæt imellem landene for at sikre effektiv og efficient overholdelse som analyseret i den økonomiske og integrerede analyse. Derudover bør den fremtidige praksis forme sig således, at tilsynsforpligtelsen er lempelig for den dataansvarlige.

Anvendte forkortelser:

Databehandleraftale – DBA

Det europæiske databeskyttelsesråd – EDPB (European Data Protection Board)

Personoplysninger – Persondata

Litteraturliste

Hjemmesider:

- Det Europæiske Databeskyttelsesråds hjemmeside. Sidst set 12. maj 2020: https://edpb.europa.eu/edpb_en.
- The Guardian, 2020. 'Fresh Cambridge Analytica leak 'Shows global manipulation is out of control'' Sidst set d. 4 Maj 2020 på The Guardian's hjemmeside: https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation
- ICO. 2019: 'ICO announces intention to fine British Airways £183,39m under GDPR for data breach' Sidst set d. 28 april 2020 på ICO's hjemmeside: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
- ICO. 2019: 'Statement: Intention to fine Marriot International, Inc more than £99 million under GDPR data breach' Sidst set d. 28 april 2020 på ICO's hjemmeside: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
- Information. 2019: 'Kinesere i netværket: Skal vi være bange for Huawei?'. Sidst set 2/5 – 2020 på Information.dk: https://www.information.dk/indland/2019/01/kinesere-netvaerket-vaere-bange-huawei
- Datatilsynet, 2020. 'Datatilsynets standarddatabehandleraftale kan også anvendes i Norge og Sverige'. Sidst set 8/5 – 2020 på datatilsynets hjemmeside: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/maj/datatilsynets-standarddatabehandleraftale-kan-anvendes-ogsaa-i-norge-og-sverige/.

Traktater, Forordninger/direktiver og love:

Traktater:

- Traktaten om den Europæiske Union.
- Traktaten om den Europæiske Unions Funktionsmåde.
- Den europæiske unions charter om grundlæggende rettigheder

Forordninger:

- EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679, 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).

Direktiver:

- EUROPA-PARLAMENTET OG RÅDETS DIREKTIV 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

Love:

- Danmarks Riges Grundlov, Lov nr. 169 af 5. juni 1953.
- Databeskyttelsesloven, Lov nr. 502 af 23/05/2018.
- Persondataloven, Lov nr. 429 af 31. maj 2000 (med senere ændringer) - historisk

Vejledninger og oversigter:

Det danske datatilsyn:

- 'Vejledning om dataansvarlige og databehandlere', publiceret i november 2017 af Datatilsynet.

- 'Vejledende tekst om risikovurdering' Publiceret juni 2019 af Datatilsynet og Rådet for Digital Sikkerhed.
- 'Vejledende tekst om tilsyn med databehandlere og underdatabehandlere' Publiceret maj 2018 af Datatilsynet.

Det britiske datatilsyn - ICO:

- ICO. 2020. 'What needs to be included in the contract?'. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/
- ICO. 2020. 'Accountability and governance'. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

EU - EDPB:

- European Data Protection Board har ligeledes revideret tidligere guidelines, vedrørende konsekvensanalyse 'Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)'
- EDPB. 2020. 'Register of certificitaion mechanism, seals and marks'. https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en
- EPDB. 2020. 'Register for Codes of Conduct, amendments and extensions'. https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en

Standard aftaletyper, udtalelser:

Standard databehandleraftaler:

- Standardkontraktbestemmelser vedr. behandling af persondata, publiceret d. 10. december 2019 af det danske Datatilsyn. Aftalen kan findes på datatilsynets hjemmeside datatilsynet.dk.
- Datatilsynet, 2018, 'Ny skabelon skal hjælpe virksomheder og myndigheder med at blive klar til databeskyttelsesforordningen' - historisk.

Udtalelser:

- Det europæiske databeskyttelsesråds kommentarer til det først fremsendte udkast kan findes på Edpb.europe.eu og bærer navnet 'udtalelse 14/2019' vedtaget 9. juni 2019, med hjemmel i forordning 2016/679 art. 64, stk. 1, litra d.

Domme og tilsynsafgørelser:

Domme:

- Patrick Breyer mod Bundesrepublik Deutschland, sag C-582/14, EU:C:2016:779.
- Sri CILFIT og Lanificio di Gavardo SpA mod sundhedsministeriet, Sag 283/81, EU:C:1982:335.

Tilsynsafgørelser:

- **Tilsynsafgørelse vedr. Randers Kommune,** https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/aug/afslutning-af-planlagt-tilsyn-hos-randers-kommune/:

I tilsynsafgørelsen vedr. Randers Kommune, publiceret d. 5/8-2019, blev der i relation til kommunens behandlingsaktiviteter undersøgt måden der førtes tilsyn på.

Det er værd at bemærke, at Datatilsynet lagde vægt på, at det var en formildende omstændighed, at der skulle indgås mange DBA'er samt at denne proces kan være tidskrævende. Rækkevidden af dette synes dog ikke at strække sig udover den situation, hvor regelsættet netop er trådt i kraft. Det vil næppe være undskyldeligt ikke at have indgået DBA'er, blot fordi det er tidskrævende og kræver planlægning. Randers Kommunes tilsyn med databehandlere indebar, at de havde modtaget revisionserklæringer fra deres databehandlere og forholdt sig til indholdet af disse – Dette levede op til kravene. Datatilsynets stikprøve bestod i at tage 2 konkrete databehandlere ud af 210, godt og vel 1% af den samlede masse. Kommunen havde dog ikke ført tilsyn med underdatabehandlere, det var ikke nok at der stod i aftalen at databehandleren førte tilsyn med underdatabehandleren, dette skal den dataansvarlige selv følge op og sikre dokumentationen.

- **Tilsynsafgørelse vedr. Viborg Kommune -** https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/aug/afslutning-af-planlagt-tilsyn-hos-viborg-kommune/**:**

I tilsynsafgørelsen vedr. Viborg Kommune, publiceret d. 5/8-2019, fandt man, at der ikke var ført tilsyn eller indhentet nogen revisionserklæringer, på trods af, at kommunen havde oplyst, at de havde haft telefoniske drøftelser med deres databehandlere. Stikprøven bestod af 3 ud af 130 databehandlere. Datatilsynet udtalte alvorlig kritik af forholdet.

- **Tilsynsafgørelse vedr. 'Databehandlers behandling af personoplysninger uden for instruks'** https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/dec/databehandlers-behandling-af-personoplysninger-uden-for-instruks/:

I tilsynsafgørelsen vedr. Herning kommune publiceret 19-12-2019, anmeldte Herning kommune, at en databehandler, ikke havde oplyst, at der blev benyttet underdatabehandlere. Dels var, der efter omstændighederne tale om en fejltagelse, men der var ingen hjemmel til overførsel til 3. land, hvorfor der alligevel var tale om et brud på persondatasikkerheden.

Bøger og artikler:

Bøger:

- Nielsen, Ruth & Tvarnø, Christina D. 2017. *Retskilder og retsteorier*. København: Jurist- og Økonomforbundets Forlag. 5. udgave.
- Knudsen, 1994. Økonomisk Metodologi, Bind 1, Videnskabsteori & Forklaringstyper. København: Jurist- og økonomforbundets forlag 2. udgave, 1. oplag 1994.
- Knudsen, Christian. 1997. *Økonomisk metodologi Bind 2*. København: Jurist- og Økonomforbundets Forlag. 2. Udgave.
- Hendrikse, George. 2003. *Economics and Management of Organizations*. London: McGraw-Hill Education.
- Christensen, Leslie & Rasmussen, Helmer, Jens. *Microeconomics*. 2013. Harlow: Pearson Education Limited.
- Andersen, Lennart Lynge & Madsen, Palle Bo. *Aftaler og Mellemmænd*. 2012. København: Karnov Group Denmark A/S, 6. udgave, 1. oplag.
- Dutta, Prajit. 1999. *Strategies and Games.* England: The MIT Press.
- Tvarnø, Christina & Denta, Sarah Maria. 2015. *Få styr på metoden*. København: Ex Tuto Publishing. 1. udgave.
- Eyben, Bo von & Isager, Helle. 2015. *Lærebog i erstatningsret*. Danmark: Jurist- og Økonomforbundets Forlag. 8. udgave, 1. oplag.
- Neergaard, Ulla & Nielsen, Ruth. 2016. *EU ret*. København: Karnov Group Denmark A/S, 7. udgave, 1. oplag.

Artikler:

- Stafford, Mark. 2015. 'Deterrence Theory: Crime'. International Encyclopedia of the Social & Behavioral Sciences.
- Craswell, Richard & Calfee, John E. 1986. 'Deterrence and Uncertain Legal Standards'. Journal of Law, Economics, & Organization, Vol. 2, No. 2 (Autumn, 1986), pp. 279-303.
- Rabin, Matthew. 1993. 'Incorporating Fairness into Game Theory and Economies'. The American Economic Review, Vol. 83, No. 5 (Dec., 1993), pp. 1281-1302.